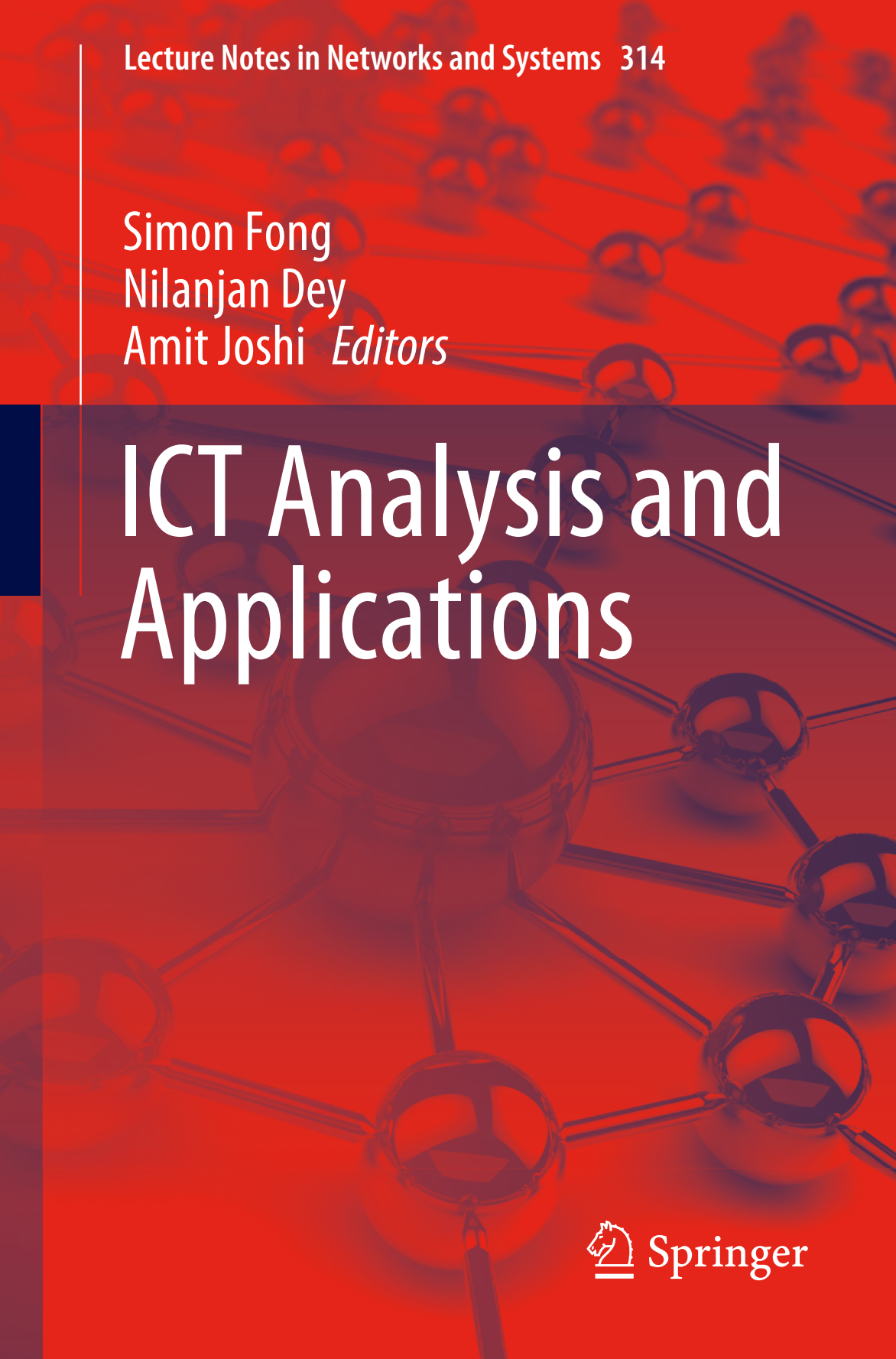
Lecture Notes in Networks and Systems 314

Simon Fong
Nilanjan Dey
Amit Joshi *Editors*

ICT Analysis and Applications



Springer

Lecture Notes in Networks and Systems

Volume 314

Series Editor

Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland

Advisory Editors

Fernando Gomide, Department of Computer Engineering and Automation—DCA, School of Electrical and Computer Engineering—FEEC, University of Campinas—UNICAMP, São Paulo, Brazil

Okyay Kaynak, Department of Electrical and Electronic Engineering, Bogazici University, Istanbul, Turkey

Derong Liu, Department of Electrical and Computer Engineering, University of Illinois at Chicago, Chicago, USA
Institute of Automation, Chinese Academy of Sciences, Beijing, China

Witold Pedrycz, Department of Electrical and Computer Engineering, University of Alberta, Alberta, Canada
Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland

Marios M. Polycarpou, Department of Electrical and Computer Engineering, KIOS Research Center for Intelligent Systems and Networks, University of Cyprus, Nicosia, Cyprus

Imre J. Rudas, Óbuda University, Budapest, Hungary

Jun Wang, Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong

The series "Lecture Notes in Networks and Systems" publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

More information about this series at https://link.springer.com/bookseries/15179

Simon Fong · Nilanjan Dey · Amit Joshi
Editors

ICT Analysis and Applications

Springer

Editors
Simon Fong
Department of Computer and Information Science
University of Macau
Macau, Macao

Nilanjan Dey
JIS University
Kolkata, India

Amit Joshi
Global Knowledge Research Foundation
Ahmedabad, India

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-981-16-5654-5 ISBN 978-981-16-5655-2 (eBook)
https://doi.org/10.1007/978-981-16-5655-2

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022, corrected publication 2022
This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The Sixth International Conference on ICT for Sustainable Development (ICT4SD 2021) targets theory, development, applications, experiences and evaluation of interaction sciences with fellow students, researchers and practitioners.

The conference may concern any topic within the conference scope. Workshops may be related to any topics within the conference scope. The conference is devoted to increase the understanding role of technology issues, how engineering has day by day evolved to prepare human-friendly technology. The conference will provide a platform for bringing forth significant research and literature across the field of ICT for sustainable development and provide an overview of the technologies awaiting unveiling. This interaction will be the focal point for leading experts to share their insights, provide guidance and address participant's questions and concerns.

The conference was to be held during August 5–6, 2021, at Hotel Vivanta, Panaji, Goa, India, but due to the pandemic, this year it was organized through digital mode, and few of the papers were presented physically at the Venue on August 6, 2021. The conference was organized by Global Knowledge Research Foundation, Supporting Partner InterYIT, International Federation for Information Processing, State Chamber Partner Goa Chamber of Commerce and Industry, and National Chamber Partner Knowledge Chamber of Commerce and Industry.

Research submissions in various advanced technology areas were received and after a rigorous peer-reviewed process with the help of program committee members and 193 external reviewers for 850+ papers from 16 different countries including Algeria, USA, United Arab Emirates, Serbia, Qatar, Mauritius, Egypt, Saudi Arabia, Ethiopia and Oman out of which 180 were accepted with an acceptance ratio of 0.17.

Technology is the driving force of progress in this era of globalization . Information and communication technology (ICT) has become a functional requirement for the socioeconomic growth and sustained development of any country. The influence of information communications technology (ICT) in shaping the process of globalization, particularly in productivity, commercial and financial spheres, is widely recognized. The ICT sector is undergoing a revolution that has momentous implications for the current and future social and economic situation of all the countries in the world. ICT plays a pivotal role in empowering people for self-efficacy and how

it can facilitate this mission to reach out to grassroots level. Finally, it is concluded that ICT is a significant contributor to the success of the ongoing initiative of Startup India.

In order to recognize and reward the extraordinary performance and achievements by ICT and allied sectors and promote universities, researchers and students through their research work adapting new scientific technologies and innovations. The two-day conference had presentations from the researchers, scientists, academia and students on the research work carried out by them in different sectors.

The summit will be addressed by eminent dignitaries including Shri Nitin Kunkolienker, President, MAIT; Shri. Prajyot Mainkar, Chairman, IT Committee of Goa Chamber of Commerce and Industry; Mike Hinchey, President, IFIP and Chair IEEE, UK and Ireland; Milan Tuba, Vice-Rector for International Relations, Singidunum University, Serbia; Prof. Jagdish Bansal, India; Mr. Aninda Bose, Springer; and Dr. Amit Joshi, Director, G R Foundation. The overall conference had 1 inaugural session, 1 keynote session and 18 technical sessions during two days.

Macau, Macao — Simon Fong
Kolkata, India — Nilanjan Dey
Ahmedabad, India — Amit Joshi

Contents

Analysis of Codon Usage Bias in *Cya, Lef,* and *Pag* Genes Exists in px01 Plasmid of *Bacillus Anthracis* 1
Sushma Bylaiah, Seema Shedole, Kuralayanapalya Puttahonnappa Suresh, Leena Gowda, Sharanagouda S. Patil, and Uma Bharathi Indrabalan

Constructing Digital Signature Algorithm Based on a New Key Scheme 11
Van Luu Xuan, Hoa Doan Van, and Dung Luu Hong

Internet of Things (IoT), Three-Layer Architecture, Security Issues and Counter Measures 23
Bonani Paul

Intermittent Leather Defect Detection Based on Ensemble Algorithms Derived from Black Hat Transformation and Hough Transformation 35
Swamiraj Nithiyanantha Vasagam and Madasamy Sornam

Efficient Strategies to Manage Road Traffic Using Big Data Analytics 47
Yogesh Golhar and Manali Kshirsagar

Travel Booking and Management Application: TravelBel 57
Elroy Gomes, Tryambak Gour, Arushi Sinha, and R. Dakshayani

Security and Privacy Issues in Internet of Things 65
Dipankar Debnath, Sarat Kr. Chettri, and Ajoy Krishna Dutta

Industry 4.0: An Overview and Further Research Directions 75
Padmanabha Aital, Rajesh Patil, Sashikala Parimi, and Prerna Singh

A Comprehensive Survey on Trust Management in Fog Computing 87
Sheenu Singh and Meetu Kandpal

Personal Identification Using Fuzzy Approach and RSA Algorithm 99
Sharmila S. More, Bhawna Narain, and Bharat T. Jadhav

ICT and Administrative Reforms: A Literature Review 107
Sridharan Kesavan, Aakansha Uppal, and Bhavna Pandey

Analysis of Fault Tolerance Techniques in Virtual Machine Environment 121
Shelly Prakash and Vaibhav Vyas

Analysis of Symmetric and Asymmetric Key Algorithms 133
Jitaksh Kapoor and Divyansh Thakur

A Hybrid Approach for Retrieving Geographic Information in Wireless Environment Using Indexing Technique 145
Prashant Vats, Zunaid Aalam, Satnam kaur, Amritpal kaur, and Neha Gehlot

A Survey on Human Action Recognition and Detection Techniques 157
Shankargoud Patil and Kappargaon S. Prabhushetty

Parallel Algorithm to Efficiently Mine High Utility Itemset 167
Eduardus Hardika Sandy Atmaja and Kavita Sonawane

A Review on Insulators in Transmission Line—Progress and Comparative Studies 179
Keka Mukhopadhyaya

Security and Privacy Issues of Blockchain Technology in Health Care—A Review 193
Nida Fatima, Parul Agarwal, and Shahab Saquib Sohail

Hardware Trojan Detection Using Deep Learning-Generative Adversarial Network and Stacked Auto Encoder Neural Networks 203
Fredin Jose, M. Priyatharishini, and M. Nirmala Devi

Automatic Credit Fraud Detection Using Ensemble Model 211
S. Srinidhi, K. Sowmya, and S. Karthika

Blockchain in Education Sector – Boon or Curse 225
Pratyush Jha, Yug Chandak, and Aman Gupta

Image Feature Generation Using Binary Patterns—LBP, SLBP and GBP 233
S. Divya, L. Padma Suresh, and Ansamma John

Location Dependent Safety Application for Women 241
M. B. Shanthi, Prakhyath Jain, and M. Prateek

A Review of Adaptive and Intelligent Online Learning Systems 251
Deshna Sachan and Kriti Saroha

Background Manipulation with Computer Vision 263
A. Tamilarasi and Gourav Kumar

Swear Words Replacement Suggestion System 271
S. Naveen, Mayank Singh, and S. Karthika

A Review of Deduplicate and Significance of Using Fuzzy Logic 281
V. Ranjith, M. K. Dhananjaya, P. Yamini Sahukar, M. Akshara, and Partho Sharothi Biswas

SIoT (Social Internet of Things): A Review 289
Saima Shahab, Parul Agarwal, Tabish Mufti, and Ahmed J. Obaid

STAT Simple Text Annotation Tool (STAT): Web-based Tool for Creating Training Data for spaCy Models 299
Darshita Kumar, Kshitija Choudhari, Pooja Patel, Shambhavi Pandey, Aparna Hajare, and Shubham Jante

Credential-Based Authentication Mechanism for IoT Devices in Fog-Cloud Computing 307
Hala S. Ali and R. Sridevi

NAYAN-DRISHTI: A Revolutionary Navigation/Visual Aid for the Visually Impaired 319
Salil Fernandes, Jordan D'souza, Anthony Kattikaren, and Dipti Jadhav

Hygieia: Smart Health and Sanitizing Dispenser 335
Vaibhav Tiwari, Sudharm Kalamdani, Rohit Raut, and P. K. Rajani

Designing an Algorithm to Support Optimized Crop Selection by Farmers 345
Mayank Phadke, Mridula Goel, Rishabh Bajpai, and Nishchay Mehta

Security in Industrial Control Systems Using Machine Learning Algorithms: An Overview 359
Pallavi Arora, Baljeet Kaur, and Marcio Andrey Teixeira

Channelising Digitalisation Amidst COVID-19 Outbreak: Case of Multichannel ICTs in Pakistan 369
Bisma Iftekhar and Hasnain Bokhari

VLSI Design Flow Using Vinyas Design Bot 379
Veena S. Chakravarthi, S. Sowndarya, and Shubham Raj

Detection and Classification of Brain Tumor Using MRI Images 393
Rahul Koli, Sahil Lotya, Prasad Govekar, Karan Sachdev, and Gresha Bhatia

Online Food Delivery (OFD) System: An Empirical Study of the Polarization of Potential Consumers and Investigating the Association Between the Determinants Molding the Polarization During COVID-19 Pandemic 403
Jarin Tasnim, Tanvir Alam, Samapty Saha, and Md Forhad Rabbi

Accident Hotspot Detection by DB-Scan Clustering 413
Pooja Shinde, Gauri Kudalkar, Shruti Pawar, Harshita Tiwari, and Hitendra Khairnar

AI Powered Language Teaching Bot Using Dialogflow 419
Chingmuankim and Rajni Jindal

Analyses of Feature Selection and Classification Techniques for Diabetes Prediction 427
Sina Patel, Vijayshri Khedkar, and Sonali Kothari Tidke

Analysis of Marketing Mix and Website Performance on E-marketplace of Agricultural Products 437
Reni Diah Kusumawati, Teddy Oswari, Tristyanti Yusnitasari, and Himanshu Dutt

A Machine Learning Approach for Gait Based Human Authentication in Smart Cities 445
Arindam Singh and Rajendra Kumar Dwivedi

Blockchain for Fool-Proof E-Voting Systems 455
Janardan Krishna Yadav, Srinivas Jangirala, Deepika Chandra Verma, Shashi Kant Srivastava, and Shehzad Ashraf Chaudhry

UAV System Using Convolutional Neural Network (1. Angle Prediction Model) 467
Abhishek Muttath, Aditya Veer, Muskan Pandey, Mayuresh Gawai, and Vaishal Wangikar

Blockchain for Aviation Industry: Applications and Used Cases 475
Janardan Krishna Yadav, Deepika Chandra Verma, Srinivas Jangirala, Shashi Kant Srivastava, and Muhammad Naveed Aman

Diabetes Mellitus Prediction Using Ensemble Learning Approach with Hyperparameterization 487
Rashmi Srivastava and Rajendra Kumar Dwivedi

Fairness, Accountability, Sustainability, Transparency (FAST) of Artificial Intelligence in Terms of Hospitality Industry 495
Sunil Sharma, Yashwant Singh Rawal, Sanjeeb Pal, and Rakesh Dani

Analysis of ECG Signal Processing for Smart Medical Technologies 505
J. N. Swaminathan, R. Rameshkumar, I. Vidyasagar, I. Divya, and R. Navaneethakrishnan

Technical Analytical Study to Forecast the Buy-Sell Signal to Determine Investment Strategy for Maximize the ROI 513
Amit B. Suthar, Hiral R. Patel, and Satyen M. Parikh

A Machine Learning and Deep Neural Network Approach in Industrial Control Systems 525
S. Ribu Hassini, T. Gireesh Kumar, and S. Kowshik Hurshan

Positioning Based on Global Navigation Satellite System 537
V. Tanuja and Sumalatha Aradhya

Online Teaching Tools: Challenges and Their Solutions During a Pandemic Available in India 547
Nitin S. More and Ram Vankadara

Cloud Computing in a Distributed Environment Implemented with Networking Technologies 557
S. Sai Satyanarayana Reddy

Detection of Insider Threat Based on Forensic Analysis of Windows 565
Kaushal Bhavsar and Bhushan Trivedi

License Plate Recognition for Stolen Vehicles Using Optical Character Recognition 575
Armand Christopher Luna, Christian Trajano, John Paul So, Nicole John Pascua, Abraham Magpantay, and Shaneth Ambat

A Meta-Analysis on Online Classes for Hotel Management Students at Chennai During Covid-19 585
T. Milton and H. M. Moyeenudin

Traveling Salesman Problem Solution Using Plate Tectonics Based Neighborhood Search Optimization 597
Lavika Goel

An Optimistic Approach for Managing the Handover Latency by Using Dynamic Data in Software Defined Networks (SDN) 607
Krishna Shah and Kishor Kolhe

The 3D Facemask Recognition: Minimization for Spreading COVID-19 and Enhance Security 619
Ashish Sharma, Ara Miran, and Zanyar Rzgar Ahmed

ICT Enabled Cloud Cafeteria of Corporate Companies with a Customized App for Employee's Expediency 639
H. M. Moyeenudin, S. Chandrachud, and A. Mohammed Faisal

Influence of Probing Action Costs on Adversarial Decision-Making in a Deception Game 649
Harsh Katakwar, Palvi Aggarwal, Zahid Maqbool, and Varun Dutt

Impact of Digital Wellbeing in Intelligent Knowledge Management Systems 659
Sapna Jain and M. Afshar Alam

Social Media Community Using Optimized Clustering Algorithm 669
Muskan Pandey, Om Avhad, Ankita Khedekar, Aarya Lamkhade, and Minakshi Vharkate

Optimal Allocation of Distributed Generation in Order to Improve the Performance of Power System Networks 677
R. B. Singh, R. P. Payasi, and K. S. Verma

E-Aid: Open Wound Identifier and Analyzer Using Smartphone Through Captured Image 691
Joie Ann W. Maghanoy, Daryl G. Guzman, Joan Stephen D. Paz, Dale R. Policarpio, Ansley D. Yanga, and Shaneth Ambat

Intelligently Trained Elman Neural Network-Based MPPT for Photovoltaic Systems 699
Sangita Bapu Patil and L. M. Waghmare

Automatic HTML Code Generation Using Image Processing 709
Shreya Khandekar, Shraddha Korade, Rutuja Kulkarni, Tejashree Pathak, and Satish Kamble

A Detailed Review on Text Extraction Using Optical Character Recognition 719
Chhanam Thorat, Aishwarya Bhat, Padmaja Sawant, Isha Bartakke, and Swati Shirsath

Cyber Threats Landscape Overview Under the New Normal 729
Indraneel Mukhopadhyay

Vulnerability Analysis of Bluetooth Technology for Defensive Application 737
Swapnil Sutar, Kishore Malladi, Priyanka Mekala, and Supriya Goel

A Recommendation System to Support the Student to Choose a Role in the College Election 747
Gayatri Bedse, Divya Ghorpade, Tejashri Gangurde, Shreya Kulkarni, and Swati Shirsath

Finite Element Method-Based Artificial Neural Network 755
Harshini Pothina and K. V. Nagaraja

An Ellipse Slotted Vivaldi Antenna for 5G Applications 769
Akshta Jagdale, H. Sairaam, Harshita Kulkarni, Lakshmi Suresh Nair, and Sanjeev Kumar

Impact of Data Mining on HCC Prediction: Survey 777
Babitha Thamby and S. Sheeja

Implementation of UVM Agents for Hexagon Subsystem RTL 785
Keerti Umesh Sankangoudar, K. Sowmya Nag, and Anshul Sharma

Hybrid Intrusion Detection System for Detecting DDoS Attacks on Web Applications Using Machine Learning 797
Madhura Shekhar Potnis, Sanjyot Kedar Sathe, Purva Govind Tugaonkar, Gayatri Laxmikant Kulkarni, and Shilpa Shrikant Deshpande

Geospatial Technology and Analytical Hierarchy Process (AHP)-Based Discrimination of Groundwater Potential Zones in Vijayawada–Mangalagiri Region, Andhra Pradesh 807
Koduganti Sai Sudha Manasa and P. Geetha

IoT Application for Spruce Fire Detection in Rwanda 823
Eric Hitimana, Gaurav Bajpai, Richard Musabe, Louis Sibomana, and Jayavel Kayalvizhi

Achieving Sustainable Village Development Through Geo-information Application 833
Sonal Mobar Roy, N. S. R. Prasad, and B. Srinuvas

An Analytical Overview of the State-Wise Impact of COVID-19 in India 845
Rupal Lohani, Vidya Suresh, Eric George Varghese, and S. Thara

An Analysis of FIPP Clauses with Respect to Data Lifecycle Phases and Privacy Properties 855
Asmita Manna, Anirban Sengupta, and Chandan Mazumdar

Mobile Deployed Measurement of RF Man-Made Noise Making Use of RTL-SDR 867
Lee McQuire, Mohamed Tariq Kahn, and Vipin Balyan

Use of Blockchain Technology in Agriculture Domain 877
Nisha N. Kamble, Shankar M. Mali, and C. H. Patil

Analysis of Impedance Matching Technique on Broadband Powerline Communication Network Topologies 885
D. Smitha Gayathri and K. R. Usha Rani

Automated People Monitoring System Using OpenCV and Raspberry Pi 905
Dipankan Bandopadhyay, Vinod Jha, Atri Bandyopadhyay, Pratik Roy, Rupesh Halder, and Swagatam Majhi

Sign Language Recognition Using Convolutional Neural Network 915
Ayush Kumar, Sumeet Kumar, Shivam Singh, and Vinod Jha

Covid Waste Management Using IoT: A Smart Framework 923
Mitra Tithi Dey and Punyasha Chatterjee

Phishing URL Detection and Vulnerability Assessment of Web Applications Using IVS Attributes with XAI 933
Vivek John Sudhakar, Srimathi Mahalingam, Vaman Venkatesh, and V. Vetriselvi

A Smart Device for Power Theft Detection 945
A. Jagadeesh, S. Praneeth Varma, A. Sreeja, and I. Mamatha

Correction to: The 3D Facemask Recognition: Minimization for Spreading COVID-19 and Enhance Security C1
Ashish Sharma, Ara Miran, and Zanyar Rzgar Ahmed

Author Index 955

Editors and Contributors

About the Editors

Simon Fong graduated from La Trobe University, Australia, B.Eng. Computer Systems degree, and a Ph.D. Computer Science degree in 1993 and 1998, respectively. Simon is now working as Associate Professor at the University of Macau, China. Prior to his academic career, Simon held various managerial and technical positions, such as Systems Engineer, IT Consultant, and E-Commerce Director in Australia and Asia. Dr. Fong has published over 300 international conference and peer-reviewed journal papers, mostly in the areas of data mining and optimization algorithms.

Nilanjan Dey is an Associate Professor in the Department of Computer Science and Engineering, JIS University, Kolkata, India. He has authored/edited more than 75 books with Springer, Elsevier, Wiley and CRC Press and published more than 300 peer-reviewed research papers. Dr. Dey is Editor-in-Chief of the *International Journal of Ambient Computing and Intelligence*; Series Co-Editor of *Springer Tracts in Nature-Inspired Computing* (STNIC); and Series Co-Editor of *Advances in Ubiquitous Sensing Applications for Healthcare*, Elsevier.

Amit Joshi is currently Director of Global Knowledge Research Foundation, also Entrepreneur & Researcher who has completed his Masters and research in the areas of cloud computing and cryptography in medical imaging. Dr. Joshi has an experience of around 10 years in academic and industry in prestigious organizations. Dr. Joshi is active Member of ACM, IEEE, CSI, AMIE, IACSIT, Singapore, IDES, ACEEE, NPA, and many other professional societies. Currently, Dr. Joshi is International Chair of InterYIT at International Federation of Information Processing (IFIP, Austria). He has presented and published more than 50 papers in national and international journals/conferences of IEEE and ACM. Dr. Joshi has also edited more than 40 books which are published by Springer, ACM, and other reputed publishers. Dr. Joshi has also organized more than 50 national and international conferences

and programs in association with ACM, Springer, and IEEE to name a few across different countries including India, UK, Europe, USA, Canada, Thailand, Egypt, and many more.

Contributors

Zunaid Aalam SGT University, Gurugram, Haryana, India

Parul Agarwal Department of Computer Science and Engineering, Jamia Hamdard University, New Delhi, India

Palvi Aggarwal Dynamic Decision-Making Laboratory, Carnegie Mellon University, Pittsburgh, USA

Zanyar Rzgar Ahmed Department of Information Technology, Lebanese French University, Erbil, Kurdistan, Iraq;
College of Engineering and Computer Science, Lebanese French University, Erbil, Kurdistan, Iraq

Padmanabha Aital MPSTME, NMIMS University, Mumbai, India

M. Akshara Department of Computer Science and Engineering, Raja Reddy Institute of Technology, Bangalore, Karnataka, India

M. Afshar Alam Jamia Hamdard, New Delhi, India

Tanvir Alam Shahjalal University of Science and Technology, Sylhet, Bangladesh

Hala S. Ali Jawaharlal Nehru Technological University, Hyderabad, India

Muhammad Naveed Aman School of Computing, National University of Singapore, Singapore, Singapore

Shaneth Ambat FEU Institute of Technology, Sampaloc Metro Manila, Philippines

Sumalatha Aradhya Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumakuru, India

Pallavi Arora IK Gujral Punjab Technical University, Kapurthala, India

Eduardus Hardika Sandy Atmaja St. Francis Institute of Technology, Mumbai, India;
Sanata Dharma University, Yogyakarta, Indonesia

Om Avhad MIT Academy of Engineering, Pune, India

Gaurav Bajpai Department of Computer and Software Engineering, University of Rwanda, Huye, Rwanda

Rishabh Bajpai Birla Institute of Technology and Science, Pilani, K.K. Birla Goa Campus, Goa, India

Vipin Balyan Department of Electrical, Electronics and Computer Engineering, Cape Peninsula University of Technology, Cape Town, South Africa

Dipankan Bandopadhyay School of Electronics Engineering, KIIT Deemed to be University, Bhubaneswar, India

Atri Bandyopadhyay School of Electronics Engineering, KIIT Deemed to be University, Bhubaneswar, India

Isha Bartakke MKSSS's Cummins College of Engineering for Women, Pune, India

Gayatri Bedse MKSSS's Cummins College of Engineering for Women, Pune, India

Aishwarya Bhat MKSSS's Cummins College of Engineering for Women, Pune, India

Gresha Bhatia Computer Engineering, Vivekanand Education Society's Institute of Technology, Mumbai, India

Kaushal Bhavsar GLS University, Ahmedabad, Gujarat, India

Partho Sharothi Biswas Department of Computer Science and Engineering, Raja Reddy Institute of Technology, Bangalore, Karnataka, India

Hasnain Bokhari University of Erfurt, Erfurt, Germany

Sushma Bylaiah Department of Computer Science and Engineering, M S Ramaiah Institute of Technology, Bengaluru, Karnataka, India

Veena S. Chakravarthi BNM Institute Technology, Bangalore, India

Yug Chandak Marwadi University, Gauridad, Rajkot, Gujarat, India

S. Chandrachud Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai, India

Punyasha Chatterjee School of Mobile Computing and Communication, Jadavpur University, Kolkata, India

Shehzad Ashraf Chaudhry Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey

Sarat Kr. Chettri Department of Computer Applications, Assam Don Bosco University, Guwahati, India

Chingmuankim Delhi Technological University, New Delhi, India

Kshitija Choudhari MKSSS's Cummins College of Engineering for Women, Pune, India

Jordan D'souza Don Bosco Institute of Technology, Mumbai, India

R. Dakshayani Department of Computer Engineering, Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai, India

Rakesh Dani Graphic Era Deemed to be University, Dehradun, India

Dipankar Debnath Department of Computer Science, St. Mary's College, Shillong, Meghalaya, India

Shilpa Shrikant Deshpande Department of Computer Engineering, Cummins College of Engineering for Women, Pune, India

M. Nirmala Devi Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

Mitra Tithi Dey Netaji Nagar Day College, Kolkata, India

M. K. Dhananjaya Department of Computer Science and Engineering, Raja Reddy Institute of Technology, Bangalore, Karnataka, India

I. Divya Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh, India

S. Divya TKM College of Engineering, APJ Abdul Kalam Technological University, Kollam, India

Himanshu Dutt Visiting Faculty, Jamia Millia Islamia (Central University), New Delhi, India

Varun Dutt Applied Cognitive Science Laboratory, Indian Institute of Technology Mandi, Mandi, India

Ajoy Krishna Dutta Department of Computer Science, St. Mary's College, Shillong, Meghalaya, India

Rajendra Kumar Dwivedi Department of IT and CA, MMMUT, Gorakhpur, Uttar Pradesh, India

Nida Fatima Department of Computer Science and Engineering, Jamia Hamdard University, New Delhi, India

Salil Fernandes Don Bosco Institute of Technology, Mumbai, India

Tejashri Gangurde MKSSS's Cummins College of Engineering for Women, Pune, India

Mayuresh Gawai School of Computer Engineering and Technology, MIT Academy of Engineering, Pune, India

D. Smitha Gayathri ECE Department, DonBosco Institute of Technology, Bengaluru, India

P. Geetha Center for Excellence in Computational Engineering and Networking (CEN), Amrita Vishwa Vidyapeetham, Coimbatore, India

Neha Gehlot SGT University, Gurugram, Haryana, India

Divya Ghorpade MKSSS's Cummins College of Engineering for Women, Pune, India

T. Gireesh Kumar Department of Computer Science and Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

Lavika Goel Department of Computer Science and Engineering, Malaviya National Institute of Technology, Jaipur, India

Mridula Goel Birla Institute of Technology and Science, Pilani, K.K. Birla Goa Campus, Goa, India

Supriya Goel C. R. Rao AIMSCS, Hyderabad Central University, Serilingampalle (m), Telangana, India

Yogesh Golhar Department of Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India

Elroy Gomes Department of Computer Engineering, Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai, India

Tryambak Gour Department of Computer Engineering, Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai, India

Prasad Govekar Computer Engineering, Vivekanand Education Society's Institute of Technology, Mumbai, India

Leena Gowda Department of Veterinary Public Health and Epidemiology, Veterinary College, Bengaluru, Karnataka, India

Aman Gupta Marwadi University, Gauridad, Rajkot, Gujarat, India

Daryl G. Guzman FEU Institute of Technology, Sampaloc Metro Manila, Philippines

Aparna Hajare MKSSS's Cummins College of Engineering for Women, Pune, India

Rupesh Halder School of Electronics Engineering, KIIT Deemed to be University, Bhubaneswar, India

Eric Hitimana African Center of Excellence in the Internet of Things, University of Rwanda, Huye, Rwanda

Dung Luu Hong Military Technical Academy, Hanoi, Vietnam

Bisma Iftekhar Willy Brandt School of Public Policy, University of Erfurt, Erfurt, Germany

Uma Bharathi Indrabalan Spatial Epidemiology Laboratory, Indian Council of Agricultural Research (ICAR)—National Institute of Veterinary Epidemiology and Disease Informatics (NIVEDI), Bengaluru, Karnataka, India

Bharat T. Jadhav Yashvantrao Chavan Institute of Science, Satara, India

Dipti Jadhav Don Bosco Institute of Technology, Mumbai, India

A. Jagadeesh Department of Electrical and Electronics Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Bengaluru, India

Akshta Jagdale Department of Electronics and Telecommunications, Symbiosis International (Deemed) University, Pune, Maharashtra, India

Prakhyath Jain Department of CSE, CMR Institute of Technology, Bengaluru, India

Sapna Jain Jamia Hamdard, New Delhi, India

Srinivas Jangirala Jindal Global Business School, O. P. Jindal Global University, Haryana, India

Shubham Jante Optimum Data Analytics, Pune, India

Pratyush Jha Marwadi University, Gauridad, Rajkot, Gujarat, India

Vinod Jha School of Electronics Engineering, KIIT Deemed to be University, Bhubaneswar, India

Rajni Jindal Delhi Technological University, New Delhi, India

Ansamma John TKM College of Engineering, Kollam, India

Fredin Jose Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

Mohamed Tariq Kahn Department of Electrical, Electronics and Computer Engineering, Cape Peninsula University of Technology, Cape Town, South Africa

Sudharm Kalamdani Pimpri Chinchwad College of Engineering, Pune, India

Nisha N. Kamble Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

Satish Kamble Pune Vidyarthi Griha's College of Engineering and Technology, Pune, India

Meetu Kandpal L.J. Institute of Computer Applications, L J University, Ahmedabad, Gujarat, India

Jitaksh Kapoor School of Computing, Indian Institute of Information Technology Una, Himachal Pradesh, India

S. Karthika Department of Information Technology, SSN College of Engineering, Chennai, Tamil Nadu, India

Harsh Katakwar Applied Cognitive Science Laboratory, Indian Institute of Technology Mandi, Mandi, India

Anthony Kattikaren Don Bosco Institute of Technology, Mumbai, India

Amritpal kaur SGT University, Gurugram, Haryana, India

Baljeet Kaur Guru Nanak Dev Engineering College, Ludhiana, India

Satnam kaur SGT University, Gurugram, Haryana, India

Jayavel Kayalvizhi Department of Information Technology, SRM Institute of Science and Technology, Chennai, India

Sridharan Kesavan Symbiosis Centre for Research and Innovation, Pune, India

Hitendra Khairnar Cummins College of Engineering for Women, Pune, India

Shreya Khandekar Pune Vidyarthi Griha's College of Engineering and Technology, Pune, India

Ankita Khedekar MIT Academy of Engineering, Pune, India

Vijayshri Khedkar Symbiosis International (Deemed University), Symbiosis Institute of Technology, Pune, India

Kishor Kolhe School of Computer Science and Technology, Dr. Vishwanath Karad MIT World Peace University, Pune, India

Rahul Koli Computer Engineering, Vivekanand Education Society's Institute of Technology, Mumbai, India

Shraddha Korade Pune Vidyarthi Griha's College of Engineering and Technology, Pune, India

S. Kowshik Hurshan TIFAC-CORE in Cyber Security, Coimbatore, India

Manali Kshirsagar Yeshwantrao Chavan College of Engineering (YCCE), Nagpur, Nagpur, India

Gauri Kudalkar Cummins College of Engineering for Women, Pune, India

Gayatri Laxmikant Kulkarni Department of Computer Engineering, Cummins College of Engineering for Women, Pune, India

Harshita Kulkarni Department of Electronics and Telecommunications, Symbiosis International (Deemed) University, Pune, Maharashtra, India

Rutuja Kulkarni Pune Vidyarthi Griha's College of Engineering and Technology, Pune, India

Shreya Kulkarni MKSSS's Cummins College of Engineering for Women, Pune, India

Ayush Kumar School of Electronics Engineering, KIIT Deemed to be University, Bhubaneswar, India

Darshita Kumar MKSSS's Cummins College of Engineering for Women, Pune, India

Gourav Kumar Department of Computer Application, Kongu Engineering College, Erode, TamilNadu, India

Sanjeev Kumar Department of Electronics and Telecommunications, Symbiosis International (Deemed) University, Pune, Maharashtra, India

Sumeet Kumar School of Electronics Engineering, KIIT Deemed to be University, Bhubaneswar, India

Reni Diah Kusumawati Gunadarma University, Jakarta, Indonesia

Aarya Lamkhade MIT Academy of Engineering, Pune, India

Rupal Lohani Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Sahil Lotya Computer Engineering, Vivekanand Education Society's Institute of Technology, Mumbai, India

Armand Christopher Luna FEU Institute of Technology, Manila, Philippines

Joie Ann W. Maghanoy FEU Institute of Technology, Sampaloc Metro Manila, Philippines

Abraham Magpantay FEU Institute of Technology, Manila, Philippines

Srimathi Mahalingam College of Engineering Guindy, Anna University, Chennai, India

Swagatam Majhi School of Electronics Engineering, KIIT Deemed to be University, Bhubaneswar, India

Shankar M. Mali Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

Kishore Malladi C. R. Rao AIMSCS, Hyderabad Central University, Serilingampalle (m), Telangana, India

I. Mamatha Department of Electrical and Electronics Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Bengaluru, India

Koduganti Sai Sudha Manasa Center for Wireless Networks and Applications (WNA), Amrita Vishwa Vidyapeetham, Amritapuri, India

Asmita Manna Pimpri Chinchwad College of Engineering, Pune, India

Zahid Maqbool Applied Cognitive Science Laboratory, Indian Institute of Technology Mandi, Mandi, India

Chandan Mazumdar Jadavpur University, Jadavpur, Kolkata, India

Lee McQuire Department of Electrical, Electronics and Computer Engineering, Cape Peninsula University of Technology, Cape Town, South Africa

Nishchay Mehta Birla Institute of Technology and Science, Pilani, K.K. Birla Goa Campus, Goa, India

Priyanka Mekala C. R. Rao AIMSCS, Hyderabad Central University, Serilingampalle (m), Telangana, India

T. Milton Tourism and Hospitality Management, Bharath Institute of Higher Education and Research, Chennai, India

Ara Miran Department of Computer Networking, Lebanese French University, Erbil, Kurdistan, Iraq;
College of Engineering and Computer Science, Lebanese French University, Erbil, Kurdistan, Iraq

A. Mohammed Faisal Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai, India

Nitin S. More Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Greenfields, Vaddeswaram, Guntur, Andhra Pradesh, India

Sharmila S. More MATS School of IT, Raipur, India

H. M. Moyeenudin School of Hotel and Catering Management, Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai, India

Tabish Mufti Department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India

Indraneel Mukhopadhyay Institute of Engineering & Management, Kolkata, India

Keka Mukhopadhyaya CMR Institute of Technology, Bengaluru, India

Richard Musabe Department of Computer and Software Engineering, University of Rwanda, Huye, Rwanda

Abhishek Muttath School of Computer Engineering and Technology, MIT Academy of Engineering, Pune, India

K. Sowmya Nag Department of ECE, R V College of Engineering, Bengaluru, India

K. V. Nagaraja Department of Mathematics, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Bengaluru, India

Lakshmi Suresh Nair Department of Electronics and Telecommunications, Symbiosis International (Deemed) University, Pune, Maharashtra, India

Bhawna Narain MATS School of IT, Raipur, India

R. Navaneethakrishnan Kumaraguru College of Technology, Coimbatore, Tamilnadu, India

S. Naveen Department of Information Technology, SSN College of Engineering, Chennai, Tamil Nadu, India

Ahmed J. Obaid University of Kufa, Najaf, Iraq

Teddy Oswari Gunadarma University, Jakarta, Indonesia

Sanjeeb Pal Amity School of Hospitality, Amity University, Rajasthan, Jaipur, India

Bhavna Pandey Amity University, Mumbai, India

Muskan Pandey School of Computer Engineering and Technology, MIT Academy of Engineering, Pune, India

Shambhavi Pandey MKSSS's Cummins College of Engineering for Women, Pune, India

Satyen M. Parikh Faculty of Computer Applications, Ganpat University, Kherva, Gujarat, India

Sashikala Parimi IBS, IFHE, Hyderabad, India

Nicole John Pascua FEU Institute of Technology, Manila, Philippines

Hiral R. Patel Faculty of Computer Applications, Ganpat University, Kherva, Gujarat, India

Pooja Patel MKSSS's Cummins College of Engineering for Women, Pune, India

Sina Patel Symbiosis International (Deemed University), Symbiosis Institute of Technology, Pune, India

Tejashree Pathak Pune Vidyarthi Griha's College of Engineering and Technology, Pune, India

C. H. Patil Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

Rajesh Patil Larsen and Tubro, Mumbai, India

Sangita Bapu Patil Department of Electrical Engineering, G. H. Raisoni Institute of Engineering & Technology, Pune, MS, India

Shankargoud Patil S.G. Balekundri Institute of Technology, Belagavi, Karnataka, India

Sharanagouda S. Patil Virology Laboratory, Indian Council of Agricultural Research (ICAR)—National Institute of Veterinary Epidemiology and Disease Informatics (NIVEDI), Bengaluru, Karnataka, India

Bonani Paul Department of Computer Science, St. Mary's College, Shillong, India

Shruti Pawar Cummins College of Engineering for Women, Pune, India

R. P. Payasi Kamla Nehru Institute of Technology, Sultanpur, Uttar Pradesh, India

Joan Stephen D. Paz FEU Institute of Technology, Sampaloc Metro Manila, Philippines

Mayank Phadke Birla Institute of Technology and Science, Pilani, K.K. Birla Goa Campus, Goa, India

Dale R. Policarpio FEU Institute of Technology, Sampaloc Metro Manila, Philippines

Harshini Pothina Department of Electronics and Instrumentation Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Bengaluru, India

Madhura Shekhar Potnis Department of Computer Engineering, Cummins College of Engineering for Women, Pune, India

Kappargaon S. Prabhushetty Veerappa Nisty Engineering College, Yadgir, India

Shelly Prakash Banasthali Vidyapith, Tonk, Rajasthan, India

N. S. R. Prasad National Institute of Rural Development and Panchayati Raj, Hyderabad, India

M. Prateek Department of CSE, CMR Institute of Technology, Bengaluru, India

M. Priyatharishini Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

Md Forhad Rabbi Shahjalal University of Science and Technology, Sylhet, Bangladesh

Shubham Raj BNM Institute Technology, Bangalore, India

P. K. Rajani Pimpri Chinchwad College of Engineering, Pune, India

R. Rameshkumar Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India

K. R. Usha Rani ECE Department, RVCE, Bengaluru, India

V. Ranjith Department of Computer Science and Engineering, Raja Reddy Institute of Technology, Bangalore, Karnataka, India

Rohit Raut Pimpri Chinchwad College of Engineering, Pune, India

Yashwant Singh Rawal Amity School of Hospitality, Amity University, Rajasthan, Jaipur, India

S. Sai Satyanarayana Reddy Sreyas Institute of Engineering and Technology, Hyderabad, India

S. Ribu Hassini TIFAC-CORE in Cyber Security, Coimbatore, India

Pratik Roy School of Electronics Engineering, KIIT Deemed to be University, Bhubaneswar, India

Sonal Mobar Roy National Institute of Rural Development and Panchayati Raj, Hyderabad, India

Deshna Sachan C-DAC, Noida, India

Karan Sachdev Computer Engineering, Vivekanand Education Society's Institute of Technology, Mumbai, India

Samapty Saha Shahjalal University of Science and Technology, Sylhet, Bangladesh

P. Yamini Sahukar Department of Computer Science and Engineering, Raja Reddy Institute of Technology, Bangalore, Karnataka, India

H. Sairaam Department of Electronics and Telecommunications, Symbiosis International (Deemed) University, Pune, Maharashtra, India

Keerti Umesh Sankangoudar Department of ECE, R V College of Engineering, Bengaluru, India

Kriti Saroha C-DAC, Noida, India

Sanjyot Kedar Sathe Department of Computer Engineering, Cummins College of Engineering for Women, Pune, India

Padmaja Sawant MKSSS's Cummins College of Engineering for Women, Pune, India

Anirban Sengupta Jadavpur University, Jadavpur, Kolkata, India

Krishna Shah School of Computer Science and Technology, Dr. Vishwanath Karad MIT World Peace University, Pune, India

Saima Shahab Department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India

M. B. Shanthi Department of CSE, CMR Institute of Technology, Bengaluru, India

Anshul Sharma DSP, Qualcomm India Pvt. Ltd, Bengaluru, India

Ashish Sharma Department of Information Technology, Lebanese French University, Erbil, Kurdistan, Iraq;
College of Engineering and Computer Science, Lebanese French University, Erbil, Kurdistan, Iraq

Sunil Sharma Faculty of Engineering, Pacific University, Rajasthan, Udaipur, India

Seema Shedole Department of Computer Science and Engineering, M S Ramaiah Institute of Technology, Bengaluru, Karnataka, India

S. Sheeja Karpagam Academy of Higher Education, Coimbatore, India

Pooja Shinde Cummins College of Engineering for Women, Pune, India

Swati Shirsath MKSSS's Cummins College of Engineering for Women, Pune, India

Louis Sibomana National Council for Science and Technology, Rwanda Government, Kigali, Rwanda

Arindam Singh Department of IT and CA, MMMUT, Gorakhpur, Uttar Pradesh, India

Mayank Singh Department of Information Technology, SSN College of Engineering, Chennai, Tamil Nadu, India

Prerna Singh Universal Business School, Bangalore, India

R. B. Singh Goverment Polytechnic, Kenura Sultanpur, Uttar Pradesh, India

Sheenu Singh L.J. Institute of Computer Applications, L J University, Ahmedabad, Gujarat, India

Shivam Singh School of Electronics Engineering, KIIT Deemed to be University, Bhubaneswar, India

Arushi Sinha Department of Computer Engineering, Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai, India

John Paul So FEU Institute of Technology, Manila, Philippines

Shahab Saquib Sohail Department of Computer Science and Engineering, Jamia Hamdard University, New Delhi, India

Kavita Sonawane St. Francis Institute of Technology, Mumbai, India

Madasamy Sornam University of Madras, Chennai, India

K. Sowmya Department of Information Technology, SSN College of Engineering, Chennai, Tamil Nadu, India

S. Sowndarya BNM Institute Technology, Bangalore, India

A. Sreeja Department of Electrical and Electronics Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Bengaluru, India

R. Sridevi Jawaharlal Nehru Technological University, Hyderabad, India

S. Srinidhi Department of Information Technology, SSN College of Engineering, Chennai, Tamil Nadu, India

B. Srinuvas National Institute of Rural Development and Panchayati Raj, Hyderabad, India

Rashmi Srivastava Department of IT & CA MMMUT, Uttar Pradesh, Gorakhpur, India

Shashi Kant Srivastava Indian Institute of Management-Sirmaur, Paonta Sahib, Himachal Pradesh, India

Vivek John Sudhakar College of Engineering Guindy, Anna University, Chennai, India

Kuralayanapalya Puttahonnappa Suresh Spatial Epidemiology Laboratory, Indian Council of Agricultural Research (ICAR)—National Institute of Veterinary Epidemiology and Disease Informatics (NIVEDI), Bengaluru, Karnataka, India

L. Padma Suresh Baselios Mathew II College of Engineering, Sasthamkotta, India

Vidya Suresh Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Swapnil Sutar C. R. Rao AIMSCS, Hyderabad Central University, Serilingampalle (m), Telangana, India

Amit B. Suthar Faculty of Computer Applications, Ganpat University, Kherva, Gujarat, India

J. N. Swaminathan QIS College of Engineering & Technology, Ongole, Andhra Pradesh, India

A. Tamilarasi Department of Computer Application, Kongu Engineering College, Erode, TamilNadu, India

V. Tanuja Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumakuru, India

Jarin Tasnim Shahjalal University of Science and Technology, Sylhet, Bangladesh

Marcio Andrey Teixeira Federal Institute of Education, Science, and Technology of São Paulo, Catanduva, SP, Brazil

Divyansh Thakur School of Computing, Indian Institute of Information Technology Una, Himachal Pradesh, India

Babitha Thamby Karpagam Academy of Higher Education, Coimbatore, India

S. Thara Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Chhanam Thorat MKSSS's Cummins College of Engineering for Women, Pune, India

Sonali Kothari Tidke Symbiosis International (Deemed University), Symbiosis Institute of Technology, Pune, India

Harshita Tiwari Cummins College of Engineering for Women, Pune, India

Vaibhav Tiwari Pimpri Chinchwad College of Engineering, Pune, India

Christian Trajano FEU Institute of Technology, Manila, Philippines

Bhushan Trivedi GLS University, Ahmedabad, Gujarat, India

Purva Govind Tugaonkar Department of Computer Engineering, Cummins College of Engineering for Women, Pune, India

Aakansha Uppal Symbiosis Centre for Management Studies, Noida, India

Hoa Doan Van Academy of Military Science and Technology, Hanoi, Vietnam

Ram Vankadara Atmospheric Science Department, Koneru Lakshmaiah Education Foundation, Greenfields, Vaddeswaram, Guntur, Andhra Pradesh, India

Eric George Varghese Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

S. Praneeth Varma Department of Electrical and Electronics Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Bengaluru, India

Swamiraj Nithiyanantha Vasagam University of Madras, Chennai, India; CSIR-Central Leather Research Institute, Chennai, India

Prashant Vats Fairfield Institute of Management and Technology, GGSIPU, New Delhi, India

Aditya Veer School of Computer Engineering and Technology, MIT Academy of Engineering, Pune, India

Vaman Venkatesh College of Engineering Guindy, Anna University, Chennai, India

Deepika Chandra Verma Jindal Global Business School, O. P. Jindal Global University, Haryana, India

K. S. Verma Kamla Nehru Institute of Technology, Sultanpur, Uttar Pradesh, India

V. Vetriselvi College of Engineering Guindy, Anna University, Chennai, India

Minakshi Vharkate MIT Academy of Engineering, Pune, India

I. Vidyasagar Rise Krishna Sai Gandhi Group of Institutions, Ongole, Andhra Pradesh, India

Vaibhav Vyas Banasthali Vidyapith, Tonk, Rajasthan, India

L. M. Waghmare Swami Ramanand Teerth Marathwada University, Vishnupuri, Nanded, MS, India

Vaishal Wangikar School of Computer Engineering and Technology, MIT Academy of Engineering, Pune, India

Van Luu Xuan People's Security Academy, Hanoi, Vietnam

Janardan Krishna Yadav Jindal Global Business School, O. P. Jindal Global University, Haryana, India

Ansley D. Yanga FEU Institute of Technology, Sampaloc Metro Manila, Philippines

Tristyanti Yusnitasari Gunadarma University, Jakarta, Indonesia

Analysis of Codon Usage Bias in *Cya, Lef,* and *Pag* Genes Exists in px01 Plasmid of *Bacillus Anthracis*

Sushma Bylaiah, Seema Shedole, Kuralayanapalya Puttahonnappa Suresh, Leena Gowda, Sharanagouda S. Patil, and Uma Bharathi Indrabalan

Abstract Anthrax is an antiquated and most serious disease that influences a wide scope of creature species and is brought about by bacterium *Bacillus anthracis*, which is a spore-framing bacterium. Harmful types of *Bacillus anthracis* have two enormous pathogenicity associated plasmids pXO1 and pXO2. pXO1 has the distinctive *Bacillus anthracis* poison qualities *pagA, lef,* and *cya,* whereas pXO2 has the qualities liable for capsule synthesis and degradation. *B. anthracis* express its pathogenic movement generally over the case and the creation of a poisonous compound including three proteins identified as defensive antigen (namely PA), deadly factor (namely LF), and edema factor (namely EF). These two enormous plasmids of *Bacillus anthracis* are fundamental for full pathogenicity, rejection of both of the plasmids very debilitates the harmfulness of *B. anthracis*. In the current assessment, we coordinated the investigation of the codon usage bias of destructive qualities stay alive in pXO1 plasmid of *Bacillus anthracis*. Codon usage bias assumes a significant part at the degree of quality articulation. Codon usage pattern of *Bacillus anthracis* is significant for understanding the transformative qualities in the species. To research codon usage pattern of the *Bacillus anthracis* genome, nucleotide arrangements of the virulent genes viz *cya, lef,* and *pag* were gathered from National Center for Biotechnology Information (NCBI). The phylogenetic investigation is done using MEGA X and Figtree. The RSCU of the selected genes were

S. Bylaiah (✉) · S. Shedole
Department of Computer Science and Engineering, M S Ramaiah Institute of Technology, Matthikere, Bengaluru, Karnataka, India

K. P. Suresh · U. B. Indrabalan
Spatial Epidemiology Laboratory, Indian Council of Agricultural Research (ICAR)—National Institute of Veterinary Epidemiology and Disease Informatics (NIVEDI), Yelahanka, Bengaluru, Karnataka, India

L. Gowda
Department of Veterinary Public Health and Epidemiology, Veterinary College, Hebbal, Bengaluru, Karnataka, India

S. S. Patil
Virology Laboratory, Indian Council of Agricultural Research (ICAR)—National Institute of Veterinary Epidemiology and Disease Informatics (NIVEDI), Yelahanka, Bengaluru, Karnataka, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_1

determined and these outcomes designated that codon usage bias exists in the virulent genes remains alive in pXO1 plasmid of *Bacillus anthracis* genome. These outcomes could be used for additional investigation on the transformative examination of the genome.

Keywords Anthrax · *Bacillus anthracis* · Codon usage bias · DNA sequences · px01 plasmid

1 Introduction

Anthrax is a zoonotic infectious disease, influences animals and human beings. It is brought about by *Bacillus anthracis*, non-motile, a gram-positive, pole molded, spore-shaping bacteria, which structure the spores that can keep on persevering in the climate for quite a long while. B. anthracis invests the greater part of its life energy in the earth as a dormant bacterium, while waiting for the appropriate ecological conditions and permitting it to affect a regenerative cycle [1]. Harmfulness of the utmost *Bacillus anthracis* strains is joined by 2 enormous px01and px02 plasmids; strains that are missing either of the plasmids are either a destructive or else altogether debilitated. *Bacillus anthracis* covers three monomeric, plasmid-encoded proteins on the whole called as *Bacillus anthracis* toxin [2]. px01 plasmid is significant for the union of the *Bacillus anthracis* proteins that are toxic, basically lethal factor, edema factor, and protective antigen. All these toxic proteins work in gathering of 2 toward yielding the two *Bacillus anthracis* toxin substances, lethal toxin substance (gathering of protective_antigen and lethal_factor) and edema toxin substance (get together of protective_antigen and edema_factor). Plasmid px02 conveys qualities vital for creation of Poly-D_glutamic_acid capsule. Independent of the significant jobs of px01and px02 in *Bacillus anthracis* destructiveness, scarcely any plasmid-encoded qualities are recognized as well as depicted [3, 4]. Plasmid px02 conveys three unique qualities critical for the capsule_synthesis (capC, capB, and capA), capsule_degradation (dep), as well as a transacting controlling gene called acpA. Plasmid px01gives space to the underlying qualities of the *Bacillus anthracis* toxin proteins, for example, lef (the lethal_factor), cya (the edema_factor), and pagA (the protective_antigen) prompts intense edema and cell demise [5, 6].

The genetic_code referred as the group of guidelines that will characterize likeness among the nucleotide trios known as codons in deoxyribo nucleic acid and amino_acids in the proteins. One of the major principal attributes in cypher is to decline, implying that various equivalent codons specify a similar amino acid [7]. The differentiations in the recurrence of event of equivalent codons in coding DNA are known as codon_usage_bias [8]. Codon_usage_bias varies from genome to genome, inside genomes, and from gene to gene. The inclination is generally prominent in particular sorts of qualities, by and large in exceptionally communicated qualities [9]. The hereditary code in messenger RNA is superfluous with 61 codons changed over into twenty distinctive amino_acids. Separate amino_acids are binded by maximum

number of six unique codons; however, interior to the codon families, few are utilized more much of the time than others. The unicellular creatures, for example, microorganisms, have a most supreme codon usage bias and the level of predisposition veers among qualities inside a similar genome [10]. Codon usage bias is brought about by variety in two essential elements (1) mutation pressure, which causes codon diversity, and (2) selection pressure against suboptimal codons, which diminishes codon diversity [11]. Various measures are created to evaluate the codon usage viz enc, rscu, etc. enc does not rely upon life form explicit information and is effectively applied to the investigation of new organic entities [12]. Difference of codon optimization among qualities gives differential proficiency just as precision in the interpretation of qualities. The investigation of codon bias is acquiring consideration with the inception of entire genome sequencing of different creatures. Atomic developmental examinations propose that the codon usage bias differs equally inside and among the genomes and may consume huge significance to comprehend the genome advancement among correlated species [13]. Further, investigation of codon_usage_bias is significant to understand atomic science, hereditary qualities, and genome development; it likewise helps in new quality disclosure, plan of groundworks, plan of transgenes, decide of root of species, and expectation of quality articulation level and quality capacity. In this manner, the investigation on codon usage bias helps with acquiring in depth information on transformations that prompts developmental changes and comprehend the adjustments in the bacterial variations. The aim of our study was to portray our discoveries on the general commitments of change and regular choice to the variety in codon bias among the *Bacillus anthracis* genes of px01plasmid (cya, lef, and pag).

2 Materials and Methods

2.1 Sequence_Data_Retrieval

Entire nucleotide sequences of cya (43 sequences), lef (93 sequences) and pag (66 sequences) genes of *Bacillus anthracis* genome were accessed using the National Center for Biotechnology Information (NCBI), nucleotide database (http://www.ncbi.nlm.nih.gov) in fasta format. All sequences were lined up utilizing mega x (Sudhir Kumar et al. 2018) (version 10.2.2). ATG and TGG are novel codons for methionine and tryptophan, which cannot be biased are excluded. Three stop codons, TAG, TAA, and TGA, are excluded from the current study.

2.2 Phylogenetic Analysis

A phylogenetic analysis is an assessment of the relationships among sequences and their approximated common ancestors. Most phylogenetic trees are constructed from DNA or protein arrangements [14]. Once in the past, the reason for most sub-atomic phylogenetic trees was to assess the connections among the species addressed by those groupings. Developing a phylogenetic tree requires four different advances in particular, identify and get a bunch of DNA or protein sequences, aligning the sequences, assessment of a tree from the aligned sequences, and present the tree to distinctly pass on the important realities to other people. Phylogenetic analysis was conducted using mega x software, http://www.megasoftware.net (version 10.2.2) and the phylogenetic trees were viewed using Figtree http://www.tree.bio.ed.ac.uk/software/figtree/ (version 1.4.4).

2.3 Relative_Synonymous_Codon_Usage (RSCU) Analysis

The Relative_Synonymous_Codon_Usage values for each and every codon were determined in deciding the pattern of synonymous_codon_usage. The proportion of noticed recurrence to natural recurrence for a given amino acid is called RSCU esteem. It stays unpretentious by the length of a sequence or the occurrence of an amino acid [13]. Codons that have RSCU esteems >1.00 demonstrate a positive codon_usage_bias, whereas codons that have RSCU esteems <1.00 show a negative codon_usage_bias [15]. Over represented codons have RSCU estimations of higher than the value 1.6, while values below 0.6 are consumed by underrepresented codons. The codons with the Relative_Synonymous_Codon_Usage esteems running somewhere in the range of 0.6 and 1.6 are viewed as fair or arbitrarily utilized [16]. The RSCU esteems are helpful in processing codon utilization among genes that are vary in size and amino acid synthesis [17] To regulate the codon_usage_bias pattern cya, lef, and pag genes, the relative synonymous_codon_usage (Relative_Synonymous_Codon_Usage) of *Bacillus anthracis* coding area was intended using R (version 3.6.2) [18].

3 Results and Discussion

3.1 Phylogenetic Analysis

'Mega x' (version 10.2.2) was used to identify the best-fit nucleotide substitution model. According to the revised Akaike Knowledge Criterion (AICc). The best-fit model of nucleotide substitution was found to be the general time reversible (GTR) model with gamma distributed evolutionary rates (G) and invariant sites (I) (GTR +

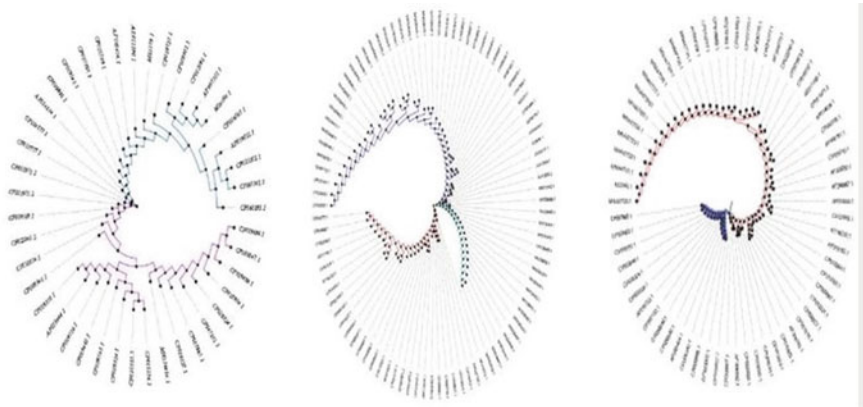


Fig. 1 Phylogenetic tree of **a** *cya,* **b** *lef,* and **c** *pag* genes

G + I). Mega x was used to construct the maximum-likelihood (ML) phylogenetic tree (version 10.2.2). The result showed the different clades of the DNA sequences of the three different virulent genes viz cya, lef, and pag (Fig. 1).

Visualization of the trees was performed by the software 'Figtree' version (1.4.4), http://www.tree.bio.ed.ac.uk/software/figtree/.

3.2 RSCU Pattern

The RSCU value is a significant boundary for determining the equivalent codon's tendency. It discusses the proportion of event recurrence of one codon and common usage reappearance in a gene sample. Codons with RSCU esteems greater than 1.0 are considered to have a positive codon usage bias. Surprisingly, individuals with RSCU values less than 1.0 remain characterized as fewer abundant codons. Total RSCU value will instinctively reproduce the predilection for codon usage in a definite genome. The complete RSCU values of cya, lef, and pag genes that resides in px01plasmid of *Bacillus anthracis* are calculated, and the results are depicted in bar graph using Microsoft excel (Fig. 2).

Codon usage bias illustrates that the blocks in those RSCU esteems are more than 1.6, which may perhaps be viewed as the abundant codons, and are ACA, AGA, AGT, CAT, GCT, TAT, TTA and TTT in cya gene, AAT, ACA, AGA, AGT, ATT, CCA, GAT, GCA, GTA, TAT, TC, TGT and TTA in lef gene, AGA, AGT, CAA, CAT, GAT, GCA, GGA, TCT and TTA in pag gene. Among them, TTA has the most elevated RSCU estimation of 3.73, 3.22 and 4.06 in cya, lef, and pag genes, respectively. The RSCU esteem bars are under 0.6 attributes, which could be referred to as the less abundant codons. Overall, RSCU values for codons that end in A or T are lower than those for codons that end in G or C. There are three stop codons

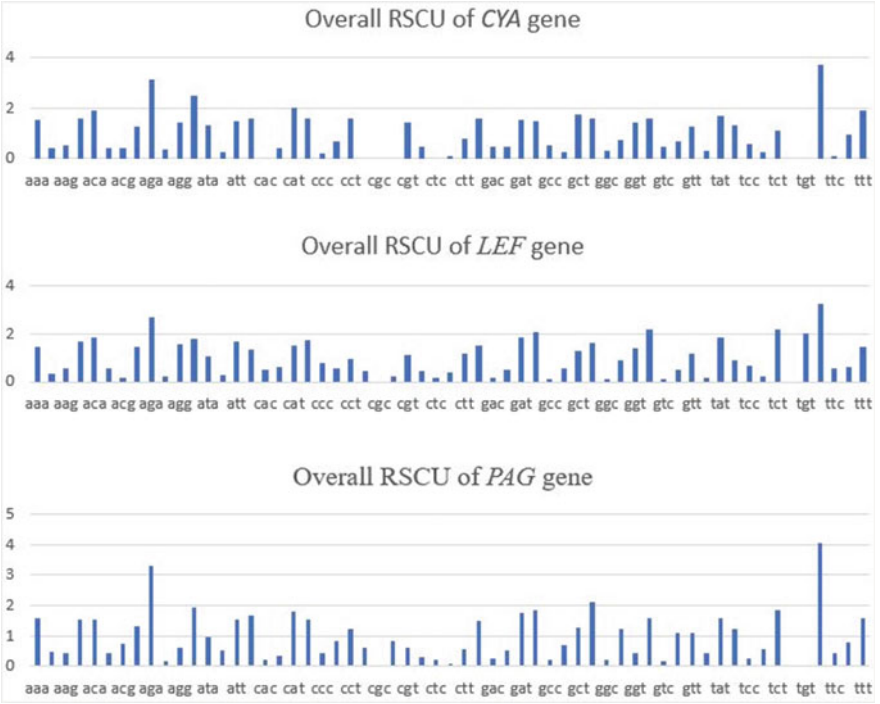


Fig. 2 Overall RSCU of *cya* gene, *lef* gene, and *pag* gene of *Bacillus anthracis* genome

(TGA, TAA, and TAG), but no related amino acids that correspond to stop codons, so the data is discarded. The estimation of RSCU is normally utilized as an estimation of codon_usage_bias. Total RSCU esteems (Fig. 2), in limited way, will mirror the qualities of codon usage, yet with regards toward the codon use of distinct grouping for an exact genome, it inclines to see that there is an extraordinary contrast of RSCU esteems from various qualities even of single genome.

Harmful types of *Bacillus anthracis* are the twoo huge pathogenicity associated plasmids: (1) px01, encodes the *Bacillus anthracis* toxin genes pagA, lef, and cya (2) px02, which conveys the genes liable for capsule amalgamation and deprivation, capA, capB, capC, and capD. *Bacillus anthracis* communicates its infective action mostly over the capsule and the creation of a harmful compound comprising of three proteins referred as protective antigen, lethal factor and edema factor. Two enormous plasmids of a *Bacillus anthracis* genome are fundamental for complete pathogenicity, end of any drastically lessens the harmfulness of *Bacillus anthracis* [1]. Toxins, alongside factors needed for microbial embodiment, are encoded on plasmids, px01and px02. The toxin proteins of *Bacillus anthracis*, edema factor and lethal factor, apiece structure paired buildings with protective antigen, instigating serious edema and cell death [6]. The px01plasmid has pagA (defensive antigen and an intra film poison carrier), lef (The lethal_factor, a zn_2+−subordinate end protease)

as well as cyaA (The edema_factor, a calmodulin sensitive adenylate_cyclase). px02 plasmid conveys the capsule biogenesis genes originate in a group and is fundamental for the complete *Bacillus anthracis* sickness [19, 20]. Harmfulness of maximum *Bacillus anthracis* strains is related to two mega plasmids, and strains not having either of the plasmid are moreover destructive or fundamentally constricted. px02 possesses the characteristics needed for the formulation of an antiphagocytic poly-D-glutamic acid pill. The *Bacillus anthracis* toxin proteins, edema factor, lethal factor, and protective antigen are all blended in the 110 MDa px01plasmid. All of these proteins were used in paired mixes to make two *Bacillus anthracis* toxins: edema_toxin (a protective_antigen and edema_factor) and lethal_toxin (a protective_antigen and lethal_factor). Three qualities needed for capsule amalgamation (capB, capC, and capA) are conveyed by plasmid px02, as well as a quality related to capsule deprivation (dep) and an executing administrative genetic factor (acpA). The underlying qualities for the *Bacillus anthracis* toxin proteins [cya (edema_factor), lef (lethal_factor), and pagA (protective_antigen)] are carried by the px01plasmid, as well as two administrative genes (pagR and atxA), gene indoctrination a type-I called topoisomerase (topA), and an as of late portrayed operon comprising three qualities whose capacities seem to influence the germination [5]. From these literatures, we found that the destructive qualities of *Bacillus anthracis* are cya, lef, and pag (px01plasmid) genes and cap genes (px02 plasmid). Subsequently chose the px01plasmid genes cya, lef, and pag for our codon usage bias investigation study.

Codon bias has an extremely expansive importance for investigating a genome. The rate of identical codon usage varies greatly among genes in micro-organisms [21]. Codon bias has an extremely wide importance for investigating a genome. On or after the atomic level, codon bias can equally clarify essential marvel of transformative cycle in science [22]. Previous research has shown that the EF gene's codon use revealed a high base composition A + T (71%) for its deoxyribo nucleic acid [23]. The lef gene's codon use revealed its high (70%) A + T content [3]. The pag gene's codon use revealed its high A + T (69%) base conformation [4]. RSCU estimations of the destructive genes cya, lef, and pag of *Bacillus anthracis* genome (Fig. 2) show strong codon usage bias. Just three genes which are harmful and stays alive in plasmid px01of *Bacillus anthracis* were investigated in the present work. It is imperative to grow the extent of the genome in the further research study.

4 Conclusion

Present work analyzed the codon usage patterns of harmful genes namely cya, lef, and pag remains alive in px01plasmid of *Bacillus anthracis* genome. Phylogenetic analysis and RSCU pattern are analyzed to identify the codon bias existence in the *Bacillus anthracis* genes. Current study is on codon usage bias in three distinctive harmful genes remains alive in px01plasmid of *Bacillus anthracis* genome. The outcome of the present study would help further uncover the hidden elements of hereditary development in *Bacillus anthracis* genome. These outcomes demonstrated that there

is a codon_usage_bias in the *Bacillus anthracis* genome. This data is significant for clarifying the function of *Bacillus anthracis* and also helps in understanding the developmental cycle of the *Bacillus anthracis* genome. Codon optimization increases protein and RNA levels significantly, implying that codon usage is an essential determinant of gene expression. Current study encompassed only px01 plasmid genes; further, this can be outstretched to px02 plasmid genes.

Acknowledgements We would like to thank the Spatial Epidemiology lab, ICAR–NIVEDI, Department of Veterinary Public Health and Epidemiology, Veterinary College and Outreach project on Zoonotic diseases, ICAR, for providing essential support to carry out the current research.

Ethical Statement
Authors declare that ethical statement is not applicable as we have not collected any animal sample for the study.

Interests in Conflict
There are no conflicts of interest, according to the authors.

References

1. A. Fasanella, *Bacillus anthracis*, virulence factors, PCR, and interpretation of results. Landes Biosci. **4**(8), 659–660 (2013)
2. A.T. John Young, R. John Collier, Anthrax toxin: receptor binding, internalization, pore formation, and translocation. Annu. Rev. Biochem. **76**, 243–265 (2007)
3. T.S. Bragg, D.L. Robertson, Nucleotide sequence and analysis of the lethal factor gene (Zef) from *Bacillus anthracis*. Elsevier **81**(1), 45–54 (1989)
4. S.L. Welkos, J.R. Lowe, F. Eden-McCutchan, M. Vodkin, S.H. Leppla, J.J. Schmidt, Sequence and analysis of the DNA encoding protective antigen of *Bacillus anthracis*. Elsevier **69**(2), 287–330 (1988)
5. R.T. Okinaka, K. Cloud, O. Hampton, A.R. Hoffmaster, K.K. Hill, P. Keim et al., Sequence and organization of pXO1, the Large *Bacillus anthracis* plasmid harboring the anthrax toxin genes. J. Bacteriol. **181**(20), 6509–6515 (1999)
6. A.B. Nicholas, B.T. James, N.G. Shea, S.M. Kevin, Y.F. Viacheslav, K. Heather, et al., Detection of *Bacillus anthracis* DNA in complex soil and air samples using next-generation sequencing. PLOS One **8**(9), e73455 (2013)
7. M.W.S. Hannah, R.O.C. Andre, Factors influencing codon usage bias in genomes. J. Braz. Chem. Soc. **19**(2), 257–262 (2008)
8. T. Pan, D. Li, L. Mengcheng, T. Fangqiang, T. Po, P. Zishu, Analysis of synonymous codon usage in classical swine fever virus. Springer **38**(1), 104–112 (2009)
9. B. Gerrit, H. Diarmaid, The selective advantage of synonymous codon usage bias in Salmonella. PLOS Genet. **12**(3), e1005926 (2016)
10. C.G. Kurnald, Codon bias and gene expression. Elsevier **285**(2), 165–169 (1991)
11. R.M. Kliman, J. Hey, The effects of mutation and natural selection on codon bias in the genes of drosophila. Genet. Soc. Am. **137**(4), 1049–1056 (1994)
12. H.M.W. Salim, A.R.O. Cavalcanti, Factors influencing codon usage bias in genomes. J. Braz. Chem. Soc. **19**(2), 257–262 (2008)
13. K.B. Susanta, W.S. David, Comparative analysis of codon usage bias and codon context patterns between dipteran and hymenopteran sequenced genomes. PLOS One **7**(8), e43111 (2012)

14. W. Huiguang, B. Zhengyu, M. Chunxiao, C. Zhenhai, Z. Jingwen, Comprehensive analysis of codon usage on porcine Astrovirus. MDPI Viruses **12**(9), 991 (2020)
15. H. Snawar, S. Pottathil, M.I. Mohammed, S.C. Muhammad, T.R. Sahibzada, Analysis of codon usage and nucleotide bias in middle east respiratory syndrome coronavirus genes. Evol. Bioinform. **16**, 1–13 (2020)
16. Y. Xiaoting, F. Qinlei, Y. Bo, L. Ping, U.R. Siddiq, C. Dekun, T. Shiheng, Codon usage bias analysis of Bluetongue virus causing livestock infection. Front. Microbiol. **11**, 655 (2020)
17. S. Aravind, N.M. Kamble, S.S. Gaikwad, S.A. Khulape, D. Sohini, K. Dhama, M.C. Madhan, Bioinformatics study involving characterization of synonymous codon usage bias in the duck enteritis virus glycoprotein D (gD) gene. Asian J. Animal Vet. Adv. **9**(4), 229–242 (2014)
18. R. RCoreTeam, A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. http://www.r-project.org/ (2020)
19. K. Paul, M.G. Jeffrey, M.K. Alexandra, M.S. James, C. Jean, O. Richard, The genome and variation of *Bacillus anthracis.* Mol. Aspects Med. **30**(6), 397–405 (2009)
20. A.B. Nicholas, B.T. James, N.G. Shea, S.M. Kevin, Y.F. Viacheslav, K. Heather, Detection of *Bacillus anthracis* DNA in complex soil and air samples using next-generation sequencing. PLOS One **8**(9), e73455 (2013)
21. M.S. Paul, W.H. Li, The codon adaptation index—a measure of directional synonymous codon usage bias, and its potential applications. Nucleic Acids Res. **15**(3), 1281–1295 (1987)
22. C.W. Tai, C.C. Feng, The evolutionary landscape of the Mycobacterium tuberculosis genome. Elsevier **518**(1), 187–193 (2012)
23. D.L. Robertson, M.T. Tippetts, S.H. Leppla, Nucleotide sequence of the *Bacillus anthracis* edema factor gene (cya): a calmodulin-dependent adenylate cyclase. Elsevier **73**(2), 363–371 (1988)

Constructing Digital Signature Algorithm Based on a New Key Scheme



Van Luu Xuan, Hoa Doan Van, and Dung Luu Hong

Abstract E-government is the latest trend in many countries in which the government is using the online system for delivering government services to citizens, and the digital signature is used to validate contents and authorize users who are involving in the E-governance system. Although there are many digital signature schemes currently known as RSA, Elgamal, the approach of improving the safety level of digital signature schemes based on the hardness of solving simultaneous difficult assumptions has still remained underdeveloped and attracted rising attentions from researchers. In this research, with the target to improve safety level of digital signature schemes, we present a new approach for constructing digital signature scheme. Algorithms that used in this digital signature scheme are built based on a new key form. This new key format is constructed using a new difficulty problem without high-efficiency solution, and it can be applied to construct digital signature algorithms. According to this research, a high-security digital signature class can be constructed by the proposed method in some actual situation.

Keywords Digital signature algorithm · Public key cryptosystem · Discrete logarithm problem

1 Introduction

Nowadays, in the development of Industry 4.0, a lot of information exchange and control activities have been carried out over the network. Along with the convenience, information security is potentially risky, increasingly important and needs special attention. All online transactions need to ensure the integrity and identity of the sender

V. L. Xuan (✉)
People's Security Academy, Hanoi, Vietnam

H. D. Van
Academy of Military Science and Technology, Hanoi, Vietnam

D. L. Hong
Military Technical Academy, Hanoi, Vietnam

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_2

of the message. Therefore, digital signatures will be widely used in the near future. In addition to applying classic digital signature algorithms such as RSA, Elgamal [12], …, scientists have researched and developed other digital signature algorithms to meet in some specific cases, for example improving safety or improving the efficiency of the algorithm. As research improves the security of digital signature algorithms, a number of studies have investigated the development of difficult problems in number theory. By combining the solvability of these difficult problems, some new digital signature algorithms have been constructed and developed.

In [1–11], several studies have combined hard problems of discrete logarithm and integer factorization to develop digital signature algorithms. In line with this research direction, we propose a method to build algorithms that can be applied to create a new digital signature scheme based on a new key scheme. The new key scheme was developed from a root problem and discrete logarithm problem, which is difficult to find an effective solution. Therefore, digital signature scheme based on this new key scheme is secure and can be applied in many actual situations.

2 Some Hard Problems Can Be Applied to Construct Secure Digital Signature Schemes

2.1 Discrete Logarithm Problem

The discrete logarithm problem (DLP) is stated as follows:

Let a large prime number p and g denote a generator of Z_p^*, *for an integer number* $\beta \in Z_p^*$, *find* α *satisfying following equation*:

$$\beta = g^{\alpha} \bmod p$$

Until now, DLP is still a difficult problem to solve. Some algorithms for the discrete logarithm problem are baby step–giant step [13], Pohlig–Hellman algorithm [14], Pollard's rho algorithm [15],…. Some algorithms can solve it quickly in a few special cases. The index calculus algorithm is a probabilistic algorithm for computing discrete logarithms, and the expected running time of that algorithm can be stated as $L_n[1/2, \sqrt{2} + o(1)]$. However, no efficient method is known for computing them in general to this day, and none of them can solve DLP in polynomial time. So that, several important algorithms in public key cryptography base their security on the assumption that the discrete logarithm problem over carefully chosen groups has no efficient solution.

2.2 Root Problem

The root problem on Z_p^* (denote as RP problem) is stated as follows:

Let two large positive numbers be (p, k), in which: p is a prime number, $k > 2$, for a positive number $y \in Z_p$, find an integer number x satisfying the following modulo equation:

$$y = x^k \bmod p$$

If $k = 2$, the root problem is not so difficult to solve. We can easily find the integer number x such that $y = x^2 \bmod p$ with some algorithms have time complexity $O(\log p)^4$. However, when $k > 2$, this problem will be more difficult to solve.

The root problem is rarely used alone in building public key cryptography algorithms or applied to construct digital signature schemes. It is often used in combination with other hard problems (discrete logarithm problem, integer factorization problem,…) to build digital signature scheme more secure. In [5], Nikolay Andreevich Moldovyan proved that the above root problem is a hard problem (cannot solve in polynomial time) if pair of integer numbers (p, k) satisfy the following condition:

$$p = N \times k^s + 1,$$

in which: $s \geq 2$ and N is an integer number.

2.3 An Expanded Form of Hard Problems

In this section, we propose a new form of hard problem (new key scheme), based on the hardness of solving simultaneously two hard problems (DLP and RP), it is stated as follows:

Let a large prime number $p \in Z_p^*$, given a pair of numbers $(r, s) \in Z_p^*$, find an integer number x satisfying the following modulo equation:

$$r^x = x^s \bmod p \tag{1}$$

Formally, we can see that, if the right side of Eq. (1) is a constant number, then the proposed problem will have the following form:

$$r^x = C \bmod p \tag{2}$$

Now, with r, C are known numbers, Eq. (2) is a discrete logarithm problem (DLP), and solving this problem is difficult.

Otherwise, if the left side of Eq. (1) is a constant number (C), then the proposed problem will have the following form:

$$x^s = C \bmod p \tag{3}$$

Easily, we can see that, with s, C are known numbers, Eq. (3) is a root problem on Z_p (RP), and solving this problem is difficult.

Though both sides of Eq. (1) are not constant numbers here, none of them is known number, as such, algorithms for solving DLP and RP cannot be applied for solving the expanded form (1). To solve the above expanded form of hard problems, we must solve two hard problems (RP and DLP) simultaneously. So that, we can assert that the new form of hard problem is proposed here as much harder to solve than root problem and discrete logarithm problem.

3 Building Digital Signature Algorithm Based on a New Key Scheme

3.1 Proposed Key Scheme

Key scheme of Elgamal digital signature algorithms is built based on the discrete logarithm problem:

$$y = g^x \bmod p \tag{4}$$

Here, (x, y) are private key and public key of a signer, (g, p) are domain parameters, system parameters were created by digital authentication service provider, in which g is generator of the group Z_p and p is a prime number. Finding private key x, from public parameters y, g and p, is a difficult problem if p is a large and strong prime number.

From (4), it can be seen that if g is also a secret parameter that is equal to x, then (4) will become the following form:

$$y = x^x \bmod p \tag{5}$$

We have

$$y = x^x \bmod p \Leftrightarrow y^{1/x} = x \bmod p \Leftrightarrow y^{\left(x^{-1}\right)} = \left(x^{-1}\right)^{-1} \bmod p \tag{6}$$

Let $x^{-1} = X$, we see that (6) will become the following form:

$$y^X = X^{-1} \bmod p \tag{7}$$

It is easy to see that (7) is a special case of (1) with $a = y, b = -1$. Thus, the difficulty of solving (5) is similar to the difficulty of solving (1).

Based on the difficulty of solving (5), we propose a new key scheme as follows: With (p_1, p_2) are prime numbers that being the domain parameters/system parameters that are created by the sender of service provider and they must satisfy the condition $p_2|(p_1 - 1)$, each object chooses a number $\alpha \in (1, p_1)$. Let sk be private key, and it is generated by the following equation:

$$sk = \alpha^{(p_1-1)/p_2} \tag{8}$$

Then, the public key is generated, according to (5), as follows:

$$pk = (sk)^{sk} \bmod p_1 \tag{9}$$

The key scheme here can be described in algorithm 1 as a key generation algorithm as follows:

Algorithm 1 Key Generation Algorithm

Input: l_1, l_2 - length by bits of p_1, p_2.
Output: p_1, p_2, sk, pk.
1: **generate** p_1, p_2: $length(p_1) = l_1, length(p_2) = l_2, p_2|(p_1 - 1)$
2: **select** $\alpha : \alpha \in (1, p_1)$
3: $sk \leftarrow \alpha^{(p_1-1)/p_2} \bmod p_1$
4: **if** $(sk == 1)$ **then**
5: **go to** 2
6: **end if**
7: $pk \leftarrow (sk)^{sk} \bmod p_1$
8: **return** $\{p_1, p_2, sk, pk\}$

Note:

- $length(.)$: function calculates the length by bits of a positive number.
- p_1, p_2: prime numbers (system parameters) are selected.
- sk: private key of signature object (S).
- pk: public key of signature object (S).

When using (5) as a key generation scheme for the digital signature algorithm, we must construct right signing and testing algorithms. The following section will present a method of constructing digital signature algorithm based on a new key scheme.

3.2 Constructing Digital Signature Algorithm Based on the Proposed Key Scheme

A digital signature scheme consists of three main algorithms: Key generation algorithm outputs the private key and a corresponding public key; signing algorithm produces a signature from the plaintext and the private key; and signature veraifying algorithm that either accepts or rejects the message's claim to authenticity based on the message, public key and signature. The method of constructing digital signature scheme based on proposed form of hard problem will be presented immediately as follows:

The key generation algorithm is described in algorithm 1, and the construction of signing algorithm and signature verifying algorithm will be presented in the following:

3.2.1 Signing Algorithm

Suppose (S_1, S_2) is the signature of message Mes and S_1 is calculated from $s \in Z_p^*$ by the following formula:

$$S_1 = s^{sk} \bmod p_1 \tag{10}$$

and S_2 is calculated from $t \in Z_p^*$ by:

$$S_2 = t^{sk} \bmod p_1 \tag{11}$$

Assume that the signature verifying equation of the algorithm has the following form:

$$S_1^H = S_2^{pk} \times pk^{(S_1 \times S_2 \bmod p_1)} \bmod p_1 \tag{12}$$

In which

- $H = Hash(M)$, $Hash(.)$ is a hash function;
- $S_1 \times S_2 \bmod p_1 = b^{sk} \bmod p_1$;
- $b = \beta^{(p_1-1)/p_2} \bmod p_1, \beta \in (1, p_1)$.

Let:

$$b^{sk} \bmod p_1 = Z \tag{13}$$

So, the signature verifying equation will be changed into the following form:

$$S_1^H = S_2^{pk} \times pk^Z \bmod p_1 \tag{14}$$

From (9), (10), (11) and (14), we have

$$s^{sk \cdot H} = t^{sk \cdot pk} \times (sk)^{sk \cdot Z} \bmod p_1 \tag{15}$$

From (15) to $s^H = t^{pk} \times sk^Z \bmod p_1$, or

$$s = t^{H^{-1} \cdot pk} \times sk^{H^{-1} \cdot Z} \bmod p_1 \tag{16}$$

Otherwise, from (10), (11) and (12), we have

$$s \times t \bmod p_1 = b \tag{17}$$

From (16) and (17), we have $t^{H^{-1}\cdot pk} \times (sk)^{H^{-1}\cdot Z} \times t \bmod p_1 = b$, or:

$$t^{H^{-1}\cdot pk+1} \times (sk)^{H^{-1}\cdot Z} \bmod p_1 = b \tag{18}$$

From (18), we have

$$t = \left(b \times (sk)^{-Z\cdot H^{-1}}\right)^{\left(H^{-1}\cdot pk+1\right)^{-1}} \bmod p_1 \tag{19}$$

From (19) and (17), we can calculate s by $s = b \times t^{-1} \bmod p_1$, or

$$s = t^{H^{-1}\cdot pk} \times (sk)^{H^{-1}\cdot Z} \bmod p_1$$

From the values s and t, we can calculate the value of S_1, a component of the signature, by Eq. (10): $S_1 = s^{sk} \bmod p_1$, and calculate S_2, the second component of the signature, by Eq. (11): $S_2 = t^{sk} \bmod p_1$.

Here, signing algorithm can be described in algorithm 2 as follows:

Algorithm 2 Signing Algorithm

Input: p_1, p_2, sk, pk, Mes.
Output: (S_1, S_2) (Signature of Mes).
1: $H = Hash(Mes)$
2: **select** $\beta : \beta \in (1, p_1), b \leftarrow \beta^{(p_1-1)/p_2} \bmod p_1$
3: $Z \leftarrow b^{sk} \bmod p_1$
4: $t \leftarrow \left(b \times sk^{-Z.H^{-1}}\right)^{\left(H^{-1}.pk+1\right)^{-1}} \bmod p_1$
5: $s \leftarrow b \times t^{-1} \bmod p_1$
6: $S_1 \leftarrow s^{sk} \bmod p_1$
7: $S_2 \leftarrow t^{sk} \bmod p_1$
8: **if** $((S_1 == 1)$ or $(S_2 == 1))$ **then**
9: **go to** 2
10: **end if**
11: **return** (S_1, S_2)

Note:

- Mes: Message need to be signed.
- $Hash(.)$: Hash function $Hash : \{0, 1\}^{\infty} \mapsto Z_n$, in which: $p_2 < n < p_1$.
- (S_1, S_2): Signature of S on the message Mes.

3.2.2 Signature Verifying Algorithm

Verifying formula of this proposed algorithm is assumed that

$$(S_1)^H = (S_2)^{pk} \times (pk)^{(S_1 \times S_2 \bmod p_1)},$$

in which, Mes is a message that must be verified and H is a hash value of the message Mes ($H = Hash(M)$). The recipient will authenticate the integrity and originality of the message Mes based on its signature. If the message Mes is consistent with its signature (S_1, S_2), the recipient can trust the message. In other words, the above expression must be true. Otherwise, the message or the signature is invalid, and its correctness is not be recognized. So, we can calculate the left side of signature verifying formula as follows:

$$V_1 = (S_1)^H \bmod p_1 \tag{20}$$

and we can calculate the right side of signature verifying formula as follows:

$$V_2 = (S_2)^{pk} \times (pk)^{\overline{Z}} \bmod p_1 \tag{21}$$

in which:

$$\overline{Z} = S_1 \times S_2 \bmod p_1 \tag{22}$$

So, if $V_1 == V_2$, then the signature received by the recipient is correct, and the message is attached to it will be accepted by integrity also originality.

Therefore, the signature verifying algorithm of the proposed digital signature scheme is described as follows:

Algorithm 3 Signature Verifying Algorithm

Input: p_1, pk, Mes, S_1, S_2.
Output: $Correct/Incorrect$
1: $H \leftarrow Hash(Mes)$
2: $V_1 \leftarrow (S_1)^H \bmod p_1$
3: $\overline{Z} \leftarrow S_1 \times S_2 \bmod p_1$
4: $V_2 \leftarrow (S_1)^{pk} \times pk^{\overline{Z}}$
5: **if** $(V_1 == V_2)$ **then**
6: **return** $Correct$
7: **else**
8: **return** $Incorrect$
9: **end if**

3.2.3 The Correctness of the Proposed Method

Assessing the validity of the proposed scheme can be stated as follows:

Let (p_1, p_2) be two prime numbers with $(p_1 - 1) \vdots p_2$, a hash function $Hash : \{0, 1\}^* \mapsto Z_n, p_2 < n < p_1, \alpha \in (1, p_1), sk = \alpha^{(p_1-1)/p_2} \bmod p_1, pk = (sk)^{sk} \bmod p_1$, $\beta \in (1, p_1)$, $b = \beta^{(p_1-1)/p_2} \bmod p_1$, $Z = b^{sk} \bmod p_1$, $H = Hash(Mes)$, $t = \left(b \times (sk)^{-Z \cdot H^{-1}}\right)^{\left(H^{-1} \cdot pk+1\right)^{-1}} \bmod p_1, s = b \times t^{-1} \bmod p_1, S_1 = s^{sk} \bmod p_1, S_2 = t^{sk} \bmod p_1$.

If $\overline{Z} = S_1 \times S_2 \bmod p_1$, $V_1 = (S_1)^H \bmod p_1$, $V_2 = (S_2)^{pk} \times (pk)^{\overline{Z}} \bmod p_1$ then: $V_1 = V_2$.

Assessing the validity of the proposed algorithm can be proved as follows:

From Eqs. (9), (10), (11), (16), (19) and (21), we have:

$$V_1 = (S_1)^H \bmod p_1 = s^{sk \cdot H} \bmod p_1 = \left(t^{H^{-1} \cdot pk} \times sk^{H^{-1} \cdot Z}\right)^{sk \cdot H} \bmod p_1 \quad (23)$$

$$= t^{sk \cdot pk} \times (sk)^{sk \cdot Z} \bmod p_1 = (S_2)^{pk} \times (pk)^{Z} \bmod p_1$$

Moreover, from Eqs. (10), (11), (16), (19) and (20), we have

$$\overline{Z} = S_1 \times S_2 \bmod p_1 = s^{sk} \times t^{sk} \bmod p_1 \quad (24)$$

$$= (s \times t)^{sk} \bmod p_1 = b^{sk} \bmod p_1 = Z$$

From (21) and (24), we have

$$V_2 = (S_2)^{pk} \times (pk)^{\overline{Z}} \bmod p_1 = (S_2)^{pk} \times (pk)^{Z} \bmod p_1 \quad (25)$$

From (23) and (25), we have the proof $V_1 = V_2$. Thus, the above algorithm is correct.

4 Safety-Level Assessment of the Proposed Algorithm Based on the Proposed Key Scheme

The safety level of the proposed algorithm based on the new key scheme can be assessed by its ability to resist some types of attacks such as

- *Safety against attacks on the private key*

From (5), finding sk by algorithms for discrete logarithm problem on Z_p such as Pollard Rho, baby step–giant step and index calculus is impossible. Nowadays, the "brute force attack" is the only algorithm that can be applied to solve (5). However, "brute force attack" is not a polynomial time algorithm that can be applied in practical applications.

- *Safety against attack on signing algorithm*

An attacker could perform an attack on the signing algorithm to find sk. Finding sk from solving equations $S_1 = s^{sk} \bmod p_1$, or $S_2 = t^{sk} \bmod p_1$, or $Z = b^{sk} \bmod p_1$ (In which: $Z = (S_1 \times S_2) \bmod p_1$).

Including to solve Eq. (5), this is a hard problem. It shows that attacking signing algorithm to find sk is completely impossible.

+ *Safety against attack on signature verifying algorithm*

From the algorithm 3 of the proposed algorithm (signature verifying algorithm), if attacker wants to forge a signature, he must create a fake signature (S_1, S_2) that will be accepted as a valid signature of the message Mes, in other words, it must satisfy the following conditions:

$$(S_1)^H = (S_2)^{pk} \times (pk)^{(S_1 \times S_2 \bmod p_1) \bmod p_2} \bmod p_1 \tag{26}$$

From (26), if S_1 is preselected and then S_2 will be calculated, the condition (26) will become the following form:

$$(S_2)^H = X^{S_2} \bmod p_1 \tag{27}$$

If S_2 is preselected and then S_1 will be calculated, the condition (26) would look like the following:

$$(S_1)^{pk} = Y^{S_1} \bmod p_1 \tag{28}$$

With X and Y being constants, it is easy to see that (27) and (28) are hard problems that currently do not have a solution. It is easy to see that if the left side of (27) (or (28)) is a constant number, then this is a discrete logarithm problem, and if the right side of (27) (or (28)) is a constant number, then this is the root problem. However, in (27) and (28), both sides contain variables to be searched, so algorithms for discrete logarithm problem and root problem on Z_p are not applicable to solve (27) and (28).

5 Conclusion

According to the above proposed method, we have tested the implementation of this algorithm with some following scenarios:

- In the first case, all message and signature were not modified during transmission, so, with the result, the message and its signature are consistent, and so that, the recipient can trust the integrity and original of the message.
- In the second case, the outgoing message has been edited, with the result, the message and its signature are not consistent, and so that, the recipient should not trust the integrity and original of the message.
- In the third case, the signature has been modified. The result shows that the integrity of the signature and the message has been lost.

The obtained results show that the proposed algorithm performed correctly.

So, the paper proposes a new method to build a digital signature algorithm based on a new key scheme. By using this new key scheme, we can develop some digital signature algorithms. These algorithms are highly secure and can be applied in some actual situation.

References

1. W.-H. He, Digital signature scheme based on factoring and discrete logarithms. Electron. Lett. **37**(4), 220–222 (2001). https://doi.org/10.1049/el:20010149
2. S.-F. Tzeng, C.-Y. Yang, M.-S. Hwang, A new digital signature scheme based on factoring and discrete logarithms. Int. J. Comput. Math. **28**(1), 9–14 (2004). https://doi.org/10.1080/00207160310001614954
3. L.-H. Li, S.-F. Tzeng, M.-S. Hwang, Improvement of signature scheme based on factoring and discrete logarithms. Appl. Math. Comput. **161**, 49–54 (2005). https://doi.org/10.1016/j.amc.2003.12.008
4. S. Wei, Digital signature scheme based on two hard problems. Int. J. Comput. Sci. Netw. Sec. **7**(12), 207–209 (2007)
5. N.A. Moldovyan, Digital signature scheme based on a new hard problem. Comput. Sci. J. Moldova **16**(2)(47), 163–182 (2008)
6. E.S. Ismail, N. Tahat, R. Rozita Ahmad, A new digital signature scheme based on factoring and discrete logarithms. J. Math. Stat. **4**(4), 222–225 (2008). https://doi.org/10.3844/jmssp.2008.222.225
7. A.-F. Mustafa, A. Sattar, A.-F. Mohammad, A new digital signature scheme based on integer factoring and discrete logarithm problem. Int. J. Comput. Appl. **17**(2), 108–115 (2010)
8. N. Tahat, Z. Mustafa, A.K. Alomari, New ID-based digital signature scheme on factoring and discrete Logarithms. Appl. Math. Sci. **6**(28), 1363–1369 (2012)
9. A.N. Berezin, N.A. Moldovyan, V.A. Shcherbacov, Cryptoschemes based on difficulty of simultaneous solving two different difficult problems. Comput. Sci. J. Moldova **21**(2) (62) (2013)
10. D. Poulakis, A public key encryption scheme based on factoring and discrete logarithm. J. Discrete Math. Sci. Cryptograp. **12**(6), 745–752 (2013). https://doi.org/10.1080/09720529.2009.10698270
11. S.-Y. Chiou, Novel digital signature schemes based on factoring and discrete logarithms. Int. J. Secur. Appl. **10**(3), 295–310 (2016). https://doi.org/10.14257/ijsia.2016.10.3.26
12. T. Elgamal, A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theo. **31**(4), 469–472 (1985). https://doi.org/10.1109/TIT.1985.1057074
13. D. Shanks, Class number, a theory of factorization and genera, in *Proceedings of Symposia in Pure Mathematics, Providence*, vol. 20 (American Mathematical Society, R.I. 1971), pp. 415–440. https://doi.org/10.1090/pspum/020/0316385
14. S. Pohlig, M. Hellman, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Trans. Inf. Theo. **24**(1), 106–110 (1978). https://doi.org/10.1109/TIT.1978.1055817
15. J.M. Pollard, Monte carlo methods for index computation (mod p). Math. Comput. **32**(143), 918–924 (1978). https://doi.org/10.2307/2006496

Internet of Things (IoT), Three-Layer Architecture, Security Issues and Counter Measures



Bonani Paul

Abstract Internet of Things (IoT) a tired framework necessitates the use of diverse technologies, for capturing, processing, analyzing, and storing large unprocessed data in cloud-based data centers for the IoTs to function as desired. The security and privacy are some of the critical concerns with increased communication among billons of IoT-connected devices. In this article, an overview of three-layered IoT architecture is provided, and the vulnerabilities and threats in all the three layers have been discussed. It also discusses the security practices that can be enforced in each layer due to limiting functionalities of current hardware technology. The article also explores some of the countermeasures and protection methods such as authentication, authorization, lightweight symmetric, and asymmetric algorithms that can be implemented against various attacks on all the three layers.

Keywords IoT architecture · Security issues and challenges · RFID · Blockchain

1 Introduction

The Internet of Things (IoT) can be defined as an integration of interconnected smart objects with embedded sensors, actuators, and processors for the purpose of exchanging data over the internet to accomplish intended objective. IoT is a seamless integration of virtual and real-world technologies working together in tandem. With more consumers and business enterprises embracing IoT technologies and solutions in real-time, more are the security concerns.

Secure communication, secure storage, and effective access control mechanism, are becoming the most pressing concerns associated with widespread application of IoT [1]. Since sensor networks are extremely vulnerable to attacks [2], it is critical to have a mechanism in place to safeguard the network, smart things, and users from all types of malicious attack, thereby creating a more robust environment. The

B. Paul (✉)
Department of Computer Science, St. Mary's College, Shillong, India
e-mail: b.paul@smcs.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_3

challenging part is the execution of light and quick cryptography algorithm because of limited processing power, limited battery, and memory capacity of these devices.

Cryptographic algorithms, like, advance encryption standard (AES), Diffi-Hellman (DH), secure hash algorithm (SHA), and Rivest Shamir Adelman (RSA), among others, can be used to address IoT security issues such as IoT data confidentiality, authenticity, and credibility [3].

The remainder of the article is structured as follows: Sect. 2 delves into the three-layer IoT architecture. Section 3 highlights some of the threats and vulnerabilities in each layer followed by potential counter measures in Sect. 4. The articles concludes in Sect. 5.

2 The IoT Architecture

The IoT architecture is a framework that defines the connectivity, communicating protocols, configuration, and organizational structure of the network to be used by the Web-enabled smart devices. Sensors, protocols, actuators, cloud services, and layers all play a significant role in IoT architecture.

There is no single IoT architecture that is widely agreed upon. Researchers have suggested a variety of architecture. In the following subsections, the three-layer architecture on IoT is discussed.

2.1 Three-Layer Architectures

The IoT architecture [4] with three layers, namely the perception layer, network layer, and application layers as shown in Fig. 1 is the most basic architecture which was initially introduced by researchers for the purpose of study.

2.1.1 Perception Layer

The perception layer is the lowest layer of the traditional three-layer IoT architecture that is responsible for hosting smart things [5]. The sensors in physical layer, senses certain physical parameters or detect other smart devices in the vicinity (such as the actuators, edge devices, and wireless sensors) to gather information from the surroundings (such as humidity, and temperature, and so on) and convert them in a digital streams. The primary function of this layer is to provide unique address identification and enable communication between low-range technologies such as RFID, near-field communication (NFC), Bluetooth, 6LoWPAN (low power personal area network) [6].

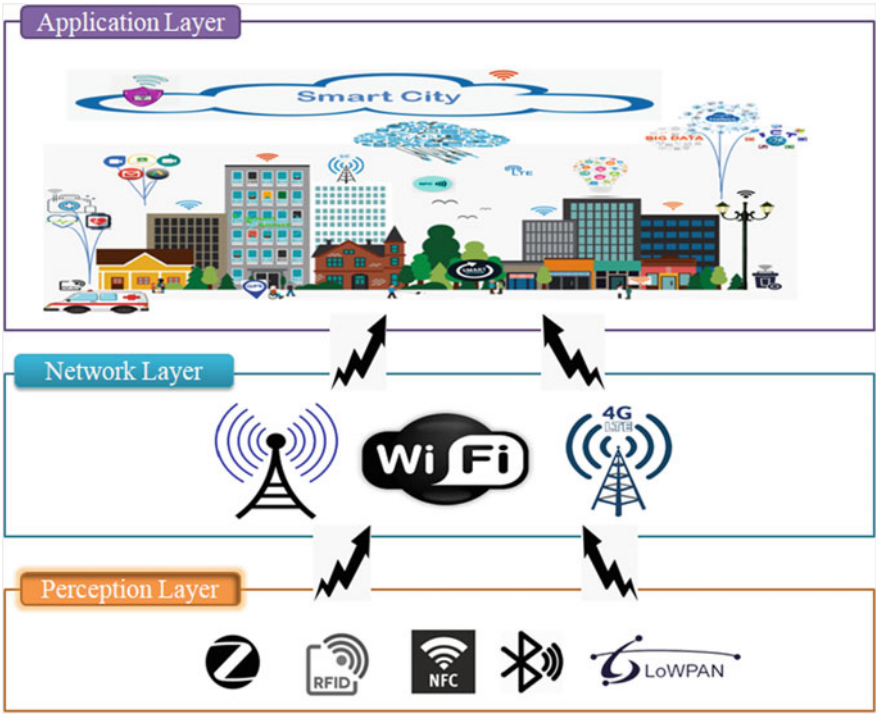


Fig. 1 The three-layer IoT architecture

2.1.2 Network Layer

The network layer is the core layer of the conventional three-layer IoT architecture that is capable of forwarding data for specific services. It enables secure communication across smart things and with the cloud via IoT gateway video networking technologies such as wired, Wi-Fi and cellular technologies. This layer also ensures that each system has its unique addressing and routing capabilities for seamless integration of infinite number of devices into a single unified network. The IETF implementation of 6LoWPAN protocol for IPV6 for unique addressing of devices is one such work involved [7].

2.1.3 Application Layer

The application layer is the topmost layer of traditional IoT architecture responsible for providing its users, customized, application specific services such as, smart education, smart health, smart energy grid, smart transportation, and many more.

3 Security Issues of Three Layer Architecture

As more and more internet-enabled smart gadgets joins the IoT community, greater the security breaches and so the attacks at the aforementioned layers. Security requirements are different at different layers of the IoT architecture. Some of them are highlighted in the following subsections.

3.1 Threats and the Vulnerabilities of Perception Layer

Lightweight encryption algorithm, data protection of sensors, and management of keys are the security requirements for the perception layer. Some of the major security threats encountered in this layer include cyber-attack, malicious code injection, fake node, sensor data security, data access, and authentication issues, malware attacks [8]. If proper security procedures, algorithms, and technologies are not applied in real time, these attacks can disrupt any form of application in IoT architecture. Technology-related attack for this layer is summarized in Table 1.

3.2 Threats and the Vulnerabilities of Network Layer

Identity authentication, encryption mechanism, and communication protection are core requirements for network layer specifications. Denial of services (DoS), man in the middle attack, eavesdropping, RFID interference, node jamming in the WSN, and network congestion attack are other security challenges faced in this layer. Some of the attacks in network layer of three-layer IoT architecture with some possible solutions are listed in Table 2.

3.3 Threats and the Vulnerabilities of Application Layer

Data exchange that protect user privacy and access controls are key security issues in application layer today. Some application layer threats include phishing, ransomware, and X scripts among others. Table 3 provides layer-wise attacks with some possible solutions.

Table 1 Attacks and possible solutions in perception layer

Technology	Attacks	Description	Possible solution
RFID	DoS [9]	Shut downs a machine or network, making it inaccessible to its users resulting in temporary or permanently incapacitated tags	Share tag with the server with a private key which can be encrypted only by authorized user [10]
	Cloning and spoofing [11]	Spoofing is the process of duplicating information from an RFID tag or smart card onto a clone tag to gain access to a protected area or object while bypassing security measures	Verify a tag's response with a OTP sent by the back-end server [12]
	MitM [13]	A hardware device captures and decodes the RFID signal between the victim's card and a card reader in an RFID enabled system	Authentication mechanism that provides evidence that message may have been tempered [14]
	Eavesdropping and replay [15]	Happens when an unauthorized reader is 'listening in' to the conversations between a tag and reader, with the intention of obtaining crucial data, replaying at a later time to steal vital information	VLFSR lightweight encryption function [16]
NFC	Eavesdropping	Happens when a third party intercepts the signal sent between two devices	Random key agreement method [17]
Bluetooth	Blue sniper rifle [18, 19]	A long-distance attacking tool with a powerful directional antenna for interception	Request for pairing before exchanging any information between paired devices [20]
	Blue jacking	Sends unsolicited messages to Bluetooth-enabled devices	
	Blue snarfing	Unwarranted access to schedules, call lists, email and SMS. It can also copy user's contents	
	Blue bugging	Technique to connect to the target device via Bluetooth connection and gain access to owners phonebook, send SMS, initiate or eavesdrop on incoming and outgoing calls	
	Blue printing	Determines the target device model and firmware version	

(continued)

Table 1 (continued)

Technology	Attacks	Description	Possible solution
Zigbee	Unauthorized traffic gathering [21]	Unauthorized access to a ZigBee sensor node causing unwarranted access to the network's shared secret key as well as the network traffic	Secure protocol which allows data flow without compromising security [23]
	Packet decoding and data manipulation [22]	The attacker captures, filters, decodes, and manipulates data packets	
	Sabotage of terminal devices	Causes the battery capacity to be depleted and the key exchange mechanism to be exploited	
6LoWPAN	Sybil attack [24]	The attacker manipulates the node to show multiple pseudo identities for the node, causing the system to be compromised resulting in false alarm. Such an attack is detrimental to distributed environment	Trusted certification, resource testing, recurring fees, privilege attenuation, economic incentives, location/position verification, received signal strength indicator (RSSI)–based scheme, and random key predistribution
	DoS [25]	Smoke screen attack causing security breach of the users' system	Intrusion detection system (IDS) solution, i.e., SVELTE
	Blackhole [26]	Happens when an intermediary captures and reprograms a group of network nodes, the packets are blocked/dropped, and false messages are generated	
	Warmhole [27]	Data packets from a source is tunneled to another location in the network	Regular monitoring of IoT sensors and the network using source routing
	Synchole [28]	This type of attack compromises data confidentiality and interrupt network service by discarding all packets	Message digest algorithm that makes use of cryptography dynamic trust elimination [29]

Table 2 Attacks and possible solutions in network layer

Technology	Attacks	Description	Possible solution
Gateways/Routers/Bluetooth/3G/4G/5G/Wi-Fi	DoS	Attacker floods network with unwanted traffic, causing resource depletion of the targeted system, resulting to inaccessible network	Traffic control, link authentication, active firewalls, and passive monitoring (probing)
	Storage attack [30]	Tempering of users vital data stored in the sensors or on the cloud leading to adversary effect	Backup for storage systems
	Exploit attack	An unethical attack through a set of code over a remote network to exploit software vulnerabilities of all the IoT resources with the intention of taking elevated privileges	
	Malicious code injection [15]	Effects data confidentiality, control flow, and device functionality by introducing a malicious code	Authentication and tamper detection
	Spoofed routing information	An attacker can spoof, alter IP addresses	Active firewalls encryption
	Cross-site scripting	Injection of malicious script into a trusted site,	
	Malicious code attack	It is a harmful script causing security breaches, data theft, and other undesired consequences to the system	

Table 3 Attacks and possible solutions in Application layer

Technology	Attacks	Description	Possible solution
	DoS attacks	Smoke screen attack causing a security breach of the users' system	Secure MQTT solution with ABE
	Gateway attacks [31]	Disconnects the IoT things from the gateway network	Identify a DDos attack early [32]
	Hello flood attack [33]	A node receives a fake HELLO packet broadcasted by attackers, assuming that it within the radio range of the parent node	Bi-directional identity verification protocol for safe communication between the sending and receiving node
	Security patch update problem [34]	Constantly evolving software bug are not being patched	Regular update with software patches/firmwares

4 Counter Measures

In addition to possible solutions listed in the above tables, below are mentioned some of the counter measures. These interventions, however, does not fully eliminate attacks, but they do help minimizes it to a great extent.

4.1 Authentication

Authentication in IoT community allows millions of IoT things to connect for effective and secure communication over an insecure network. The authentication process grants each IoT device in the IoT ecosystem with a unique id that can be authenticated when device attempts to communicate via a gateway or cloud server [35]. However, in IoT device authentication, efficient encrypted key generation and key communication is a challenging task due to lack of guaranteed authorization mechanisms. Authentication is important at any layer of IoT. To prevent DoS attacks, sensor nodes must authenticate themselves at the perception layer. In the network layer Wi-Fi, authentication methods guarantee the security of users' data when it travels over insecure gateway [36]. Security patch update in application layer ensures reliable use of application specific devices. OpenID, a standard open, decentralized framework allows users to be authenticated by relying sites through a third-party provider.

4.2 Authorization and Access Control

Authorization involves security mechanisms to determine users/clients privilege levels to different resources while access control mechanisms guarantees access right of only authorized resources [37]. Installation and regulation of numerous authorization and access control mechanism is a challenge in a heterogeneous IoT network [38]. Authorization controls a device's access throughout the network. Using authentication and access control the relationship between IoT devices is established to exchange appropriate information. OAuth, a standard authorization framework, will grant access to resource, data and features from one application to another through the use of access tokens. However, one challenge encountered by OAuth and Connect is that they have so far only been bound to HTTP, and HTTP is believed to be insecure for communications between IoT devices. Constrained application protocol and MQ telemetry transport are new class of protocols that promises to be better suited than HTTP.

4.3 Secure Architecture

Creating a framework that addresses the aforementioned security issues in an IoT environment is a daunting task. Any IoT architecture should be able to address previously stated security concerns and also the new challenges that comes with installation of IoT devices over software defined networks (SDN) and cloud infrastructure [39], which otherwise will invariably be passed down to the underlying IoT sensors. Furthermore, the difficulties of securely connecting smart IoT objects with cloud services would slew new security risks [40]. Finally, existing intrusion detection and prevention systems face a difficult challenge in detecting malicious traffic rerouted through heterogeneous networks (i.e., SDN, Cloud, and IoT) by unauthorized users [41].

4.4 Block Chain

The Blockchain, an emerging digital technology, has recently gained much popularity in providing secure IoT solutions that can significantly aid in achieving the Internet of Things vision in various ways, such as increasing decentralization capability, promoting interactions, validate new transaction models, and enable autonomous smart objects to seamlessly coordinate through peer-to-peer (P2P) network. The authors in [42] suggests a blockchain-based framework that enables smart devices with single-board computers (SBCs) to communicate with the cloud and send/receive transactions to other internet connected devices on the blockchain network for IoT data in real time. As a proof of concept, experts have conducted simple experiments

using Arduino Uno board and Ethereum smart contracts to demonstrate how the platform can be used for MTM interaction and smart prognosis.

4.5 Cryptographic Algorithm/Encryption

Encryption is used to not only protect the data from being tampered with but also to preserve data confidentiality and integrity. Encryption can be accomplished in either of the two ways: node-to-node encryption or end-to-end encryption. Node-to-node encryption performs cipher text altercation at every node, making the network layer more stable. End-to-end encryption, on the other hand, is performed at the application layer where the recipient decrypts the encrypted data sent by the sender. Mathematical algorithm like cryptographic hash functions authenticates a message by generating message authentication codes (MACs). AES, 3DES, and blowfish are other approved symmetric-key algorithms used for encryption/decryption services covering data breaches and unauthorized disclosure of personal information. Among others Hummingbird, Simon and speck, TEA are suggested light weight cryptographic algorithm providing data security [43].

5 Conclusion

IoT is reshaping the next generation Internet. Beyond laptops and smart phones, the idea of connectivity is expanding towards smart cities, smart transport, smart homes, smart farming, connected vehicles, connected wearables, and connected healthcare among others. With the revolution in the usage of Internet-enabled smart gadget and smart decisions being made in real time, the security concerns has also increased many fold. Research in the field of IoT security is still in its infancy, which needs to be explored further to develop secure solutions for its applications. This survey paper not only elicits and explains in depth, different kind of attacks that occur at all the layer of three layer IoT security protocol stack—perception, networking and application layers—but also provide possible solutions that can be applied at these layers. The article may provide researchers with insight as well as an opportunity to work on developing advanced concepts and techniques to deal with the various attacks that exists in the layered IoT architecture.

Future research will be directed toward addressing the vulnerabilities of communication technologies on all the layers of three-layer IoT architecture and implementing secure authentication and authorization methods using encryption algorithm to prevent data from being tempered. This paper can also aid in doing a comparative study between different layered architecture and understand which would offer better service depending on the application need as a single architecture cannot cater to heterogeneous business requirement.

References

1. H. Suo, J. Wan, C. Zou, J. Liu, Security in the Internet of Things: a review, in *International Conference on Computer Science and Electronics Engineering (ICCSEE)* (2012), pp. 648–651
2. A.M. Sadeeq, et al., Internet of Things security: a survey, in *International Conference on Advanced Science and Engineering (ICOASE)*, Kurdistan Region, Iraq (2018)
3. B.N. Silva, M. Khan, K. Han, Internet of Things: a comprehensive review of enabling technologies, architecture, and challenges, IETE Tech. Rev. 1–16 (2017)
4. M. Farooq, M. Waseem, A. Khairi, S. Mazhar, A critical analysis on the security concerns of Internet of Things (IoT). Int. J. Comput. Appl. **111**, 1–6 (2015)
5. L. Zheng, H. Zhang, W. Han, X. Zhou, Technologies, applications, and governance in the Internet of Things. in*Internet of Things—Global Technological and Societal Trends From Smart Environments and Spaces to Green ICT* ed. by O. Vermesan, P. Friess. (River Publishers, 2011), pp. 141–175
6. H. Eun, H. Lee, H. Oh, Conditional privacy preserving security protocol for NFC applications. IEEE Trans. Consumer Electron. **59**, 153–160 (2013)
7. H. Zhang, Y. Zhang, Architecture and core technologies of Internet of Things. J. Changchun Univ. Technol. (Natural Science Edition) 176–181 (2012)
8. U. Kumar, T. Borgohain, S. Sanyal, Survey of security and privacy issues of Internet of Things. Int. J. Adv. Netw. Appl. **6**, 2372–2378 (2015)
9. S. Ghildiyal, A.K. Mishra, A. Gupta, N. Garg, Analysis of denial of service (DoS) attacks in wireless sensor networks. IJRET Int. J. Res. Eng. Technol. 2319–1163 (2014)
10. A. Mitrokotsa, M.R. Rieback, A.S. Tanenbaum, Classifying RFID attacks and defenses. Inf. Syst. Front. **12**(5), 491–505 (2010)
11. Y. Chen, W. Trappe, R.P. Martin, Detecting and localizing wireless spoofing attacks, in *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks* (2017), pp. 193–202
12. R. Padhy, M. Patra, S. Satapathy, Cloud computing: security issues and research challenges. Int. J. Comput. Sci. Inf. Technol. Secur. (IJCSITS) **1**(2), 136–146 (2011)
13. M. Conti, N. Dragoni, V. Lesyk, A survey of man in the middle attacks, (c). IEEE Commun. Surv. Tutorials **18**, 2027–2051 (2016)
14. P. SaiKiran, E. SureshBabu, D. Padmini, V. SriLalitha, V. Krishnanand, Security issues and countermeaaures of three tier architecture of IOT—a survey. Int. J. Pure Appl. Math. **115**, 49–57 (2017)
15. J. Garcia-Alfaro, J. Herrera-Joancomartí, J. Melià-Seguí, Security and privacy concerns about the RFID layer of EPC Gen2 networks, in *Advanced Research in Data Privacy*, ed. by G. Navarro-Arribas, V. Torra. (Springer International Publishing, 2015), pp. 303–324
16. H.P.T.M. Jayawardana, R.L. Dangalia, Hybrid encryption protocol for RFID data security, in *IEEE International Conference on Decision Aid Sciences and Application (DASA)* (2020)
17. R. Jin, X. Du, Z. Deng, K. Zeng, J. Xu, Practical secret key agreement for full-duplex near field communications. IEEE Trans. Mob. Comput. **1233**, 1–16 (2015)
18. S. Sandhya, K.S. Devi, Analysis of Bluetooth threats and v4.0 security features, in *International Conference on Computing, Communication and Applications, ICCCA* (2012), pp. 1–4
19. J.P. Dunning, Taming the blue beast: a survey of Bluetooth based threats. IEEE Secur. Priv. **8**, 20–27 (2010)
20. S. Sicari, A. Rizzardi, L. Grieco, A. Coen-, Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. **76**, 146–164 (2015)
21. N. Vidgren, K. Haataja, J.L. Patiño-Andres, J.J. Ramírez-Sanchis, P. Toivanen, Security threats in ZigBeeenabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned, in *Proceedings of the Annual Hawaii International Conference on System Sciences* (2013), pp. 5132–5138
22. Y. Zhang, L. Bo, Q. Ma, A secure data exchange protocol for the Internet of Things (2012), pp. 224–225

23. W. Razouk, G.V. Crosby, A. Sekkaki, New security approach for ZigBee weaknesses. Procedia Comput. Sci. **37**, 376–381 (2014)
24. P. Pongle, C. Gurunath, A survey : attacks on RPL and 6LoWPAN in IoT, in *International Conference on Pervasive Computing (ICPC)* (2015), pp. 1–6
25. M.U. Farooq, W. Muhammad, A. Khairi, S. Mazhar, A critical analysis on the security concerns of Internet of Things (IoT). Int. J. Comput. Appl. **111**, 0975 8887 (2015)
26. J. Jiang, Y. Liu, B. Dezfouli, A root-based defense mechanism against RPL blackhole attacks in Internet of Things networks, in *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)* (2018)
27. J. Eriksson, S.V. Krishnamurthy, M. Faloutsos, A practical countermeasure to the wormhole attack in wireless networks, in *Proceedings of the 2006 IEEE International Conference on Network Protocols* (2006)
28. I. Raju, P. Parwekar, Detection of sinkhole attack in wireless sensor network. Adv. Intell. Syst. Comput. **381**, 629–636 (2016)
29. G.W. Kibirige, C. Sanga, A survey on detection of sinkhole attack in wireless sensor network, arXiv preprint arXiv:1505.01941 (2015)
30. S.A. Kumar, T. Vealey, H. Srivastava, Security in Internet of Things: challenges, solutions and future directions, in *Proceedings of the Annual HI International Conference on System Sciences* (2016), pp. 5772–5781
31. R. Zheng, M. Zhang, Q. Wu, C. Yang, An IoT security risk autonomic assessment algorithm. Indonesian J. Electr. Eng. Comput. Sci. **11**, 819–826 (2013)
32. A. Kanuparthi, R. Karri, S. Addepalli, Hardware and embedded security in the context of Internet of Things, in *Proceedings of the 2013 ACM Workshop on Security, Privacy and Dependability for Cyber Vehicles*. (ACM, 2013), pp. 61–64
33. V.A.B.B. Gupta, Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommun. Syst. (2017)
34. L. Kvarda, P. Hnyk, L. Vojtech, M. Neruda, Software implementation of secure firmware update in IoT concept. Adv. Electr. Electron. Eng. **15**(4), 626–632 (2017)
35. F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.-K.R. Choo, et al., An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. J. Netw. Comput. Appl. **89**, 72–85 (2017)
36. R. Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan, Internet of Things (IoT) security: current status, challenges and prospective measures, in *10th International Conference for Internet Technology and Secured Transactions* (2015)
37. E. Bertino, K.-K.R. Choo, D. Georgakopolous, S. Nepal, Internet of Things (IoT): smart and secure service delovery. ACM Trans. Internet Technol. **16**(4), 1–7 (2016)
38. F. Li, J. Hong, A.A. Omala, Efficient certificateless access control for industrial Internet of Things. Future Gener. Comput. Syst. (2017)
39. S. Raza, T. Helgason, P. Papadimitratos, T. Voigt, SecureSense: end-to-end secure communication architecture for the cloud-connected Internet of Things. Fut. Gener. Comput. Syst. (2017)
40. C. Stergiou, K.E. Psannis, B.-G. Kim, B. Gupta, Secure integration of IoT and cloud computing. Fut. Gener. Comput. Syst. (2016)
41. H.H. Pajouh, R. Javidan, R. Khayami, D. Ali, K.-K.R. Choo, A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Trans. Emerg. Top. Comput. (2016)
42. A. Bahga, V.K. Madisetti, Blockchain platform for industrial Internet of Things. Tech. Rep. (2016)
43. S. Surendran, A. Nassef, B.D. Beheshti, A survey of cryptographic algorithms for IoT devices, in *IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (2018)

Intermittent Leather Defect Detection Based on Ensemble Algorithms Derived from Black Hat Transformation and Hough Transformation



Swamiraj Nithiyanantha Vasagam and Madasamy Sornam

Abstract During the leather processing, identification of defect is highly critical because each and every square foot are significant while calculating the value in terms of currency. This process is unaviodable to make decision in the quality of intermittent leather which is predominately carried out by manually. However, it requires to be handled with the involvement of a human expertise, but there could be always risk for human error. To overcome this, a novel method is proposed which has been derived from Black Hat and Hough Transformations. The feature selection is done with the ensemble algorithms. The proposed method exhibits classification accuracy of 94.25% on validation dataset. Further, performance measures such as precision, ROC curve, sensitivity, error rate, specificity, and false positive rate have been reported to verify the effectiveness of the proposed approach.

Keywords Intermittent leather · Black hat transformation · Hough transformation · Ensemble algorithm · Support vector machines

1 Introduction

The definition of leather is based on the requirement that it must be made from the intact hide or skin of an animal [1]. The popularity of leather is based on the way it feels, the way it looks, the way it interacts with and moulds to the body, the way it wears in use, and even the way it smells. The aesthetics of leather ensure it is likely to remain the preferred material of choice for many modern applications: shoes, clothing, upholstery, belts, handbags, etc. Grain pattern of the follicles on the surface of the skin or leather: It characterizes the leather, and it is a prized feature [2, 3]. However, this is carried out only by a well experienced person from the industry, and there is no fully analytical method has been devised for the crust or intermittent leather [6]. Hence, the end result will vary between one expert to another

S. N. Vasagam · M. Sornam (✉)
University of Madras, Chennai 600025, India

S. N. Vasagam
CSIR-Central Leather Research Institute, Chennai 600026, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_4

expert. Moreover, the sales associated wiht the export value is depend on the experts opinion of the intermittent leather. Crust or intermittent leathers usually assorted by only exports by manual intervention, and it is a tedious process and exports does meticulously checking based on the position and distribution of the irregularity of the color on the surface. In order to overcome the traditional practice, it is proposed a novel approach in distinguishing the crust or intermittent leather to support the experts while making the decision.

2 Literature Review

Krastev et al. [4] have investigated histogram and measures of statistical inference for leather surface images analysis. They have concluded that feature set of most appropriate for leather surface defect detection based on the values of median, histogram, and mean. Viana et al. [5] were reported that using the parameter simulated annealing the accuracy of classification significantly configured the LIBSVM and Weka SMO. Yeh et al. [6] have proposed a machine vision based on semi-automatic method to classify and grade wet blue hides to measure the surface defect areas unusable.

He et al. [7] have reported an efficient algorithm for detection of defects embedded using multiresolution energy, approach, and entropy matrices in leather surface images. They have also separated the defective regions through adaptive binary thresholding in the restored image from the uniform gray-level background. Amorim et al. [8] have reported that reduction during the leather defect classification by comparing of five discriminant analysis techniques like CLDA, FisherFace, YLDA, KLDA, and DLDA using four different classifiers, namely Naíve Bayes, C4.5, support vector machines and kNN. Kwak et al. [9] have introducted a system to surface defects detection on leather fabric in a gray-level image had reported through morphological processing, thresholding and their geometric information.

Vasagam et al. [10] have presented an insight on crust leathers of defects identification using computer-aided grading. Sornam et al. [11] have proposed a model to group the intermittent leather images using linear discriminant model among the categories between normal leather and defective leather.

The majority of the research in this field is done in classifying the images on the basis of surface level as indicated in the Table 1 and which confirms the importance in studying the images on surface. Accordingly, in our research, the authors propose a new feature extraction method using leather image surface feature extraction [LISFE] in the intermittent leather images which is derived from Black Hat transformation and Hough transformation. We also proposed to use ensemble algorithms, support vector machine in feature selection and classification. The contributions to this manuscript can be summarized as follows:

– Collection of crust or intermittent leather images
– Pre-processing based on de-noising and followed to with edge detection technique

Table 1 Techniques discussed in literature review

S. No	Authors	Name of the technique or method
1	Krastev et al. [4]	Second-Order Statistics and Histogram
2	Viana et al. [5]	Support Vector Machines
3	Yeh et al. [6]	Semi-Automatic Machine Vision Method
4	He et al. [7]	Adaptive Binary Thresholding
5	Amorim et al. [8]	Discriminant Analysis Techniques, Naíve Bayes and SVM
6	Kwak et al. [9]	Thresholding and Morphological Processing
7	Vasagam et al. [10]	Computer Aided Grading
8	Sornam et al. [11]	Linear Discriminant Model

– A novel leather image surface feature extraction [LISFE] method is proposed which is derived by Black Hat and Hough Transformations
– Feature selection using ensemble algorithm such as random forest and gradient boosted regression treess
– Classification using support vector machines

The remaining work is organized of this manuscript as follows. Section 3 details of various methods such as pre-processing, ensemble algorithm, and classification. Section 4 details the proposed method. Presenting the architecture of our proposal, including a detailed description of the image analysis methods, as well as the classification component. In Sect. 5, we introduce the datasets used, a description of the conducted experiments, and discuss the results. Finally, Sect. 6 presents a conclusion.

3 Details of Various Techniques

This chapter covers the various techniques covering from pre-processing to classification.

3.1 De-noising

Image denoising is the technique to remove noise from an image and also to estimate the noise-contamination so as to restore the original or true image. Traditional filters like spatial filters and transform filters are predominantly used in images to remove noise and in which wiener filter and wavelet transform are popular image denoising techniques [12, 13]. However, Wiener filter is use statistical approach to remove

noise through signal (Eq. 1), and Wavelet transforms also removes based on statistical approach.

$$W(m,n) = \frac{H*(m,n)S_g(m,n)}{||H(m,n)||^2 S_g(m,n) + S_p(m,n)} \tag{1}$$

3.2 Edge Detection Technique

In computer image vision, pointing out the true edges are vital in obtaining the best significant results during the matching process. Shrivakshan et al. [14] have observed the advantages and disadvantages of filters such as Canny edge detector, Laplacian-based edge detector and gradient-based Roberts along with Sobel and Prewitt edge detection operators. Maini et al. [15] have observed that computationally the Canny's edge detection algorithm is more expensive among the Sobel, Prewitt, LoG (Laplacian of Gaussian), and Robert's operator.

3.3 Black Hat Transformation

Morphological process which thickens the edges of the final image while appling to the input image. To understand the thickens at small element level, Black Hat transformation operarions can be used as stated in Eq. (2) to process morphologically to definethe difference between the final and the input image [16].

$$dst = blackhat(S,E) = close(S,E) = close(S,E) = dilate(erode(S,E)) \tag{2}$$

where, S—Source and E—Element.

3.4 Hough Transformation

Hough transformation technique is applied of a particular shape in image to isolate features. Baygin et.al. [17] have applied in identification of holes along with marking the identified holes as per the pseudo code given below.

```
For each PX (p,q)
    For each R r=10 to r=60
        For each T t=0 to t=360
            aa = p – r * cos(t * pi/180)
            H[aa,b,r] += 1;
        End
    End
End
```

Where PX is defined as PIXEL, R is defined as radius, and T is defined as Theta

3.5 Ensemble Algorithm

Ensemble methods are models with consisting of multiple weaker models to make the prediction in overall. Dong et al. [18] have reviewed learning of ensemble and classified based on different characteristics on the research progress of the mainstream approaches. Friedman [19]. Stochastic gradient boosting. Feature selection using ensemble algorithm (Random Forest & Gradient Boosted Regression Trees). Song et al. [20] have achieved the best performance with gradient boosting machine (GBM). Verma et al. [21] have applied machine learning algorithms to categorize classes of skin disease using ensemble techniques. Saeys et al. [22] have shown great promising result, while investigating the usefulness of ensemble feature selection techniques. Yadav et al. [23] have identified that feature selection methods Pearson correlation and Lasso regularization with random forest ensemble method.

3.6 Classification Method

Support vector machines (SVM) are that used to analyze data including regressiong and classification. Ogunlana et al. [24] have classified the recognition of fish for its commercial and agricultural usefulness. Singh et al. [25] have suggested a real-time forecasting model to predict among the various cases such as confirmed, deceased, and recovered case duing the investigation of the novel Corona Virus Disease 2019.

4 Proposed Method

4.1 Architecture

The proposed method is composed of three stages: pre-processing, proposed model for feature extraction and feature selection and classifications. The entire architecture of the method can be seen in Fig. 1a.

4.2 Pre-processing

Initially, the authors have applied Wiener filter to remove noise on the original image, and subsequnetly, Canny edge detector is adopted to narrow down further on the image in identifying the edges as shown in Fig. 2.

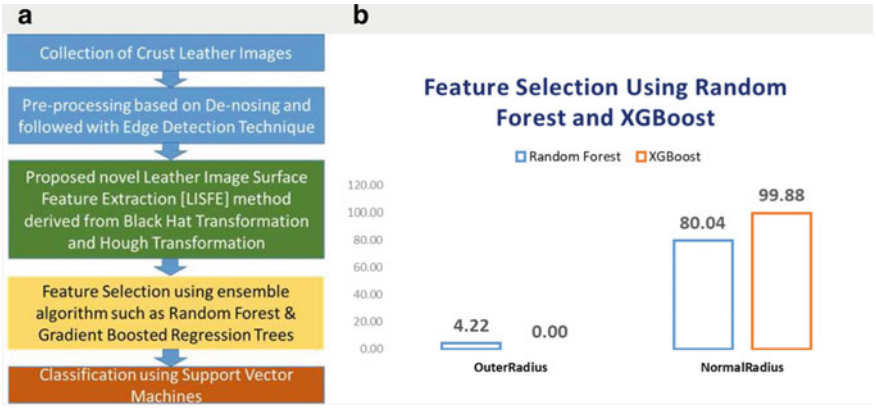


Fig. 1 **a** Workflow and **b** Feature selection

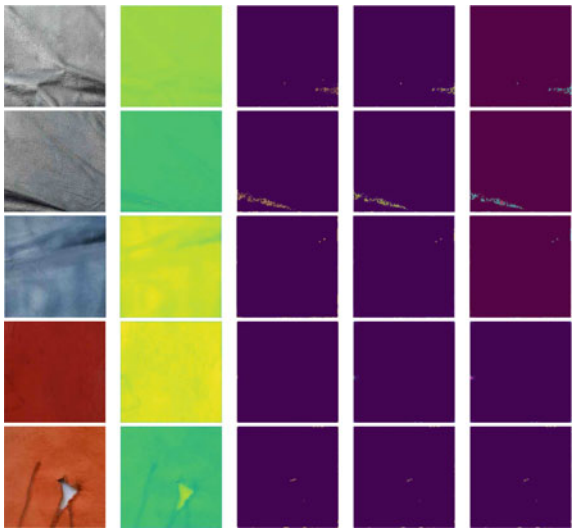


Fig. 2 Actual Image to De-noising to Edge Detection to thickening to narrow down the identication

4.3 Proposed Model for Feature Extraction

A novel model called leather image surface feature extraction [LISFE] method is proposed by morphological process through thickening the image which is derived from the image dataset by combining Black Hat transformation and Hough transformation and generation of a new dataset following to which the isoloation of defect is processed by taking into consideration of a vector that stores sets of three values, namely radious associated with the respective rows and columns. In this process, the minimum distance between the detected circle at rows/16.

$$C = C(RowCenter, ColumnCenter, R) \tag{3}$$

where C is Circle, RC is Row Center, CR is Column Center and R is Radius.

4.4 Feature Selection and Classifications

The features of Outer Circle, Outer Radius, Normal Count, Inner Circle, and Inner Radius for the respective images have been generated. The ensemble algorithms like random forest and XGBoost are employed in finding out the suitable features. Support vector machine classifies on data points and generates significant accuracy having less computation and is employed to understand the various performance metrices. Further, in the confusion matrix (CM), each and every value in the column represents the actual number of class of classification instances similarly each and every value in the row represents the predicted class of instances for defective leather and non-defective leather. It basically represents the four outcomes of binary classification is a 2×2 matrix which denotes true positive of true classification of defect leather (TPTCDL), false negative of false classification of non-defect leather (FNFCNDL), false positive of false classification of non-defect leather (FPFCNDL), and true negative of true classification of defect leather (TNTCDL) by which various performance measures such as sccuracy Eq. (4), precision Eq. (5), recall Eq. (6), specificity Eq. (7), error rate (8), false positive rate (9), and F1-score Eq. (10) are computed.

$$Accuracy(A) = ((TPTCDL+) + (TNTCDL))/TotalValue \tag{4}$$

$$Precision(P) = (TPTCDL)/((TPTCDL) + (FPFCNDL)) \tag{5}$$

$$Recall(R) = (TPTCDL)/((TPTCDL) + (FNFCNDL)) \tag{6}$$

$$Specificity(S) = (TNTCDL)/((TNTCDL) + (FPFCNDL)) \tag{7}$$

$$ErrorRate = ((FPFCNDL) + (FNFCNDL))/TotalValue \tag{8}$$

$$FalsePositiveRate = ((FPFCNDL)/(TNTCDL + FNFCNDL)) \tag{9}$$

$$F1 - score(F1) = 2x((Recall * Precision)/(Recall + Precision)) \tag{10}$$

5 Results and Discussion

5.1 Dataset and Image Details

Images of size 300 × 300 have been collected with 96 dpi for training and testing dataset consisting, respectively, of 142 and 383 images with defects and non-defects. The images are respectively taken into further processing as Wiener filter for denoising, Canny Edge fo edge detection, Black Hat transformation for thickening, and Hough transformation to narrow down the identication of defect areas and the same as per the Fig. 2 for five images. Subsequently, the features of Outer Circle, Outer Radius, Normal Count, Inner Circle, and Inner Radius for the respective images have been generated to understand the defect and non-defect of the intemittent leather images. The ensemble algorithms like random forest and XGBoost are employed in finding out the suitable features. Both the algorithms recommend Normal Count which is derived from Normal Radius for the further image classification as shown in Fig. 1b).

The values of Outer Radius, Normal Count, and Inner Radius for the above images are shown in the Table 2 which confirms the position of the pixel corresponding to the row and column of the particular detection.

5.2 Performance Measures

According to the analysis of various performance measures connected to classification of defects versus non-defects, two common measures derived from confusion martix are accuracy and error rate confirms the better results. The score of correct classificaion of defected leather is laid in true positive, and the score of incorrect classification of defected leather falls under false postive. Similarly, the correct and incorrect classification of non-defects can be clearly observed under true negative and false negative. By taking into consideration of correct versus incorrect binary collection for defect versus non-defect in 2 × 2 matrix, the accuracy score for training, testing, and validation datasets are computed, respectively, as 99.29%, 94.51%, and

Table 2 Values of radius and normal count

S. No	Outer radius	Outer radius	Normal count
1	0	0	0
2	3	1	4
3	3	0	0
4	2	1	3
5	0	0	0

Table 3 Comparison of training dataset

Metrics	Training	Testing	Validation model
SVM Accuracy	99.29	94.51	94.25
Precision	99.29	94.5	94.25
Sensitivity	1	1	1
Specificity	NA	50.0	4.54
F1-score	99.64	97.17	97.04
Error Rate	0.70	5.48	5.74
False Positive Rate	NA	5.0	95.45

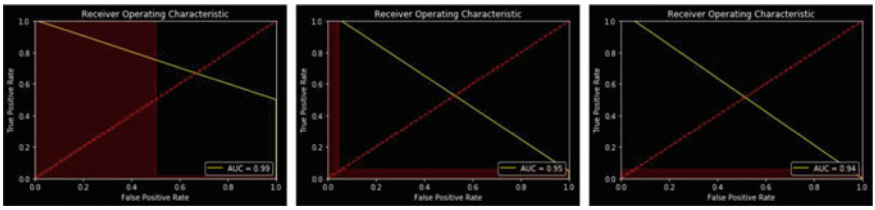


Fig. 3 ROC for datasets of training, testing and training versus testing

94.25%. The results of the SVM confirm that validation model of proposed method shows an accuracy level of 94.25% as shown in Table 3.

Similarly for the error rate is 0.7, 5.48, and 5.74, respectively, for the datasets training, testing, and validation which are also confirms the prediction is in acceptable range. With respect to the measures precision and sensitivity, this two measures confirms the best, and other measures such as specificity and false positive rate are also confims the better for testing and validation datasets. Meanwhile, the receiver operating characteristic (ROC) plots true positive rate versus false positive rate of different classification thresholds. ROC curve, as shown in Fig. 3, is also confirms that the results are in positive trend as 99, 95, and 94, respectively, for for the datasets training, testing, and validation.

6 Conclusion

During the leather processing, identification of defect is highly critical because each and every square foot is significant while calculating the value in terms currency. In this manuscript, the authors have presented a novel method which has been derived from Black Hat and Hough transformations in classifying the images as defect and non-defect, and the proposed method exhibits 99.29% classification accuracy on the train data and 94.51% on the test data. The results of the performance measures confirm that validation model of proposed method shows an accuracy level of 94.25%.

Further, the effectiveness of the other measures such as ROC curve, F1-score, precision, and specificity and Sensitivity are also confirms effectivens in the defect classification.

Acknowledgements The authors are thankful to University of Madras, Chennai, India and CSIR-Central Leather Research Institute, Chennai, India. The authors would like to sincerely acknowledging the support extended from Tanners Association. The authors also acknowledge the CSIR-CLRI Com. No. 1555.

References

1. British Standard Glossary of Leather Terms, British Standards Institution, BS 2780 1983
2. Tanning Chemistry: The Science of Leather By Anthony D. Covington; Royal Society of Chemistry, Technology & Engineering—520 pages (2015)
3. S. Harris, A.J. Veldmeijer, *Leather* (Sidestone Press, Leiden, 2014)
4. K. Krastev, L. Georgieva, N. Angelov, Leather features selection for defects recognition using fuzzy logic. Energy **2**(3), 1–6 (2004)
5. R. Viana, R.B. Rodrigues, M.A. Alvarez,H. Pistori, SVM with stochastic parameter selection for bovine leather defect classification, in *Pacific-Rim Symposium on Image and Video Technology* (Springer, Heidelberg, 2007), pp. 600–612
6. C. Yeh, D.B. Perng, Establishing a demerit count reference standard for the classification and grading of leather hides. Int. J. Adv. Manufacturing Technol. **18**(10), 731–738 (2001)
7. F.Q. He, W. Wang, Z.C. Chen, Automatic visual inspection for leather manufacture, in *Key Engineering Materials* (Vol. 326, Trans Tech Publications Ltd, 2006), pp. 469–472
8. W.P. Amorim, H. Pistori, M.C. Pereira, M.A.C. Jacinto, Attributes reduction applied to leather defects classification, in *2010 23rd SIBGRAPI Conference on Graphics, Patterns and Images*. (IEEE, 2010), pp. 353–359
9. C. Kwak, J.A. Ventura, K. Tofang-Sazi, A neural network approach for defect identification and classification on leather fabric. J. Intelligent Manufacturing **11**(5), 485–499 (2000)
10. S.N. Vasagam, B. Madhan, B. Chandrasekaran, J.R. Rao, Studies on selective defect identification of crust leathers for computer-aided grading. J. Am. Leather Chem. Assoc. **108**(06), 210–220 (2013)
11. M. Sornam, S.N. Vasagam, Surface defect identification and grouping of intermittent leather images using linear discriminant model. Int. J. Innov. Technol. Exploring Eng. **8**(12), 2253–2259 (2019)
12. S.K. Mohideen, S.A. Perumal, M.M. Sathik, Image de-noising using discrete wavelet transform. Int. J. Comput. Sci. Netw. Security **8**(1), 213–216 (2008)
13. P. Patidar, M. Gupta, S. Srivastava, A.K. Nagawat, Image de-noising by various filters for different noise. Int. J. Comput. Appl. **9**(4), 45–50 (2010)
14. G.T. Shrivakshan, C. Chandrasekar, A comparison of various edge detection techniques used in image processing. Int. J. Comput. Sci. Issues (IJCSI) **9**(5), 269 (2012)
15. R. Maini, H. Aggarwal, Study and comparison of various image edge detection techniques. Int. J. Image Process. (IJIP) **3**(1), 1–11 (2009)
16. D.J. Graham, I. Reid, S.P. Rice, Automated sizing of coarse-grained sediments: image-processing procedures. Math. Geol. **37**(1), 1–28 (2005)
17. M. Baygin, M. Karakose, A. Sarimaden, A.K.I.N. Erhan, Machine vision based defect detection approach using image processing, in *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)* (IEEE, 2017), pp. 1–5
18. X. Dong, Z. Yu, W. Cao, Y. Shi, Q. Ma, A survey on ensemble learning. Front. Comput. Sci. **14**(2), 241–258 (2020)

19. J.H. Friedman, Stochastic gradient boosting. Comput. Statistics Data Anal. **38**(4), 367–378 (2002)
20. X. Song, L.R. Waitman, Y. Hu, A.S. Yu, D. Robins, M. Liu, Robust clinical marker identification for diabetic kidney disease with ensemble feature selection. J. Am. Med. Informatics Assoc. **26**(3), 242–253 (2019)
21. A.K. Verma, S. Pal, S. Kumar, Comparison of skin disease prediction by feature selection using ensemble data mining techniques. Informatics Med. Unlocked **16**, 100202 (2019)
22. Y. Saeys, T. Abeel, Y. Van de Peer, Robust feature selection using ensemble feature selection techniques, in *Joint European Conference on Machine Learning and Knowledge Discovery in Databases* (Springer, Heidelberg, 2008), pp. 313–325
23. D.C. Yadav, S.A.U.R.A.B.H. Pal, Prediction of heart disease using feature selection and random forest ensemble method. Int. J. Pharmaceutical Res. **12**(4) (2020)
24. S.O. Ogunlana, O. Olabode, S.A.A. Oluwadare, G.B. Iwasokun, Fish classification using support vector machine. Afr. J. Comput. ICT **8**(2), 75–82 (2015)
25. V. Singh, R.C. Poonia, S. Kumar, P. Dass, P. Agarwal, V. Bhatnagar, L. Raja, Prediction of COVID-19 corona virus pandemic based on time series data using Support Vector Machine. J. Discrete Math. Sci. Cryptography, 1–15 (2020)

Efficient Strategies to Manage Road Traffic Using Big Data Analytics



Yogesh Golhar and Manali Kshirsagar

Abstract The on-road traffic increases due to the exponential growth of the number of vehicles on the road. That leads to undesirable road conditions and makes urban population life uncomfortable. It includes traffic congestion, traffic jams, and long queues at traffic signals and toll booths. Many people violate road traffic rules and regulations rules every day. Manual human effort and supervision are not enough to resolve these issues. Still, many road traffic managements follow the traditional approach, which results increase in road accidents that makes humans seriously injured and even loss of life. To address these issues, we have proposed four strategies as (1) congestion status on square, (2) efficient toll tax collection, (3) fine collection on road for the people who violate road traffic rules and (4) shortest pathfinder for drivers. This research work mainly focuses on the various strategies and their implementation with the help of the MapReduce framework. We have combined video surveillance, big data analytics algorithm and implemented efficient road traffic management system.

Keywords Big data · Congestion degree · HDFS · Hadoop · Video surveillance

1 Introduction

In India, travel by highway is risky because of two reasons: (1) due to road conditions and (2) irresponsible behavior of drivers on road leading to accidents. India is at the top position in the world in traffic-related deaths. In other countries like the USA people suffered from severe traffic accidents in recent times. Everyone should be more careful when crossing streets, even in imprinted pedestrian zones, and try to practice only vehicles that have seatbelts. Seat belts are not common in taxis. Helmets should be used by every motorcycle and bicycles drivers. Travel in the evening

Y. Golhar (✉)
Department of Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra 441110, India

M. Kshirsagar
Yeshwantrao Chavan College of Engineering (YCCE), Nagpur, Nagpur, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_5

is especially dangerous. Buses are habituated by hundreds of millions of Indian people. However, they are mostly driven fast, carelessly and without consideration for the rules and regulations of the road. Accidents are quite obvious. Trains are safer than buses, but train accidents still occur more frequently than in other countries in the world. Hence, there is a need of efficient traffic management system in India and other countries. Current traffic management system is manual. Human traffic controller monitors and manage the on-road traffic in India. At many places, the surveillance camera are used to monitor the traffic and capture traffic rules and regulation scenarios. But not all the roads are under surveillance in India. Existing on road traffic surveillance cameras-based traffic management system have different issues and challenges such as huge traffic record management, active surveillance missing on road because in current system, no automated fine collection module is not included. It is getting enhanced day by day in India. Recently, traffic control management organization in India comes with the initiative of FastTrack system on toll booth. It is used for the collection of tax on toll booth for avoiding the long queue on the road. In FastTrack system, every vehicle has their own unique QR code attached with the account. Whenever, the vehicle comes on toll both, the camera on the toll booth mounted on the top scanned the QR code of vehicle. Then amount is automatically deducted from the account without any human involvement. But, issues with FastTrack system include (1) vehicle and camera mounted camera calibration, position of vehicle should be appropriate to capture the QR code on vehicle. (2) Quality of camera on toll booth is poor. Sometimes it is difficult for vehicle driver to position the vehicle on the toll booth. We try to address these issues with our proposed strategies of traffic management using big data analytics. In proposed work, we have come with four efficient strategies to overcome the existing system drawbacks. The proposed framework utilized the MapReduce framework to manage the traffic big data efficiently. The four strategies include (1) traffic status on the road based on the congestion degree, (2) efficient toll tax collection, (3) fine collection on road for the people who violate road traffic rules, (4) shortest pathfinder for drivers. We think that the proposed implementation will be helpful in the urban environment for efficient traffic management. The remaining paper is organized as follows. Section 2 represents existing strategies available for road traffic management with its advantage and limitation. Section 3 describes the proposed strategies for road traffic management. Section 4 discusses the experimental results and comparison of existing strategies with proposed approach. The last section concludes with a future research direction.

2 Literature Survey

Nowadays, due to better standard of living and employment opportunities, the urban cities have become a center of attractive living places, and the world is seeing an increasing inclination of the rural population moving over to urban cities. Up to 2025, about 70% of the global population is expected to live in cities [1]. The National Smart

Cities Mission of India reveals a budget of $160 billion for the next five years to enhance the 100 smart cities of the country [2, 3]. In [4], proposed a hybrid approach that combines a centralized and decentralized approach to enhance and optimize traffic flow on highways. The system gathers traffic density information as input from different surveillance camera or sensors, and manages traffic signals automatically. For this purpose, it will utilize a cloud server to store the captured and processed images and data. Hence, there is a risk of single source failure. However, change in illumination, temperature variation, overcast condition and humidity affects the traffic density values which is based on the weather situation. In [6], proposed adaptive control system to control traffic light of roads. In this system, based on on-road traffic condition, traffic light color changes adaptively. Due to this, long queue on signal get reduced, the drivers can always take the lowest estimated waiting path for reaching destination. In this system, if all the drivers select or opts for the same route, the optimal and less time-consuming path becomes overcrowded and thus, the system may become inefficient for all. In [7], proposed improved traffic management system by taking into consideration of the uncertain and unpredictable behavior of traffic flow. In [8] proposed a remote location one fingertip mobile application and cloud-based traffic management system. The system uses the intelligent traffic monitoring and navigation system using formal methods and graph theory techniques. This system works efficiently when the on-road traffic is heavy, and this system will be more effective as manual traffic management system does not work well in emergency situations. Further, the drivers notified with the alternative path notification to reach to their destination in case of special timings. Again, if all the drivers select or opts the same path, the route may be congested. In [9], proposed a service-based intelligent transportation system framework to manage heavy traffic scenarios, providing efficient road traffic flow scenarios, and systematic accident management and providing reliable information. In [10], proposed a RFID-based intelligent traffic management system that creates a map of shortest time paths for the whole city. These include vehicle type, frequency, number plate detection, average speed of vehicles and lane occupancy information, etc. [11]. The limitation of this is misclassification of traffic jam scenarios due to in-accurate vehicle of GPS location. In [14], author has proposed an Intelligent Video System (IVS) Framework with Massive Data Management for Indian Road. The limitations of this approach include (1) not suitable for large-scale deployment, (2) misclassification of traffic jam scenarios due to in-accurate vehicle localization. Due to existing system limitation in real-time environment, it is observed that there is a need of efficient traffic management system to handle the current traffic scenarios in the urban environment.

3 Proposed Methodology

The proposed approach is divided into three parts as (1) efficient framework for road traffic data acquisition using the video camera, (2) collection of traffic information from road traffic video surveillance camera (1) and (3) process the traffic data in the

HDFS using the MapReduce framework. The proposed system is categorized into two area: A. video processing/analysis, i.e., preprocessing of video footages and B. storage of data in HDFS and analyzing it using Hadoop to find the congestion degree. Pre-requisite for this project: implementing camera for recording traffic information on various prominent location. This will detect the types of vehicles, vehicles speed, then calculating a congestion degree. Implement a complete system for vehicle registration system with various other modules, such as vehicle registration, fine collection system, toll tax collection and shortest path.

3.1 Video Analysis

The vehicle in a video detected and classified using the vehicle detection and classification algorithm. It uses HAAR cascade classifier [16]. It describes in brief as follows.

Algorithm 1: Vehicle Detection and Classification

Step 1: a. Input Video and divide it into frames (25 frames per second).
b. Initializing total count, bike, car, bus = zero.

Step 2: By using HAAR cascade algorithm following information is extracted

$$\int (x, y, w, h)$$

Step 3: Draw a rectangle around the identified moving object in each frame using

$$(x_1, y_1), (x_2, y_2) \text{where } x_2 = x_1 + w, y_2 = y_1 + h$$

Step 4: Finding the centroid $C = \left(x_1 + \left(\frac{w}{2}\right)\right), \left(y_1 + \left(\frac{h}{2}\right)\right)$.

Step 5: Input the training set for cascade classifier

Step 6: Frame by frame reading of video

Step 7: Identifying region/area of each lane where each vehicle can be detected defined as spatial coordinate

Step 8: if the length of rectangle is not equal to zero then, Vehicle exists, increment the total count of vehicle.

If area of the rectangle is less than 10,000 classified it as bike.
If area of the rectangle is 10,000–17,000 classified it as car.
If area of the rectangle is greater than 17,000 classified it as truck/bus.

Step 10: Repeat step 2 to 9 for each video input otherwise Exit.

Step 11: End

3.2 Storage of Data in HDFS and Congestion Degree Computation

The extracted parameter in algorithms is used by Mapper Reducer function in HDFS for processing data in Hadoop. The congestion degree is computed to get the current status of traffic state using following algorithm.

Algorithm 2: Computation of Congestion Degree

Step 1: [Initialization and consideration]

Let,

Total number of vehicles on road → *Tvr.*

Average speed → *ASvr* for every 5 min.

Stationary vehicles → *Sv.*

Road speed → *Rs* (Actual road speed without congestion).

Running vehicles → *Rv.*

Average speed → *As.*

Step 1: When finding the average speed of vehicles out of total vehicle's.

Rv → *Tvr* – *Sv.*

(if R_{veq} Sv that means traffic is fully congested else go to step 2).

Step 2: Finding the average speed of road only for moving vehicles.

As = *Average * speed (Rv).*

Step 3: Congestion degree → *(Rs- As)/Rs.*

The above congestion degree is calculated every 5 min and stored it in HDFS, i.e., in 1 h, there will be 60/5 = 12 entries, and for every 24 h, there will be 12*24 = 288 entries; now, historical trends are calculated for every 24 h and peak hours are decided for that road with the vehicle carrying capacity output is shown in the following example. The decision tree and above data can now identify the congested areas/timing/peak areas of the congestion that will occur. All the above process runs in Hadoop in the form of Mapper and reducer function. Next, we have detected the number plate of vehicle and obtain the vehicle's unique vehicle number extracted from the number plate. The extracted traffic information from the input source is processed in HDFS. First, the input data is uploaded in the HDFS in the forms of clusters; later, the data is divided into key value pair at different nodes using Mapper function. Then, it is shuffle in next stage before reducer process the input data. At the end, the Reducer function group together the homogeneous data into different categories with respective to the key value pair. The consolidated result is obtained at the end without any ambiguity (Fig. 1).

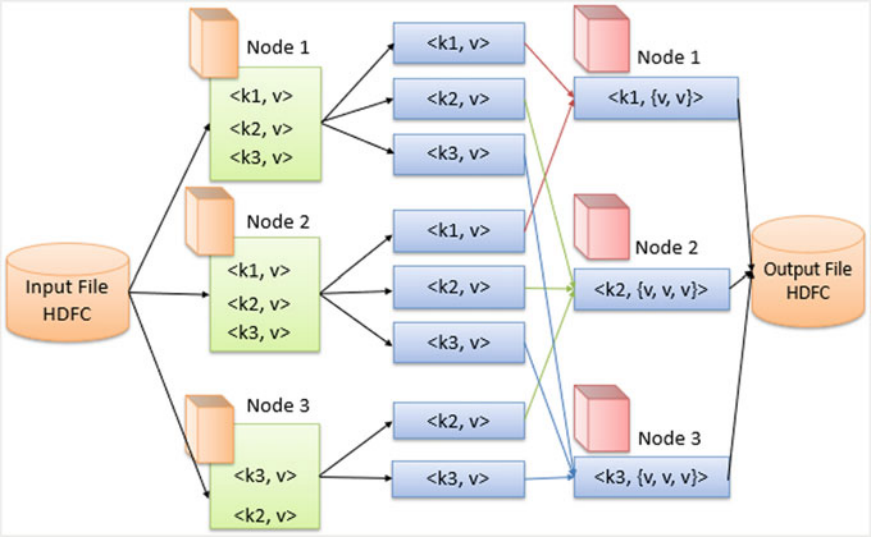


Fig. 1 MapReduce framework of proposed system

The proposed system uses the Hadoop environment to process the input data. The processed output results in traffic jam or no traffic jam as shown in Fig. 2. The input source information include speed, vehicle category, congestion degree, road average speed, congestion status, geolocation of vehicle, etc. The Mapper Reducer function

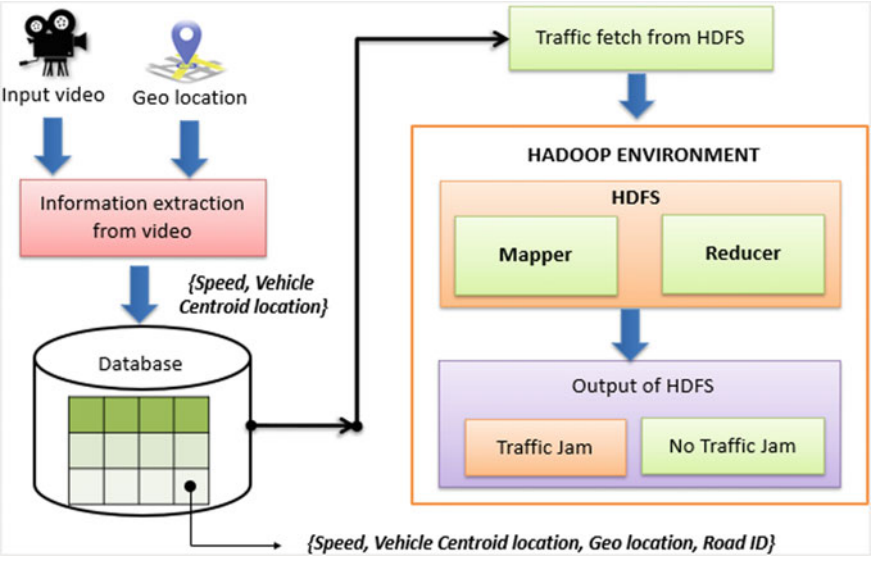


Fig. 2 Proposed system architecture

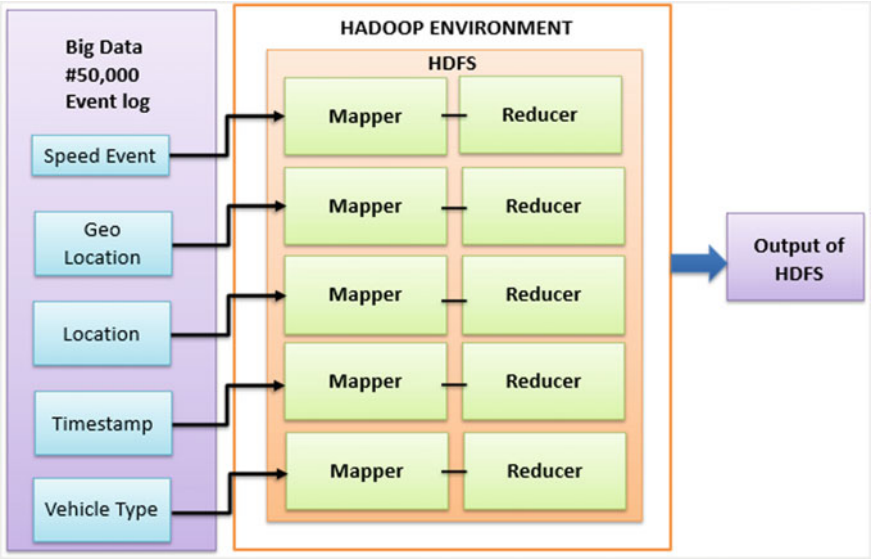


Fig. 3 HDFS input data process using MapReduce framework

designs in such a way that it will process all of these parameters at once in Hadoop distributed environment. Figure 3 shows the Mapper Reducer function utilized for the different traffic log information.

The Mapper Reducer function is used for the traffic state detection at the end. Later, all of the processed data visualized on the Map using geolocation. The toll tax collection and fine collection mechanism is implemented on cloud platform, in which detected number plate and other driver related information are stored in database and all the status of collected fine or toll tax visualize on the map using geolocation. The shortest path routing navigation feature also embedded in the framework for finding the shortest routing path between different locations. In the next section, we have described all the experiments conducted.

4 Experimental Results

Traffic data collected from the densely populated traffic area of the city of Nagpur, Maharashtra. Figure 4 shows the camera setup to capture traffic footage of different traffic lane. The camera placed at the top position in different angles over the bridge 5°, 20° and 25° from the base location. The road distance from the camera is 25 m. The camera placement is done in such a way that it captures the incoming and outgoing vehicle in two different directions. Next, the proposed algorithm is applied on the region of interest to identify the type and speed of the vehicle, which is processed in HDFS using double MapReduce framework on batch of job. The camera is manually

Table 1 Comparative analysis of proposed traffic management system with the state-of-the art approaches

Name of author	Algorithms/methodology	Dataset	Time complexity (s)
Caárdenas-Benítez et al. [12]	Traffic event detection algorithm, route monitoring algorithm	SUMO event logs	20
Gupta et al. [13]	Identification of on-road clusters algorithm, binary traffic output algorithm	GPS enabled devices data	19
Rajagopal et al. [14]	Intelligent video systems (IVS) in big data	Video data	15
Hamilton [15]	Traffic event detection using MapReduce	Apache Flume	25
Proposed approach	Traffic event detection algorithm	Video data real time data	10

recording the incoming and outgoing vehicles on the various location of the road. The database consists of all the traffic log and event details. The proposed approach compares with the existing approach based on the time complexity. It is observed that the proposed approach requires less time compare to the approach of [12–14] and [15]. The four strategies are useful for efficient traffic management. The result comparison of proposed system with the existing approaches is shown in Table 1.

5 Conclusions and Future Work

In this paper, we proposed the framework traffic event detection system for Indian traffic control system. We have proposed four different strategies as (1) congestion status on square, (2) efficient toll tax collection, (3) fine collection on road for the people who violate road traffic rules, (4) shortest pathfinder for drivers. This research work mainly focuses on the various strategies and their implementation with the help of the Mapreduce framework for efficient traffic management in urban cities of India. The proposed system used Hadoop distributed platform and the Mapper Reducer function for the implementation. It will help in managing big data efficiently. Experiment results shows that the time required is less compare to the existing system, and the proposed strategies are needed for the current state-of-the art traffic management system. In future, it will be extended by adding other strategies such as adaptive traffic signal management, mobile computing platform for the ease of users and traffic management authority.

References

1. R. Dobbs, S. Smit, J. Remes, J. Manyika, C. Roxburgh, A. Restrepo, Urban world: mapping the economic power of cities. Mc. Global Insti. Rep. 1–7 (2011)
2. N. Abbu, L. Bhagavatula, A.R. Ghorpade, *Urban Green Growth Strategies for Indian Cities*, vol. 1. (Local Governments for Sustainability, South Asia, 2015)
3. S.V. Nandury, B. Beneyaz, Smart WSN based ubiquitous arch. for smart Cities, in *International Conference on Advances in Computing, Communications and Informatics*, Kochi, Kerela (2015), pp. 2356–2363
4. S. Javaid, A. Sufian, S. Pervaiz, M. Tanveer, Smart traffic management system using Internet of Things, in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, Chuncheon-si, Gangwon-do, Korea (South), February 2018, pp. 393–398
5. K. Swathi, V. Sivanagaraju, A.K.S. Manikanta, D. Kumar, Traffic density control and accident indicator using WSN. Int. J. Mod. Trends Sci. Technol. **2**(4), 2455–3778 (2016)
6. M. Wiering, J. Veenen, J. Vreeken, A. Koopman, Intelligent traffic light control, Technical report, Department of CS, Universiteit Utrecht, 9th July 2004, pp. 1–30
7. S. Calvert, H. Taale, Improving traffic management through consideration of uncertainty and stochastics in traffic flow. Case Stud. Transp. Policy **6**(1), 81–93 (2018)
8. S. Kim, Kim, J.H. Park, Traffic management in the mobile edge cloud to improve the quality of experience of mobile video. Comput. Commun. **118**, 40–49 (2018)
9. S. Latif, H. Afzaal, H.A. Zafar, Intelligent traffic monitoring and guidance system for smart city, in *International Conference on Computing, Mathematics and Engineering Technologies* (2018), Sukkur, pp. 1–6
10. H.Y. Liu, E. Skjetne, M. Kobernus, Mobile phone tracking: in support of modelling traffic-related air pollution contribution to individual exposure and its implications for public health impact assessment. Environ. Health **12**(1) (2013)
11. P. Manikonda, A.K. Yerrapragada, S.S. Annasamudram, Intelligent traffic management system, in *2011 IEEE Conference on Sustainable Utilization and Development in Engineering and Technology*, Malaysia, 20th–21th October 2011, pp. 119–122
12. N. Caárdenas-Benítez, R. Aquino-Santos, J. Aguilar-Velazco, A. Edwards-Block, A. Medina Cass, Traffic congestion detection system through connected vehicles and big data. Sens. MDPI **16**(599), 1–10 (2016)
13. A. Gupta, DTC: a framework to detect traffic congestion by mining versatile GPS data, in *1st IEEE International Conference on Emerging Trends and Applications in Computer Science*, Shillong, India, 13th–14th September 2013, pp. 97–103
14. B.G. Rajagopal, S. Appavu, An intelligent video surveillance framework with big data management for Indian road traffic system. Int. J. Comput. Appl. **123**(10) (2015)
15. Hamilton, The MapReduce-based approach to improve vehicle controls on big traffic events, in *International Colloquium on Logistics and Supply Chain Management*, 27th–28th April 2017, pp. 1–6
16. A. Souza, C. Brennand, R. Yokoyama, Traffic management systems: a classification, review, challenges, and future perspectives. Int. J. Distri. Sens. Netw. **13**(4), 1–14 (2013)

Travel Booking and Management Application: TravelBel



Elroy Gomes, Tryambak Gour, Arushi Sinha, and R. Dakshayani

Abstract In a world, where travelling is now not just limited to leisure family trips, an up-to-date optimal solution for business tours, event travelling is yet awaited. The aim is to accomplish this by creating a web application, called TravelBel-Business, Events and Leisure Travels (will be called TravelBel hereafter), using simple route based optimization algorithms, which processes real time data and gives the user(s), i.e. business travellers or people travelling for various events like competitions, weddings, etc., a complete travel package from the start to the end; which includes stay and travel with the best possible plans at the current time for the associated party, all in one place. The web application will take certain inputs from the users regarding the trip, which will be used to select and create the most relevant and optimal tour packages for the user(s). The web application gives the users various travel packages for the enterprise/planners who can chose one among the given options and edit a few particulars in it, for, e.g. the required level of luxury. In turn, the user, instead of doing different bookings through different websites, will get to complete all travel related bookings in one place, with tailor-made packages. Thus, making the booking and travelling experience simplified and efficient for all stakeholders.

Keywords Optimization · Travel package · Tailor-made

1 Introduction

The Travel Industry has always been one of the major industries of the world. People always look forward to a stress-free and a relaxing holiday trip. Apart from vacations, a sharp rise has been observed in business tours for corporate meetings. Rigorous planning is an essential component for such trips to be successful, hassle-free and up to the mark of industrial and contemporary standards of luxury in a friendly budget. Extensive search for best ticket prices, place to stay, and the timeline of the tour through the various sources on the internet takes centre stage, where the

E. Gomes (✉) · T. Gour · A. Sinha · R. Dakshayani
Department of Computer Engineering, Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai, India
e-mail: dakshayani@fcrit.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_6

respective department of tour regulation is burdened with the goals of reducing firm's cost and providing best-in-class facilities. The need of tailor-made tour and reliable travelling packages for more than just leisure have been recognized and now being catered to the businesses as it has been an unexplored niche by many. A system wherein the stakeholders can thrive with the least amount yet promising results based on various algorithms which will suggest and give the optimal plan for execution based on various parameters. On the whole, a solution catering to the travel needs of corporates, events and leisure can be efficiently planned making the complete process a hassle-free experience. The new world we are entering, post Covid-19 will see a drastic rise in tours for businesses, various sports events, weddings, etc. Having a system prepared for it in place will be a big step towards a better and closely-knit world. The subsequent Sect. 2 gives a comprehensive literature review, Sect. 3 talks about the proposed system, Sect. 4 gives a comparative study with existing systems, Sect. 5 gives a glimpse of the complete web application and Sect. 6 talks about the conclusion and future scope of TravelBel.

2 Literature Review

In order to create TravelBel, a lot of research has been done in fields of web application development, security, smartphone as a tool and online payment systems among others. Few research papers were reviewed and studied in order to get a better understanding of the current problem and propose innovative solutions. The paper titled "Smartphones—a powerful Tool for Tourism—Romanian Travel Apps" [1] puts forth the view that smartphones are an integral part of one's life and pose to be a powerful tool for tourism. The paper analyses the use of smartphones in travel and tourism and the overall usage of smartphones in the US and Europe regions. According to the authors, the modern traveller is fast and pacey and to fulfil this need the speed of smartphones come in handy to give users travel options, accommodations, bookings, etc. In order to survive in the travel market space, one needs to adapt to the constant changes majorly being the switch from computers to smartphones, around 1 billion smartphones are sold every year [2] and to keep up with it one needs to build apps for phones. The authors have proved that more and more tourists and travellers use smartphones to book and plan their travel and have stated that mobile apps are a must in today's world. The next paper "Security Testing of Web Applications: Issues and Challenges" [3] talks about the increasing complexity of web applications and how security testing plays a vital role in keeping the application data secure from threats and allows the application to function as intended without any leakage of information. The paper focuses on the issues and challenges faced by security testing of web applications and the tools used to perform security testing since the recent explosion in security vulnerabilities. The ultimate objective is to find the defects that can possibly be used to attack. Security testing assists to imitate and reveal vulnerabilities like SQL injection, buffer overflow, cross-site scripting, file inclusion, URL injection and cookie modification among others. The authors have identified 29 issues related

to security testing, some of the notable ones being-Malicious file execution: In cases when the code execution occurs through untrusted sources, web applications are at high risks of harmful file's execution; Bad code or fault in implementation: Poor or inappropriate coding and/or unsound implementation may also lead to a compromise on the security of the web application; Missing or inadequate validation of input data: In case of insufficient or missing input data, an attacker can access sensitive information by injecting scripts in the web page. Further the paper gives insights about the challenges faced by security testing such as automated testing is not yet possible for complex applications and has to keep up with the evolving and changing technologies. Using agile techniques in the software development process assists the developer to build high-quality applications in terms of security. The paper strongly supports the point that focusing on these issues can improve the security of the application. Accordingly, the security tester should keep a complete record of such possible flaws, whilst testing the security for a web application as well as consolidate all the information related to the flaws and vulnerabilities of the system, thus creating solutions for removing the security vulnerabilities of the system. Lastly "A Comparative Study: MongoDB versus MySQL" [4] has provided us a direction to work once the project came to a standstill. TravelBel was designed to fetch real time data of flights, trains, buses and hotels through high performance APIs. However, this approach couldn't be put to practical use owing to the pandemic, creating deficit of data in the required format. A crisp explanation about MySQL and MongoDB on how various operations involved in application development are performed in each of them, pros and cons of both the databases and a comprehensive performance tests of significant functions in them, namely insert, query, delete and update was done which helped in gaining the desired clarity to choose MongoDB over MySQL. The flexibility of using a non-relational database and features like cloud-based storage, easy updating and scalability allowed a real time simulation database for TravelBel with a robust database.

3 Proposed System

3.1 System Design

The web application has been created using Angular, MongoDB is used for the simulation database of the system including flights, trains, buses and hotels, Node.js frameworks namely express and mongoose for backend functionalities of the web application. Below is the block diagram of TravelBel (Fig. 1).

3.2 User's Interaction with the System

TravelBel has been created to serve larger groups of people planning travel by taking in some inputs from the traveller(s) based on their preferences. It aims to create

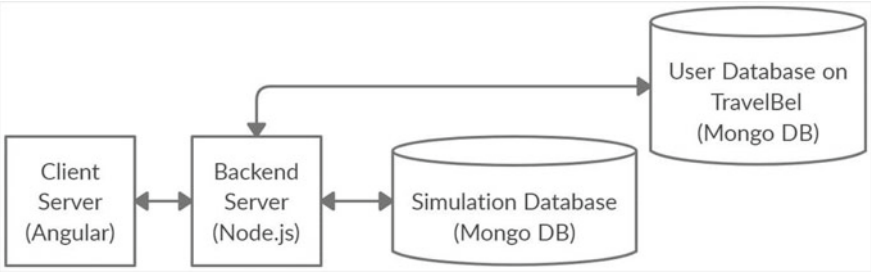


Fig. 1 Block diagram of TravelBel

events and business trips and allow customers to book tickets to places via the best possible modes as well as provide them desired accommodation at the destination. The web application will also be equipped with filters so as to serve the customers with their tailor-made plans, within their monetary budget and/or the stipulated time duration of travel. The algorithm is made in such a way that the customer gets to select the parameters in the beginning as well as gets to modify a few particulars in the various packages availed (Fig. 2).

The algorithm used is as given below:

1. The customer selects the type of trip he/she wants to make, i.e. business trip, event trip or leisure trip.
2. The customer creates the trip gives the trip a name and is given the options of inputting the booking source and destination, date of departure and the whether the trip will be single or return trip.
3. The source and destination will be fetched and searched in the simulation database having about 500 data entries consisting of all the flights, trains and buses with the total ticket prices and other details, which will be displayed along with the hotels in the area with their respective distances from the airports, and stations in the form of packages.
4. The packages will be classified and sorted for the ease of access and understanding of the itinerary and will have options of further customization and booking the package.
5. The customer also has an option to login and check the details like payment details, package details, packages in cart and other personal details.

4 Comparison with Existing System

The existing systems which are available in the market also provide reliable options. But TravelBel takes a step ahead in serving the niche of group travels especially for corporates and event travelling. Following is a comparison with two major similar contemporary applications in the market, namely MakeMyTrip and TravelTriangle.

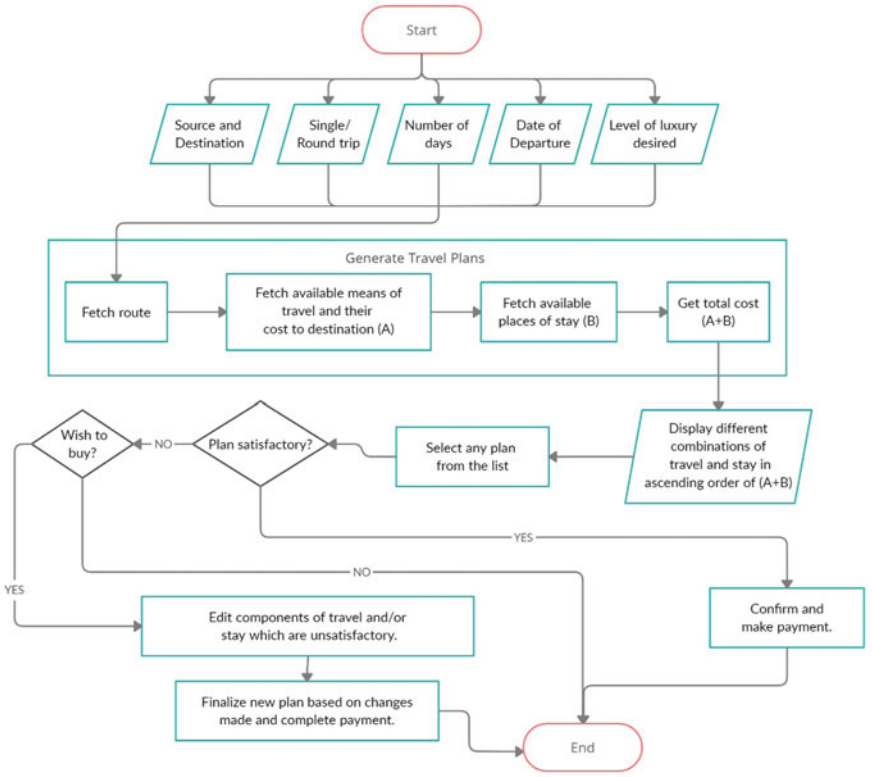


Fig. 2 Flowchart depicts the user's interaction with the system

MakeMyTrip.com: One of the most used and trusted contemporary travel booking and management systems, MakeMyTrip today caters to a large customer base. They have evolved into an ecosystem of franchisee partnership and are a household name for travel related bookings, owing to attractive advertising [5]. MakeMyTrip is aimed at providing predesigned travel packages for leisure trips and vacations, apart from regular ticket booking services, to different types of customers, ranging from families to bachelors. They have a partner-based business model, wherein they give partnerships to third-party travel agents who act as mediators to MakeMyTrip and thus create an agent-based ecosystem. However, TravelBel is designed for a different niche of customers who are corporates, booking tours for the employees, and people travelling for a particular event. TravelBel is not aimed at engaging in a partnership-based business model but to directly provide services to the clientele, thus eliminating the middle man and reducing costs. However, this may also mean employment of middlemen in the organized corporate sector.

TravelTriangle.com: Travel Triangle is a budding start up in the field of providing highly personalized travel itineraries to its customers, with various options [6]. They also offer a partnership system like MakeMyTrip but are mainly aimed in providing

real time leisure travel packages of various types ranging from honeymoon trips to family trips, solo trips among others. They have a niche market and are not a very renowned service platform amongst customers. Though Travel Triangle has a lot to offer, it has emphasized on knowing the user more to suggest better offers. This may be a good way to make the offering highly personalized but in the contemporary times of highly reduced attention span of consumers to not more than 10 s [7], such pop-ups and higher number of questions make the website less preferable to consumers and thus has not allowed Travel Triangle to achieve what it should have. Learning from this, TravelBel has ensured to limit the input parameters to as less as possible from the user and is clearly placed to the target consumers not just as a booking platform, but as a tool to making the functionalities crisp clear.

Apart from the above described major existing systems in the field of travel booking management, there are many other systems which do not directly aim at presenting complete packages but offer other functions, like reduced costs in ticket bookings, last minute bookings, discount offers in bookings, membership to customers in booking systems to recommend them trips and thus create a loyal customer base. However, the above two are the closest systems which provide personalized travel packages to customers amongst other competitors in the market.

5 Results

The following screenshots provide a glimpse to the web application TravelBel in both mobile and desktop views (Figs. 3, 4 and 5).

6 Conclusion and Future Scope

TravelBel is a web application that provides end-to-end solutions to the problems faced, whilst planning business, events and leisure trips. It fulfils all the requirements of the travellers, from their location to their flight bookings, rail and bus seat bookings, place of accommodation as well as the return trips, with a complete plan, promising tailor-made travel plans for an exciting experience. The system is currently using a simulation database due to the lack of required data but will be using application programming interfaces (APIs) or a service-provider login system, to fetch the real time data post pandemic and thus yielding the best available resources for the customers ranging from high end corporates to small scale event managers as a one stop solution.

In the future, this project is expected to go to product level so that the customers can cover all their travelling needs in a single-web application and plan their trips for events ranging from corporate tours to national competitions, weddings amongst many others. Improvisation of UI and UX will be focussed upon by using technologies like ML and AR so as to provide many more details about a destination to the

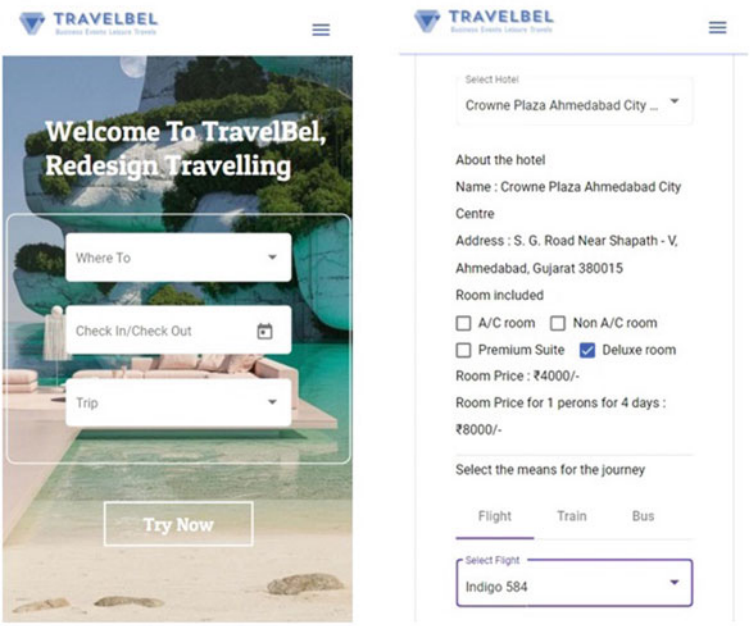


Fig. 3 Mobile view of TravelBel

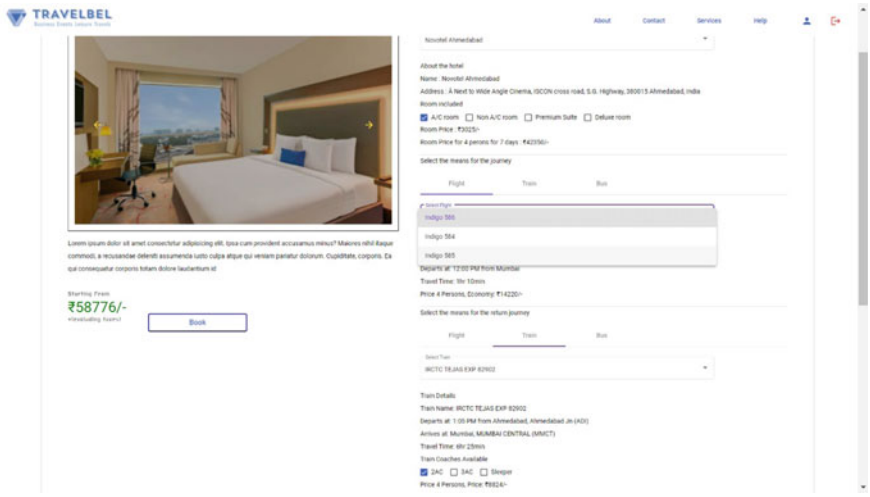


Fig. 4 Customize travel plan

user providign an immersive experience [8], and there will be a shift in data being fetched, which will be real time and not simulated. A new login for flight companies, train and bus services will be created so that these services get their own dashboard where they can update the availability of seats and the facilities they offer as well

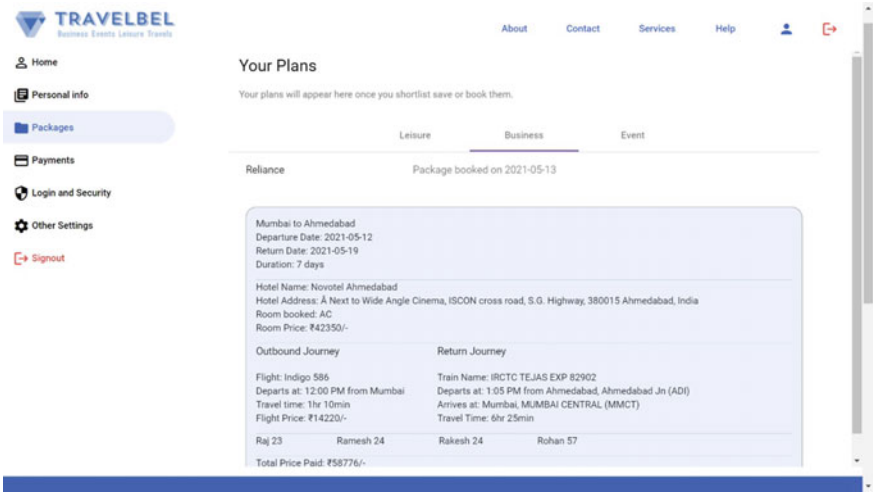


Fig. 5 Booked package in user's profile

as use the dashboard to analyse their business and grow with the insights provided by user data. Also, after getting a good customer base and data, it is planned to implement a recommendation system to target various groups of people based on their requirements and give them suggestions, using machine learning algorithms and implement a sentiment-based travel review system [9] to get significant reviews thus improving the application.

References

1. R. Sergiu, L.M. Csorba, Smartphones—a powerful tool for tourism- Romanian travel apps. J. Econ. Bus. Res. (2016)
2. One billion smartphones sold every year. https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/
3. A. Jaiswal, G. Raj, D. Singh, Security testing of web applications: Issues and challenges. Int. J. Comput. Appl. (2014)
4. C. Gyorodi, R. Gyorodi, G. Pecherle, A. Olah, A comparative study: MongoDB vs. MySQL, in *The 13th International Conference on Engineering of Modern Electric Systems*, Oradea (2015). https://doi.org/10.1109/EMES.2015.7158433
5. MakeMyTrip franchise model. https://www.makemytrip.com/franchisee/franchisee_model.php
6. Travel Triangle. https://traveltriangle.com
7. Reduced attention span in humans. https://www.wyzowl.com/human-attention-span/
8. M.S.B.W.T.M.P.S.B. Thennakoon, R.D.T.N. Rajarathna, S.P.B. Jayawickrama, M.P.D.S.M. Kumara, A.M. Imbulpitiya, N. Kodagoda, TOURGURU: Tour guide mobile application for tourists, in *International Conference on Advancements in Computing (ICAC)* pp. 133–138 (2019). https://doi.org/10.1109/ICAC49085.2019.9103380
9. M. Afzaal, M. Usman, A. Fong, Tourism mobile app with aspect-based sentiment classification framework for tourist reviews. IEEE Trans. Consumer Electronics **65**(2), 233–242 (2019). https://doi.org/10.1109/TCE.2019.2908944

Security and Privacy Issues in Internet of Things



Dipankar Debnath, Sarat Kr. Chettri, and Ajoy Krishna Dutta

Abstract The Internet of Things (IoT) is used in a variety of fields, covering almost all the aspects of the individuals' day-today-life, organisations and society. With the Internet revolution, the IoT framework provides a platform for connecting many smart and self-configuring objects, such as watches, cars, tablets, wearable devices and home appliances. Despite the technological and societal advantages and the enormous economic potential of IoT, the issue of security and privacy in IoT is a major concern. IoT systems have problems with scalability, centralization, data security and privacy. This article provides an overview of IoT systems and reviews the IoT's typical security and privacy issues taking into consideration the biomedical domain. In addition, this article explores the convergence of blockchain and computing technologies for IoT applications and blockchain based mitigation of DDoS attacks.

Keywords Internet of Things (IoT) · Blockchain · Edge computing · DDoS · eHealth · Privacy and security challenges · Cryptomining

1 Introduction

The Internet of Things (IoT) is defined as a network of real objects or "Things" embedded with sensors that communicate with and exchange data with other devices and networks via the Internet. IoT is applied in several diverse fields is used in a variety of fields, covering almost all the aspects of the day-today-life of individuals, organisations and society. Some of the major application areas for IoT include healthcare

D. Debnath (✉) · A. K. Dutta
Department of Computer Science, St. Mary's College, Shillong, Meghalaya, India
e-mail: d.debnath@smcs.ac.in

A. K. Dutta
e-mail: a.dutta@smcs.ac.in

S. Kr. Chettri
Department of Computer Applications, Assam Don Bosco University, Guwahati, India
e-mail: sarat.chettri@dbuniversity.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_7

and medicine, agriculture and irrigation, the automotive industry, the manufacturing industry (e.g., Industrial IoT), public transportation, smart homes, and so on. Using blockchain, various limitations of traditional IoT applications can be addressed, such as securing the data transfer between IoT devices and applications, protection of sensitive information when delivered via the IoT network, without any requirement of third party to validate the IoT data, optimizing the computational power of IoT devices, reducing the operating costs of IoT applications, etc. In reality, blockchain provides IoT devices, applications and platforms with a scalable and decentralized environment. Moreover, blockchain-based IoT systems allow companies to run smart applications and execute multiple legal procedures between business partners through smart contracts. However, IoT systems suffer from problems of scalability, data security and centralization and thus the convergence of blockchain and artificial intelligence for IoT applications together with cloud and fog computing could lead to the development of a secure, scalable, decentralized and intelligent IoT ecosystem. Although the idea of IoT has been around for a long time, recent advances in various supporting technologies such as low-cost low-power sensors, edge and advanced computing, machine learning and data analytics have made it the most important technology of twenty-first century. The following is how the article is structured: A brief description of edge computing technology is provided in Sect. 2, followed by Sect. 3's discussion of blockchain technologies and their applications in the biomedical domain. Various risks of privacy leakage and security threats in IoT systems and applications are discussed in Sect. 4. Section 5 discusses on DDoS attacks in IoT platform and its mitigation using blockchain. Section 6 concludes the article.

2 IoT-Edge Environment

Fog computing and Edge computing [1], both has the same objective of brining computing and processing closer to the end node, however the key point that differentiate between fog computing with edge computing is the location where the computing or processing is done. In case of fog computing, the processing is conducted in the middle layer between end device and cloud called the fog layer, whereas in case of edge computing, computing and processing is performed at the edge or end device.

Edge computing offers several advantages, including less delay in data processing, analyzing data in real time, low network traffic, and reduced operating cost. Figure 1 shows taxonomy of IoT-edge environment comprising of various features such as computing paradigm, network technologies, service objectives, technologies and application areas. The computing paradigm can be categorized as cloud computing, fog computing, edge computing, mobile ad-hoc computing and hybrid computing. The addition of IoT platform with Cloud computing technologies [2] addresses the issues in data storage and management, data exchange among heterogonous devices and network, privacy, security, unified and ubiquitous access. Fog computing [3] bridges the gap between cloud and end devices by bringing computing, storage,

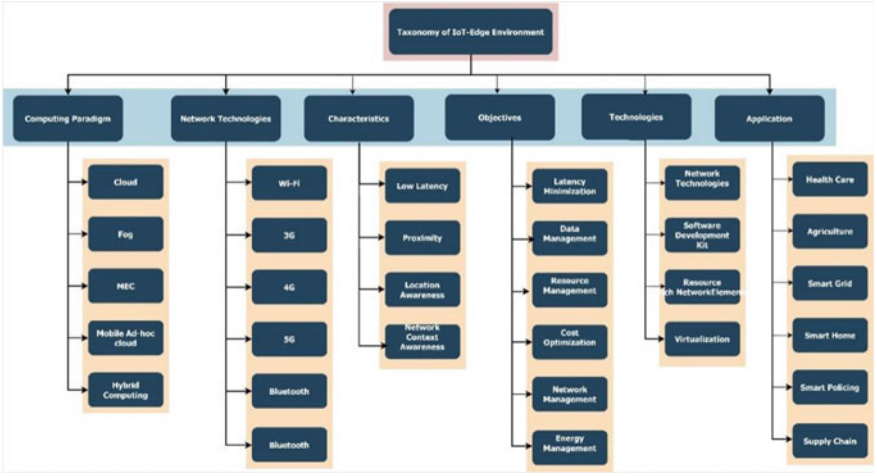


Fig. 1 Taxonomy of IoT-edge environment

privacy and security closer to IoT nodes thus providing fast and on-time response. IoT nodes collect data using sensors and actuators and transmit them to the nearest edge or fog layer. The primary objective of IoT-edge paradigm is latency minimisation, transmission and aggregation of data, optimum use of available resources, cost efficiency and energy efficient IoT node management. Low latency sensitive IoT-edge computing is applied in a multitude of sectors, including agriculture, retail, healthcare, smart cities, smart grid, smart policing and many others.

3 Blockchain Technology with IoT

A blockchain [4] can be defined as a time-stamped series of data records that are immutable and managed by a group of computers without any central authority. Such data records are securely stored as blocks, which are linked to each other using the ideologies of cryptography. A blockchain is a decentralized, time-stamped collection of immutable records called blocks distributed over peer-to-peer networks. Each block consists of a series of transactions that are secured and chained to each other using cryptographic hash functions. The blockchain technology is seen as a recent breakthrough in an open networked system where computation is secure and transparent and where everyone involved is accountable for their actions without any ownership by a single entity. IoT-cloud infrastructure has enormous potential in the field of Smart healthcare. IoT enabled devices have made continuous and remote monitoring of patients possible. IoT wearable device like fitness bands, blood pressure, heart rate, glucometer monitoring cuffs and many more enabled personalized health care. IoT sensors and tagging devices help hospital authorities to track various

assets such as wheelchairs, oxygen pumps, nebulizers and other monitoring equipment in real-time. The large set of medical data collected from real world cases using these diverse IoT devices increases both accuracy and precision of various services such as medical care, emergency care, resource utilization, insurance claims, resource, medical information system etc. The data is a prime asset in IoT-cloud infrastructure and therefore is most vulnerable to cyber-attacks. In the biomedical domain, the blockchain technology is mainly used in order to maintain the data integrity, enable distributed access control, data lineage and non-repudiation. The data refers to medical records, personal health records, personal biosensor data, clinical trial data, medical insurance etc. Mostly, blockchain is used to address the issues of data security and privacy prevalent the distributed environment. Other uses include the assurance of non-repudiation of medical acts or transactions and to build a reliable and transparent ecosystem in the healthcare sector. The integration of blockchain technology with IoT in biomedical domain addresses the IoT paradigm's issues of reliability, data privacy, and secure information.

4 Privacy and Security Challenges in IoT

In spite of the technological and societal benefits of IoT, as well as its enormous economic potential, the security and privacy issue [5] is a major concern. The problem is complicated by the inherent complexities involved in its deployment and mobility. It is one of the main reasons why many technologies are unsuitable for industrial applications and are only used at the consumer level. Some of the open questions related to IoT security [6] are: How can the security characteristics of IoT devices be identified and quantified? How do we assess the efficacy of initiative and countermeasures in terms of IoT security? How do we ensure that best practices for IoT security are followed? Should there be any regulations that penalise device manufacturers for selling software or hardware with known vulnerabilities for IoT? Privacy protection of data in the IoT environment is a serious issue because of the prevalence of different types of attacks on IoT entities, lack of transparency due to insufficient authentication, authorization, strict rules and regulations against the data collection and use etc. For example, in ehealth services [7], IoT devices are used to collect and transmit patient health information over a network, allowing healthcare professionals to remotely monitor the status of patient's health at any time. Nonetheless, there is a risk that sensitive patient data will be stolen, resulting in a breach of privacy, or that it will be tampered with. Again, in the food industry, for example, bio-sensors [8] are used for early detection of target bacteria for safe food delivery and food contamination prevention. Such data is transmitted over a network and must be treated with utmost confidentiality in order to protect the food company's professional image. There are a number of issues related to privacy and security threats to IoT that affect the smooth functioning of IoT. For example, botnet malware, industrial espionage and eavesdropping, IoT device hijacking, IoT bot crypto-mining, DDoS, botnet malware,

middle attack man, flood attacks, ransomware, and so on. Some of the privacy and security issues in IoT are discussed in the following subsections.

4.1 Inadequate Security Standards Adopted by IoT Manufacturers

Most IoT device manufacturers does not possesses adequate privacy policy for their devices [9] and due to lack of such security standards, IoT devices with poor security are manufactured. For example, after pairing, the Bluetooth on most smart wearables remains visible, a user's Gmail account details may be revealed by a smart refrigerator at home, and the smart fingerprint padlock can be accessed via Bluetooth key using a phone app, among other things. Access Control and Data Encryption mechanisms alone may not guarantee privacy, but the type of information transmitted, its use, and with whom it has been shared also play a role. As a result, there is a need for a standard privacy policy to be followed by IoT device manufacturers, which also ensures that the IoT device's actual behaviour is consistent with the privacy policy agreement.

4.2 Lack of User Knowledge and Awareness on IoT Functionality

Being a new technology, people still don't have ample knowledge about the functionality of IoT. Although most Internet users comprehend spam and phishing prevention, and many are aware of viruses and how to secure Wi-Fi networks with secure processes, security issues in IoT persist. It has been observed that the majority of IoT potential threats remain on the manufacturing, consumer, and business sides. User ignorance is one of IoT's biggest security risks [10] and challenges. Their lack of knowledge and awareness of IoT functionality put them at greater risk.

4.3 Vulnerabilities in IoT Device Updates

Unsafe software [11] is another potential source of risk to the security of IoT devices. Users can purchase an IoT device with the most up-to-date software; however, new vulnerabilities are unavoidable and may necessitate updates to ensure the safety and security of IoT devices. Some IoT devices may be provided with automatic updates, while some may still run without the necessary updates. There is a risk during an update, as the device update process sends backup to the cloud, and if the connection is unencrypted, sensitive information on the device may be stolen by a hacker. On

the other hand, if the device is not upgradeable, there will be vulnerability for the rest of the lifetime of the device. As a counter measure, adequate security measures must be designed to allow automatic updates of IoT devices.

4.4 Detection of Rogue IoT Devices

Wi-Fi has become the preferred communication medium for connecting IoT devices. Wi-Fi connections, on the other hand, are vulnerable to spoofing attacks from rogue access points (APs) or devices with identical SSIDs and/or MAC/IP addresses to legitimate devices. Such attacks may not be mitigated by conventional network security systems. A rogue device impersonates or integrates with the original device as a member of the group to collect or distort confidential data [12]. It claims that exchanging and collecting data generated by other IoT devices for malicious purposes is permissible. Rogue IoT devices may breach the network's perimeter. Devices such as the Raspberry Pi can be converted into a rogue AP (Access Point) and intercept incoming data communications without the users' knowledge.

4.5 Cryptomining with IoT Bots

The popularity of cryptocurrencies has grown tremendously over the last decade, and IoT security has also seen a significant increase in the risk. Various unconventional methods are used to acquire cryptocurrencies. It is known that mining cryptocurrency requires massive CPU and GPU resources, resulting in crypto mining with IoT bots, which is another security issue in IoT [13]. These IoT bots or botnets attack IoT devices without harming them while secretly mining cryptocurrency with their resources. One such example is the Monero (open-source cryptocurrency), the first cryptocurrency mined using IoT botnets. Device like video camera with its limited resources may make it unsuitable for cryptocurrency mining, but a group of video cameras has the potential. IoT botnet miners pose a significant threat to the cryptocurrency market because the entire market can be flooded and disrupted by a single attack caused by such botnets.

4.6 Ransomware

Ransomware has emerged as one of the biggest cyber threats in the world. Ransomware is a type of malware in which a hacker encrypts [14] the victim's data before threatening to publish it. The data is decrypted unless a ransom is paid. Generally, users' data are not destroyed, but ignoring IoT ransomware can have disastrous consequences. It is widely considered to be one of the most infamous types of

malware ever devised. In the year 2017, the WannaCry ransomware attack was the most serious threat to computers running the Microsoft Windows operating system. The ransomware encrypted data and demanded ransom payments in bitcoin.

4.7 DDoS Attack

One of the most common Internet attacks is a distributed denial-of-service (DDoS) attack [15]. The aim of these attack to disrupt normal operation to damage economic cost and credibility, users' privacy and security, extortion, and cyber warfare, etc. This is accomplished by the flooding the target machine with superfluous request to overload the system so that it cannot perform any legitimate work. Some of the most recent DDoS attacks are Spamhaus attack (2013), GitHub attack (2015), Mirai Dyn attack (2016), Memcached DDoS attack (2018) and Takedown attack (2019) [16]. In general, DDoS attacks can be categorized as bandwidth depletion attack [17] and resource depletion attack. In case of bandwidth depletion attack, large volume of malicious packets are flooded into the target system to overload network system. The target system tries to process the incoming data and fails to forward these malicious packet to the target application. As a result, the system slows down or crashes preventing access by legitimate users. DDoS resource depletion attack aims to send packets to misuse network communication protocols. Resource depletion attack is designed to quickly deplete the system resouces such as CPU, memory and network resources such as gateways and sockets.

5 Blockchain Based Mitigation of DDoS Attacks

The number of attacks on IoT devices are increasing and existing mitigation technique are facing problems due to lack of resources, high cost, low flexibility and mostly use centralized approach. The emergence of blockchain technology can support secure P2P network, where IoT devices can communicate with reliable public key cryptography and avoid threats from malicious sources.

A list of cloud based DDoS attacks and their mitigation strategies are summarized in Table 1.

Blockchain can be used to prevent DDoS attacks in several ways.

(a) Blockchain can be utilized for decentralized DNS naming system [18] allowing registering, managing, and resolving of domain names on the blockchain where network participants acting as nodes connect to each other directly without middlemen. Ethereum Name System and Namecoin were the first to bring name resolution to the blockchain. At present, DNS system allows one-to-one mapping of IP addresses to domain name. These systems are centralised in nature and only trusted persons are allowed to access the database and update

Table 1 A list of DDoS attacks with description and defence mechanism

DDoS attack	Description	Probable defence mechanism
IP spoofing attack	IP packets from false source address are sent by the attackers that appears to be from legitimate source address in order to overload the system	(a) Hop Count Filtering (HCF) (b) Secure encryption protocols like HTTPS
SYN flooding attack	A SYN (half-open attack), where the attacker sends repeatedly large number of SYN packets to overwhelm the targeted port on the server machine	(a) SYN Cache (b) SYN Cookies (c) Reducing time for receiving SYN packet (d) Firewall Filtering
Smurf attack	Attacker sends large number of ICMP packets using target spoofed address and renders a computer network inaccessible	(a) Disabling the IP-directed broadcast command on routers (b) Setting up the operating system to disable all responses to ICMP packets sent to IP broadcast addresses
Buffer Overflow	Here the attackers takes advantage of buffer overflow problem and execute its own malicious code to take control of the system	(a) Address space randomization (b) Data execution prevention
NTP Attack	In a Network Time Amplification (NTP) attack, publicly accessible NTP servers are used to overpower a target server with UDP packets. It is called amplification attack because query-to-response ratio is very high	(a) Block source port (b) Block Monlist responses (c) Rate limiting at the source or destination (d) Regular expression (traffic signature) filter
Zero-day DDoS attack	All unknown and new attacks for which no patch has been released yet are known as zero-day attack	(a) Block hack attempts (b) Using advanced AI techniques (c) Using encryption techniques

it. DDoS attacks take place, when a malicious user gets access to the database and performs illegitimate activity. The DNS database would be stored in a blockchain and would be distributed ubiquitously across all the nodes. As a result, no single point of failure will exist.

(b) Another futuristic idea discussed in the literature is to create a blockchain based decentralised client–server internet paradigm [19]. Since there will be no centralized single server, thus alleviating the chances of DDoS attack. Here, data and applications would reside in peer-to-peer network and distributed across multiple nodes. Data communication and retrieval would take place using various cryptographic techniques.

Blockchain based DDoS mitigation system is an active area of research and still in its infancy stage.

6 Conclusion

IoT comprises devices ranging from simple electronics to mobile devices and industrial devices where communication takes place between humans and devices or direct communication between devices without human intervention. Despite the technological and societal advantages and the enormous economic potential of IoT, the issue of security and privacy in IoT is a major concern. The article explores current research and discusses blockchain technologies and their applications in the biomedical domain. It focuses mainly on security and privacy challenges in IoT with some potential solutions. It explores the various attacks in IoT with special attention to distributed denial of service attacks and probable defence mechanisms to alleviate such attacks. Being an active research area, and in its infancy stage, the article provides potential research directions for future works in using the blockchain to mitigate the DDoS attacks in IoT.

References

1. K. Dolui, S.K. Datta, Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing, in *2017 Global Internet of Things Summit (GIoTS)*. (IEEE, 2017), pp. 1–6
2. L.M. Dang, M. Piran, D. Han, K. Min, H. Moon, A survey on internet of things and cloud computing for healthcare. Electronics **8**(7), 768, 1–49 (2019)
3. S.P. Singh, A. Nayyar, R. Kumar, A. Sharma, Fog computing: from architecture to edge computing and big data processing. J. Supercomput. **75**(4), 2070–2105 (2019)
4. M. Xu, X. Chen, G. Kou, A systematic review of blockchain. Finan. Innov. **5**(1), 21–24 (2019)
5. G. Sun, V. Chang, M. Ramachandran, Z. Sun, G. Li, H. Yu, D. Liao, Efficient location privacy algorithm for Internet of Things (IoT) services and applications. J. Netw. Comput. Appl. **89**, 3–13 (2017)
6. R. Jaren, E. Scott, L. Chapin, The Internet of Things: an overview—understanding the issues and challenges of a more connected world. Internet Soc. (2015)
7. B. Farahani, M. Barzegari, F.S. Aliee, K.A. Shaik, Towards collaborative intelligent IoT eHealth: from device to fog, and cloud. Microprocess. Microsyst. **72**, 102938 (2020)
8. N. Massad-Ivanir, G. Shtenberg, N. Raz, C. Gazenbeek, D. Budding, M.P. Bos, E. Segal, Porous silicon-based biosensors: towards real-time optical detection of target bacteria in the food industry. Sci. Rep. **6**(1), 1–2 (2016)
9. A. Subahi, G. Theodorakopoulos, Ensuring compliance of IoT devices with their privacy policy agreement, in *6th International Conference on Future Internet of Things and Cloud (FiCloud)*. (IEEE, 2018), pp. 100–107
10. V.D. Soni, Security issues in using IoT enabled devices and their impact. Int. Eng. J. Res. Dev. **4**(2), 7 (2019)
11. N.S. Mtetwa, P. Tarwireyi, A.M. Abu-Mahfouz, M.O. Adigun, Secure firmware updates in the Internet of Things: a survey, in *International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*. (IEEE, 2019), pp. 1–7
12. P. Liu, P. Yang, W.Z. Song, Y. Yan, X.Y. Li, Real-time identification of rogue Wi-Fi connections using environment-independent physical features, in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. (IEEE, 2019), pp. 190–198
13. A. Zimba, Z. Wang, M. Mulenga, N.H. Odongo, Crypto mining attacks in information systems: an emerging threat to cyber security. J. Comput. Inform. Syst. **60**(4), 297–308 (2020)

14. A. Wani, S. Revathi, Ransomware protection in loT using software defined networking. Int. J. Electr. Comput. Eng. **10**(3), 3166–3175 (2020)
15. T. Mahjabin, Y. Xiao, G. Sun, W. Jiang, A survey of distributed denial-of-service attack, prevention, and mitigation techniques. Int. J. Distrib. Sens. Netw. **13**(12), 1–33 (2017)
16. R. Singh, S. Tanwar, T.P. Sharma, Utilization of blockchain for mitigating the distributed denial of service attacks. Sec. Privacy **3**(3), e96 1–13 (2020)
17. M. Darwish, A. Ouda, L.F. Capretz, Cloud-based DDoS attacks and defenses, in *International Conference on Information Society*. (IEEE, 2013), pp. 67–71
18. E. Karaarslan, E. Adiguzel, Blockchain based DNS and PKI solutions. IEEE Commun. Standards Mag. **2**(3), 52–57 (2018)
19. K. Kim, Y. You, M. Park, K. Lee, DDoS mitigation: decentralized CDN using private blockchain, in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*. (IEEE, 2018), pp. 693–696

Industry 4.0: An Overview and Further Research Directions



Padmanabha Aital, Rajesh Patil, Sashikala Parimi, and Prerna Singh

Abstract Prupose—The term 'Industry 4.0' commonly used for fourth industrial revolution. It is mainly grounded on Internet of Things (IoT) where cloud based data exchange is done between machines or machine and human beings. In Industry 4.0, Internet of Things is widely used in manufacturing industry. Industry 4.0's design emphasizes worldwide machine networks in an intelligent plant environment that can exchange data and control each other autonomously. Manufacturing industries are adopting digitalization and automation to cope up with competition. Productivity improvement is possible by the fast development in manufacturing techniques and Digitalization. There are many issues and challenges while implementing Industry 4.0. The aim of this study is to offer an outline of research conducted on Industry 4.0, to identify difficulties and problems that arise with execution of Industry 4.0 and to identify gaps between academic research and industry requirement. Methodology—A Systematic Literature Review method is used in this study. Findings—Authors have outlined prominence of research in Industry 4.0 and at end given further research directions. Originality/Value—The findings in this paper is very crucial for industry leaders, policy makers, governments, researchers, decision makers and professionals.

Keywords Industry 4.0 · Internet of Things · Smart manufacturing · Supply chain management

P. Aital (✉)
MPSTME, NMIMS University, Mumbai, India

R. Patil
Larsen and Tubro, Mumbai, India

S. Parimi
IBS, IFHE, Hyderabad, India
e-mail: sashikala@ibsindia.org

P. Singh
Universal Business School, Bangalore, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_8

1 Introduction

Today around the world, there is a huge technological change-taking place. Technology has performed a major part in promoting most requirements of our daily life, but it can also have a major influence on how we conduct trade. This transition is characterized by the increasing pace and range of the IT platforms and technologies that influences contemporary industrial culture. Many people call this the fourth industrial revolution. It has become the most discussed topic in the last few years. Firstly suggested by the German government in 2013, Industry 4.0 is the tag given to the on-going amalgamation of traditional manufacturing and what industry does with the increasing technological world around. In his paper [1] explained "Creative Destruction" a way towards innovation. In recent years, the worldwide manufacturing landscape has altered profoundly and is the consequence of advances and innovations in technology. Industry 4.0 can be briefly contrasted with earlier industrialised uprisings that have taken place in the last decades, representing the major disruption in manufacturing resulting from several technological improvements. The first industrial revolution began through the mechanization of the steam engine in Britain in the late eighteenth century. The Succeeding Industrial Revolt went into being in Europe and the United States during the second quarter of the nineteenth century. Several industry and mechanization techniques were created to satisfy the growing requirement, such as the assembly line with automatic activities, enabling increase in productivity. The Assimilated Circuit (microchip) development is based on the advancement in technology which caused the Third Industrialised revolt. In order to attain further automation in manufacturing, the usage of microchip and information expertise is the main components of this revolution that arose in many industrialized countries round the world in the twentieth century [2]. Industry 4.0, that ultimately constitute a fourth industrial revolt, is a complicated technical structure that's widely deliberated and explored, leading to major impact in the engineering segment as this brings appropriate advances linked to intelligent factories and potential ones. This evolving notion of Industry 4.0 is the canopy word for a fresh manufacturing prototype that encompasses numerous potential manufacturing innovations in Internet of Things (IoT), Internet of Services (IoS), Robotics, Big Data, Cloud Manufacturing, Machine learning and Augmented Reality. The implementation is essential to the growth of smarter manufacturing procedures that include equipments, machines, production components and goods proficient of separately swapping data, prompting behavior and governing each other, allowing a s mart manufacturing atmosphere [3]. This fresh strategy will combine the electronic and physical domains over CPS technology, implementing numerous potential industrial innovations that empower businesses adopting this fresh production paradigm to improve productivity and effectiveness. "Industry 4.0" is having enormous capacity and will deliver several financial and social possibilities over the exemplar change in jobs, business models and technology of manufacturing. In Industry 4.0, the linked Internet of Things (IoT) ecosystem helps both producers and customers in providing enhanced automation, enhanced communication and tracking, as well as self-diagnosis and fresh stages

of evaluation which is prospective. Plants will develop progressively in automation and self-observing, as the devices offer the capacity to evaluate and interact with employees, providing businesses with much smoother procedures that liberate employees for other duties [4].

1.1 Need of Industry 4.0

In Industry 4.0 Machines gather evidence from other machines, supply chain, and organize production themselves. Modern factories are in the phase of technological transformation, which affects not only factories but also entire supply chain. To meet to fact changing needs of customer, industry should adopt the flexible systems [5]. By becoming versatile and making it simpler to react to industry modifications, Industry 4.0 enables producers deal with present problems. Workers at the manufacturing centre can become coordinators, potentially improving employee work-life balance [2]. This will create work life balance for future generations. All this highlights the need of Industry 4.0.

2 Research Methodology

To know the significance of Industry 4.0 as a complicated technological scheme and try to consolidate this notion, an extensive literature review was conducted using the 5 databases of research papers, newspaper articles, conference papers, books and other records as the source of the secondary data.

2.1 Research Objective

The objectives of research are as given below. (i) To offer an outline of Industry 4.0. (ii) To identify Industry 4.0 implementation practices. (iii) To find influence of Industry 4.0 practices on social environment (iv) To identify impact of Industry 4.0 practices on business environment (v) To identify research gaps in existing practices (v) To provide further research directions The Literature survey is conducted to find out (i) How Industry 4.0 evolved (ii) definition of Industry 4.0 by various authors (iii) Implementation strategy and practices for Industry 4.0 (iv) effect of Industry 4.0 on social and business environment.

2.2 Research Questions

In order to achieve overall objective of the research, the research questions are: RQ1: What research is carried out on Industry 4.0? RQ2: What are the Industry 4.0 implementation practices followed by industry? RQ3: What is the impact of Industry 4.0 on social and business environment? RQ4: What is the research gap between the practices followed and expectations from industry? RQ5: What are the further research directions for Industry 4.0?

2.3 Systematic Literature Review

Above research questions are answered based on Systematic Literature Review. Research Protocol: Inclusion Criteria: Research papers on Industry 4.0, Fourth industrial revolution, Internet of Things. Exclusion Criteria: Research Papers which merely indicates Industry 4.0 but the aim of research paper is not related to research questions mentioned in this paper. Information/Data to be extracted:6 (i) Definition of Industry 4.0 (ii) Industry 4.0 implementation practices (iii) Benefits and impacts on business We have searched following databases and sources for peer reviewed research papers (i) EBESCO (ii) ProQuest (iii) Google Scholar (iv) Research Journals We selected total 55 research papers, which mentioned "Industry 4.0" a key word. We have found 31 papers relevant to this review, which exclusively dealt with topic on "Industry 4.0".

3 Literature Review

The Industry 4.0 is a merger of real production with virtual world as per German Institute for Industrial Standardization. The chief components of Industry 4.0 are Internet of Things (IoT), Industrial Internet of Things (IIoT); Cloud centred engineering and smart engineering aids in converting the engineering procedure into completely digital. Industry 4.0 leads to superior efficacy and transform into traditional production relationships among dealers, manufacturers, and consumers as well as between machines and humans [2].

3.1 Roadmap of Industry 4.0

Industry 4.0 visualize digital enterprise from strategic and technological Perspective [6]. In order to develop the situation in the market and business performance to achieve the objective of the organization, a roadmap has to be drawn. Industry 4.0,

coupled with the Internet of Things and Services, cloud computing and large data can improve industrial efficiency. Identification, selection, acquisition and implementation of technology shall be mentioned in roadmap [6]. Digital Beginner: Industrial enterprises are novices on the industrial 4.0 trajectory. In all areas as well as in distinct products and service portfolios, original digitalisation outcomes are achieved at this phase. Compliance at this point is not guaranteed and digital risks are not recorded. Vertical Integrator: This is Industry 4.0's second maturity phase. Companies use combined software also referred to as embedded systems and enables Internet-8 based product diffusion through the production media. Explicit internet locations and product inventory provide for the network to arrive at the market. Horizontal employee—Is the third phase of maturity that integrates with clients and stakeholders in the value chain. It integrates the production line with clients, distributors and subcontractors. It is better aligned with suppliers of logistics services and thus increases performance, improves the process time or reduces working expenses. Compliance with all company tasks is retained and enhanced techniques are used to manage digital risks.

3.2 Literature Review on Industry 4.0 Components

Advanced algorithms The application of Artificial intelligence and Robotics in Industry 4.0 requires advanced algorithms. An equipment will not be stand-alone. It has to communicate with other equipments. The required technology will cause radical changes in business process. Specific algorithms are required for this process and equipment [6].

Big Data and Analytics Big Data analytics is surely one of Industry 4.0's most significant technique. It concerns the wide collection, handling and evaluation of data with smart algorithms of organized and unstructured information. It has been extensively discussed lately in the company and academic globe, since it provides companies a range of fresh possibilities [7]. Semiconductor manufacturer Infineon Technologies has reduced defects by associating single-chip information recorded in the test stage at the start of the manufacturing procedure with information gathered previous stage. Infineon can thus recognize models that assist release defective chips soon in the manufacturing method and enhance the performance of manufacturing [8].

Autonomous Robots The use of automated machines straight operated by the smart plant and linked to the remainder of the company scheme shall be included in Industry 4.0. Automatic robots are generally employed for ergonomically challenging or tough employment [2].

Simulation Simulation technologies and software are also widely used. Business systems and manufacturing procedures can be simulated through these instruments

by evaluating the live data which can be as independent and values and the target values and delivering a complete analysis on the methodology [4]

Horizontal and Vertical System Integration Cross company information integration depending on information transfer norms can be achieved through horizontal and vertical integration technology. In other words, there is increasing networking and integration of computer and control procedures [11].

The Industrial Internet of Things In the current world very few instruments and computers from a manufacturer use networks and integrated calculating. Usually, it has a structure of a pyramid of automation where radars and equipment are with restricted acumen and mechanisation systems fed into an primary production mechanism. With the advent of Industrial Internet of Things, new equipment—including incomplete goods enriched by integrated technology and linked using conventional techniques. It also makes analytics and policy creation decentralized [13].

Cyber security Many businesses still depend on unconnected or closed management and manufacturing structures. The necessity to safeguard crucial industrial installations and manufacture from cyber security extortions rises radically with the enhanced connectivity and use of conventional communications protocols that arrive with Industry 4.0. Safe, consistent communications, advanced machine and user identification and approachable leadership are therefore crucial. Through alliances or purchases, numerous manufacturing tools suppliers entered powers with cyber security firms over the previous year [15].

The Cloud computing is another significant technology that enables large quantities of 11 information to be managed realtime for the production system. Cloud computation enables access to data at any moment from anywhere in the globe, thereby improving flexibility [16].

Augmented Reality New instructional designs 4.0 are exploiting enhanced technology of truth through enhanced truth. By learning the correct activities to do for servicing or device configuration, it is feasible to teach users through virtual reality. The scheme of augmented reality is intended to substitute ancient hard-to-understand paper manuals [18]. For instance, employees may obtain directions for repairing how to substitute a specific portion as they look at the real scheme that needs repair. Using equipment such as augmented-reality glasses, this data can be presented straight in the field of view of employees [17]. Virtual learning is another option. Siemens has created for its Cosmos software a virtual plant operator learning module using a real time, data created in 3-D atmosphere with augmented-reality to teach staff to manage situations. In this virtual world, by clicking on a cyber presentation, operators can study how to work with machines. The parameters are changed and obtain directions for information and servicing [19].

3.3 Literature Review—Definitions of Industry 4.0

The challenge facing the present globalization is to satisfy the continually increasing global mandate for assets and products by confirming a viable evolution of life in its societal, ecological and cost-effective aspects. To meet this challenge, the creation of industrial value must focus on sustainability. The advancement toward the fourth phase of industrialization, the so-called Industry 4.0, is presently shaping to create economic importance in the initial developed nations [21]. Its very crucial to integrate the Internet of Things and Services (IoTS) tools into the development of fiscal value. This paradigm is referred to as "Industry 4.0" or "Industrial Internet of Things" (IIoT) and transmutes conventional workshops into intelligent and autonomous manufacturing [22]. Industry 4.0 concentrates on complete digitization of all physical resources and amalgamating with value chain partners into digital environments. The unified cohort, analysis and communication of information reinforces the profits assured by Industry 4.0, in generating significance by interacting with a extensive assortment of novel techniques [23]. Industry 4.0 is a combined term for significant technological organisations and Industry 4.0 categorised as Things Internet, Services Internet, and Smart Factory [24]. In one of the most radical modifications IT systems have undergone a modification from computers to smart devices using cloud-based setup. This evolution of the Internet period, earmarked with computer-based automation and pervasive 13 systems, also linked by the Internet, defines Industry 4.0 to the wireless network [25]. The enterprises are benefitted with the advances in the technology which led to digitalization, the Internet of Things (IoT). It has become important across sectors including manufacturing. These terms are used to define the Fourth Industrial Revolution (Industry 4.0) [26].

3.4 Social Impact of Industry 4.0

Industry 4.0 has a deep impact on culture, factories, households, the public sector, economies and so on. Developing nations, such as China and India, are already preparing and implementing Industrial policies. They have trained work force for specific skills and work in the past. This is not feasible with the introduction of Industry 4.0, because extremely skilled carriers are needed. Some skills may not be required in Industry 4.0 environment and some new skills will be required. Industry 4.0 provides possibilities such as enhanced efficiency, decreased waste, circular economy advancement and more viable manufacturing and usage habits. Industry 4.0 needs the implementation of various prerequisites. The most significant variables are certainly digital abilities. Additionally, other substantial characteristics are automation and big data analytics that associate all of a system's stakeholders and build an intelligent network that communicates information in real time. The appropriate application within a business of Industry 4.0 depend on its ability to respond to shift and governance of technology. Industry 4.0 can transform social environment of

developing nations by helping them for reducing poverty, best healthcare with lowest cost, increasing farmer's income by providing new technologies and equipment.

3.5 Impact of Industry 4.0 on Business Environment

Apart from product and processes, Industry 4.0 will have main effect on business environment. As real time data will be streamed from PoS (Point of Sales), business decisions will be faster and flexible. Automation will make many traditional jobs extinct and totally new types of jobs will be created. New technology is an important factor of future business environment. In a paper by [27] authors find it essential to see how an Industry 4.0 drive organizations and business models. The model shall be capable to guide old and new organizations for implementation of Industry 4.0. Competitiveness of the companies are determined by flexibility and specific cost of manufacturing. As per [28] the main objective of Industry 4.0 is to create more complex manufacturing systems where productivity of intermittent manufacturing and specific cost is realized. Quality assurance faces new challenges due to increase in complexity in manufacturing after deploying Industry 4.0. Stock [16] in their paper examines the role of Industry 4.0 benefactors and their influence on advances in the processes. The role of small and medium-sized enterprises (SMEs) which provide Industry 4.0 based solutions is important as they provide access to Industry 4.0 by this to their customers. Predictive maintenance is now days used extensively in industries to monitor status of the equipment and predict potential failures. Predictive maintenance helps industry to reduce breakdowns and operating cost. Erol [29] in their paper explains the importance of digitalization and role of Industry 4.0 in predictive maintenance.

While reviewing the literature, the following gaps are observed. There is a need to adopt Industry 4.0 in different industries (manufacturing, services and IT industries) to understand the effect of the enhancement the results of a company [15]. The concept of Industry 4.0 shall be clear which will make its implementation easier to organizations and adopt methods suggested in literature. Present literature is more focussed on manufacturing. If entire supply chain from upstream to downstream is considered, we can measure actual effect of Industry 4.0. Industry 4.0 have presence mainly in manufacturing sectors. Authors can explore other sectors, such as the infrastructure, agriculture and food sectors. One of the most critical problems is that most companies do not have a generalized Industry 4.0 execution model. Therefore, in various phases of the application of Industry 4.0, there are no definite instrument uses. There is little research done on social impact of Industry 4.0. This is because Industry 4.0 is still a novel idea and we have to wait to see, if any social impact it creates. However, industry leaders and policy makers can anticipate the impact and prepare future policies accordingly.

4 Implementation Plan for Industry 4.0

Implementation of Industry 4.0 is inevitable for industries. However industries shall prepare for financial and cultural impact. Implementation of Cyber Physical System and Big data analytics create new avenues in product and service quality [28]. Though large industries can design strategy and make investment, SMEs need different strategy [27]. Main prerequisite for Industry 4.0 implementation is developing new skills in employees. Distinguishing the anticipated modifications with the Industry 4.0 system execution is crucial. The execution of Industry 4.0 in developed countries includes several difficulties: The need for testing and teaching, to allow businesses to reinforce their company data burst, to transmit information faster and faster and to boost data volume. Implementing an Industry 4.0 involves significant variations in the businesses. Since industries need to be digitalized, it requires strong investments. Apart from investments, there is also a necessity for strong leadership so as to encourage the proposed changes. The incompetence in predicting return on investment is one most important hurdle for implementing the process of digitization, and this drives many companies not to invest. As per the study by Accenture and General Electric, Big data analytics is crucial as most of the operations needs to be managed by smart sensors so as to transfer enormous volumes of data in short span of time. The major mission of an operator is to obtain and investigate the data and add value to generate business opportunities. Another challenge faced by the organizations is the data security. They need to develop certain standards to ensure communication between smart systems without any external interference so that the data is not leaked. Its necessary for the organizations to retain the confidence of the customer of their information and gain competitive advantage.

5 Issues and Challenges in Industry 4.0

The pace of change in technology is so high that for traditional manufacturing, it is difficult to catch this pace. In an intelligent manufacturing system more decision making autonomy is required which is lacking in current system [30]. Insufficient capability of present IWN for providing sufficient bandwidth required for high volume data transmission. To get reliable implementation partner and allocate resources [6]. Getting data, analysing it for benefit of manufacturing, to implement data driven culture is a big challenge. Systems should be modelled for self-organised manufacturing system in Industry 4.0. Cyber security threats are very high in Industry 4.0 due interconnected systems inside and outside organizations. Industry shall find solution for this challenge. Modularized and flexible physical artefacts: Equipment for machining or testing shall be combined for distributed decision making when processing a product. Therefore, there is a requirement to construct a flexible and smart conveyor device that can vigorously reorganize the manufacturing tracks.

6 Conclusion

The purpose of this work is to concentrate on the idea fourth industrial revolution, termed as Industry 4.0. It discusses the ongoing research on application of Industry 4.0. With the advent of Industry 4.0, the production can become smarter, competent, effective, personalized at an affordable price. This allows the machines to learn from each other Digitization is going to have a long-lasting effect on the working background. This expansion provides the full variety of prospects for the manufacturing sector to develop its important universal situation by expanding the prevailing produce and service collection so as to guaranteed progress in sales. The execution of the Industrial Internet signifies a multi-year conversion procedure for most of the companies, causing in significant changes to their value chains. Industries and countries will hold Industry 4.0 at varied proportions and in altered ways. Industries with a high level of product variants, such as the automotive and food-and-beverage industries will benefit from a greater degree of flexibility that can create efficiency in industries that claim high value, such as semiconductors and pharmaceuticals, and reduce error rates. More research on effect of Industry 4.0 implementation on developing countries is required. Especially there will be huge impact on society and business. In order to have a smooth transmission, the producers and suppliers need to hold on to the advances in technology and adjust to the suitable infrastructure and knowledge. The findings in this paper are very crucial for industry leaders, policy makers, governments, researchers, decision makers and professionals.

References

1. K. Witkowski, Internet of Things, big data, industry 4.0-innovative solutions in logistics and supply chain management. Procedia Eng. **182**, 763–769 (2017)
2. S. Vaidya, P. Ambad, Industry 4.0—a glimpse. Procedia Manuf. 233–238 (2018)
3. A. Pereira, F. Romero, A review of the meanings and the implications of the Industry 4.0, in *Manufacturing Engineering Society International Conference 2017, MESIC 2017*, 28–30 June concept 2017, Vigo (Pontevedra), Spain concept (2017), pp. 1206–1214
4. T.H.-J. Uhlemann, C. Lehmann, The digital twin: realizing the cyber-physical production system for industry 4.0 (2017), pp. 335–340
5. N. Szozda, Industry 4.0 and its impact on functioning of supply chains. Logforum 13(4), 401–414 (2017)
6. P. Sarvari, Technology Roadmap for Industry 4.0. inbook (2018), pp. 95–103
7. J. Lee, H.-A. Kao, Recent advances and trends of cyber-physical systems and big data analytics in industrial informatics (2014)
8. H.D. Ardakani, S. Yang, Industrial big data analytics and cyber-physical systems for future maintenance and service innovation (2015), pp. 3–7
9. D. Ibarra, J. Ganzarain, Business model innovation through Industry 4.0 (2018), pp. 4–10
10. S. Gierej, The framework of business model in the context of industrial Internet of Things (2017), pp. 206–212
11. A. Riel, C. Kreiner, Integrated design for tackling safety and security challenges of smart products and digital manufacturing (2018), pp. 4–8
12. B. Magdalena, M.K. Wyrwicka, Towards lean production in Industry 4.0 (2017), pp. 466–473

13. S.T. Newman, R.Y. Zhong, Intelligent manufacturing in the context of Industry 4.0 (2017), pp. 616–630
14. A. Jager, P. Hold, Tangible Industry 4.0: a scenario-based approach to learning for the future of production (2016), pp. 13–18.
15. M. Fiorentino, S. Debernardis, Augmented reality text style readability with see-through head-mounted displays in industrial context (2013, September 24), pp. 111–126
16. T. Stock, G. Seliger, Opportunities of sustainable manufacturing in Industry 4.0 (2016), pp. 536–541
17. A. Albers, B. Gladysz, Procedure for defining the system of objectives in the initial phase of an industry 4.0 project focusing on intelligent quality control systems (2016), pp. 262–267
18. T. Gartzen, G. Schuh, Promoting work based learning through Industry 4.0 (2015), pp. 82–87
19. D. Kolberg, D. Zühlke, Lean automation enabled by Industry 4.0 technologies (2015), pp. 1870–1875
20. U.M. Dilberoglu, B. Gharehpapagh, The role of additive manufacturing in the era of Industry 4.0 (2017), pp. 545–554
21. L. Safar, J. Sopko, Concept of SME business model for Industry 4.0 environment. TEM J. **7**(3), 626–637 (2018, August)
22. B. Illes, P. Tamás, New challenges for quality assurance of manufacturing processes in Industry 4.0. Solid State Phenomena **261**, 481–486 (2017)
23. J.M. Mülle, S. Däschle, Business model innovation of Industry 4.0 solution providers towards customer process innovation. Process **6**(260), 1–19 (2018)
24. P. Poor, J. Basl, Predictive maintenance as an intelligent service in Industry 4.0. J. Syst. Integr. **1** (2019)
25. M. Rubmann, M. Lorenz, Industry 4.0: the future of productivity and growth in manufacturing industries (2015, April 09), pp. 1–14
26. R. Neugebauer, S. Hippmann, Industry 4.0—form the perspective of applied research, in *49th CIRP conference on Manufacturing Systems* (2016), pp. 2–7
27. K.D. Thoben, S. Wiesner, Industry 4.0 and smart manufacturing—a review of research issues and application examples. Int. J. Autom. Technol. 4–16 (2017)
28. K. Sipsas, K. Alexopoulos, Collaborative maintenance in flow-line manufacturing environments: an Industry 4.0 approach, in *The CIRP Global Web Conference Research and Innovation for Future Production.* Procedia CIRP 236–241 (2016)
29. S. Erol, A. Jäger, Tangible Industry 4.0: a scenario-based approach to learning for the future of production, in *6th CLF—6th CIRP Conference on Learning Factories.* Procedia CIRP 13–18 (2016)
30. S. Simons, P. Abe, Learning in the AutFab—the fully automated Industrie 4.0 learning factory of the University of Applied Sciences Darmstadt, in *7th Conference on Learning Factories, CLF 2017*. Procedia Manuf. 81–88 (2017)

A Comprehensive Survey on Trust Management in Fog Computing



Sheenu Singh and Meetu Kandpal

Abstract Fog computing—an add-on of cloud computing—is an emerging computing paradigm having the capabilities to address the requirements of Internet of Things (IoT). Fog is well suited to find the key for latency, and bandwidth issue exists in cloud computing to fulfill the demand of IoT. Due to decentralized distributed nature of fog, several security and privacy challenges exist when fog nodes work together and exchange data to execute certain piece of work. One of the issues is how to establish reliable and trusted communication between fog nodes in fog layer. Trust is the level of assurance that is calculated on the basis of communication behavior used to detect malicious fog nodes in network (Patwary, Abdullah Al-Noman, et al. "FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain." Computer Communications 162 (2020): 212–224.). The conventional authentication methods (password based, certificated based and biometric based) will not work in fog because of its unique architecture. Additionally, it also consumes significantly more computation power and provokes latency issue. This survey paper discusses the fog computing three-layer architecture, state-of-the-art models and identifies various trust and security open challenges in fog computing.

Keywords Access control · Fog computing · Trust management · Trust computing · Malicious fog node · Attack · Authentication · Security · Privacy · Cloud computing

1 Introduction

As Internet of Things (IoT) [26] referred as the Internet of objects emerges continuously, a large number of smart IoT objects are connected to the Internet and generating

S. Singh (✉) · M. Kandpal
L.J. Institute of Computer Applications, L J University, Ahmedabad, Gujarat, India
e-mail: sheenu.singh@ljinstitutes.edu.in

M. Kandpal
e-mail: meetu.joshi@ljinstitutes.edu.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_9

tremendous data every second. Looking to the future, according to Cisco's Annual Report (2018–2023), the number of devices connected to IP networks will be more than three times the global population by 2023 [1]. Cloud is powerful for data storage and data processing, but fog can solve the issues of high energy utilization, heavy communication bandwidth burden and inadmissible latency arises due to growing volume of data. Fog has many applications in areas like smart city, health care, smart traffic, smart vehicles, smart grids, smart agriculture, etc. As compared to cloud, fog is more secure because local fog node analyzes the data that is situated in close proximity to the data source and difficult for unauthorized access. The existing security methods cannot be directly applied to the fog due to its geographically distributed, decentralized, mobility, dynamic and heterogeneity nature. This paper reviews the security and trust concern in fog environment especially in fog-to-fog collaboration. Further, this survey paper is structured as follows. Section 2 details the fog architecture along with security and trust issues, Sect. 3 summarizes related work, and Sect. 4 concluded the survey paper and explored upcoming challenges.

2 Background

2.1 Fog Computing Architecture

Fog computing is one of modern virtual platforms that administer data storage, data processing and provide network services between edge devices and cloud [2–4, 28]. Fog architecture composed of end devices, fog layer and cloud layer as shown in Fig. 1. The bottom-most layer (also called as thing) comprises of IoT devices, sensors, actuators and gateways. In middle layer (fog), fog nodes are interconnected in the core network. The top-most layer (cloud) is far away from edge where cloud components are located for big data processing. Moreover, cloud layer is the core of fog computing which performs data virtualization, data analysis, machine learning, and upgrades rules and patterns in the fog layers. In this architecture, bidirectional communication exists between fog–edge, fog–fog and fog–cloud.

End devices layer: It is also known as *Things layer.* It consists of several edge devices (physical devices) where data is generated. This layer includes devices like sensors, actuators, smart phones, smart meters, smart home, smart agriculture, smart-cards, etc. Here, edge devices are enabled with their identification and facilitated with communication protocol (Wi-Fi, Bluetooth, NFC, Zigbee, cellular, etc.). These protocols permit to channel the produced data to the fog layer.

Fog layer: This is a network of interconnected geographically distributed decentralized fog nodes. Fog nodes include devices like gateways, router, base stations, access points, fog servers, etc. This layer handles data collection, data filtering, data processing, data compression and data uploading. Fog nodes store only recently used data and can process only significant amount of data temporarily. On the flip side for

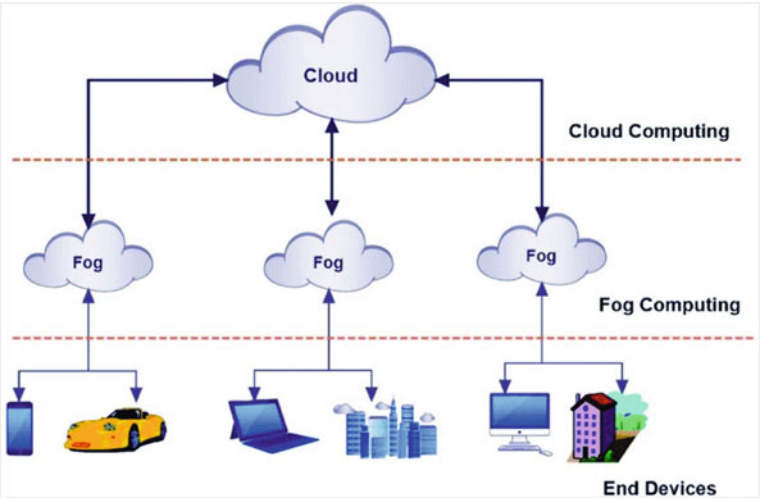


Fig. 1 Three-tier fog computing architecture [7]

large datasets, fog node can send request to other fog node or cloud in the network to process and control.

Cloud layer: It consists of data centers having high storage and efficient processing capacity to handle heavy services that fog layer unable to perform like big data processing. Cloud layer performs computational analysis, and data is stored permanently which can be accessed anytime by the users.

Fog architecture akin to other distributed architecture is designed upon networking components [3]. Every fog node is independent fog node but can serve for limited service request. At the time of computational offloading, task may switch between fog nodes. Because of distributed, decentralized and open nature of fog computing, security and trust issue exists. One of them is to establish trusted communication between fog nodes in fog network.

2.2 Trust Management System

Ghazvini et al. [15] Trust exist in almost all sciences, including management, networking, economics, philosophy, computing, etc. Trust is the level of faith to predict the behavior of object. Fog is decentralized, distributed and open computing environment where numerous fog devices participate from different geographical locations. Fog devices are owned by different independent owners, and they can join and leave fog networks dynamically [5]. One security mechanism is access control which describes access rights of an object on another object.

Patwary et al. [11] traditionally, authentication with access control protocols like password-based, ticket-based system, public key-based, biometric-based, certificate-based solutions, etc. was used. Password-based authentication techniques are inadmissible because it is difficult to manage password of massive number of devices connected in a distributed network and may exposed to dictionary/Brute force attack. Biometric-based authentication has powerful potential to provide security in various applications like banking machine, personal computer, credit card, military bases, etc. but not suitable for fog computing, especially IoT devices as it is time-consuming to process it. Certificate-based authentication approach convey information about holder that expires automatically that cannot be forgotten and guessed like password. Along with advantages, it also have limitations like (1) infrastructure is required to manage the issuing of certificates, (2) certificate must be distributed with care as it automatically grant access and (3) scalability challenge an intermediate authority is required to manage and verify certificate (4) may lead to latency issue. These protocols cannot be fit in the distributed architecture of fog, and they also require encryption/decryption, heavy processing and storage.

Trust management term coined by Blaze et al. [23] is a unique approach to define and interpret security policies, credential information and relationships that allow direct authorization to take security critical actions. Trust management systems calculate the trust value of fog node and reflect the opinion of one fog node on the trustworthiness of another fog node. It classifies the network object into trusted, untrusted and uncertain fog nodes that are trusted fog node and malicious fog node. Malicious node is a node that is already authenticated, and it is already a part of system which is a threat for whole network. Malicious node may make an effort with different attacks to increase its trust values. Table 1 listed various trust attacks within fog.

Trust computing methods can be classified into five dimensions: trust composition, trust propagation, trust update, trust formation and trust aggregating as shown in Table 2 [8]. Trust composition decides what trust parameters and sub-parameters are included to calculate trust value of fog node [6]. Trust parameters can also be

Table 1 Trust-specific attack

Trust attack	Description
Self-promotion attack	In this attack, malicious node increases its trust value by giving good recommendation about itself
Bad-mouthing attack	Collectively in group, malicious node gives bad recommendation about a good node that will decrease its trust value
Ballot-stuffing attack	In this type, one malicious node gives good recommendation about other malicious node to raise its reputation
Opportunistic service attacks	In this kind of attack when malicious node reputation dropped, then it starts performing good services to regain its reputation
On–Off attack	Here, both good and bad services are performed by malicious node randomly to avoid being recognized as a bad node

Table 2 Trust Dimension. Trust parameter and Sub-Parameter

Tire trust dimension		
Trust composition	Trust parameter	Trust Sub-Parameter
	QoS (Quality of Service)	Latency, transmission energy, packet loss ratio, reliability, cooperative, capability, response time, throughput, node service rate, end-to-end packet forwarding ratio, competence
	QoSec (Qualitv of Security)	Confidentiality, integrity, availability, access control, location, device configuration detail
	Social trust	Honesty, friendliness, service reputation, similarity , cooperativeness, community of interest, centrality, connectivity
	Past reputation	Experience satisfaction, time duration
	Recommendation	Recommendation from neighboring node/community node are used for evaluation
	Feedback rating	Service requester give feedback to service provider
Trust propagation	Centralized	Centralized entity for instance, the cloud or trusted entity' is responsible for storing trust values to all objects in Network
	Distributed	In this approach every object has the responsibility of storing and computing trust values
Trust update	Event-driven	Trust value is updated after an event and can be stored locally, shared or centralized
	Time-driven	Trust value are updated periodically with fixed time intervals
Trust formation	Single trust	Only one property is considered like QoS
	Multiple trust	Several Trust properties are taken into account to compute trust
Trust aggregation	Belief Theory, Bayesian systems. Fuzzy logic. Weighted sum (static or dynamic), regression analysis, subjective logic, logistic Regression	How to collect experiences from objects in the network. It can be both centralized and distributed manner

categorized into direct trust and indirect trust. Direct trust parameters means direct interaction between fog nodes like QoS, QoSec and past experiences. Indirect trust parameters mean indirect fog interaction that is based on recommendation/feedback from other nodes. Trust value is calculated considering both types of trust parameters because when fog node is new in network and it does not have past record, then its trust value will be based on recommendations from other fog nodes. The node having highest trust value will be selected during fog–fog collaboration. Trust propagation is distributed and can be updated periodically or after event. Trust formation will be multi-trust because in fog network, their exist node having no prior interaction so for first time recommendation may be considered along with QoS/QoSec parameters [9]. According to fog computing nature, fog node trust is dynamic, subjective, asymmetric, context dependent and may not transitive. Along with providing security, trust management can also help in rendering other tasks like while deciding to add new fog node and selecting fog node dynamically with different parameter to hide the object location. It also helps in switching between fog nodes at the time of computational offload and former node failure.

3 Related Works

Recently, a limited research is driven out to establish trusted communication between fog nodes in distributed fog network. There are many types of trust models in cloud such as agent based, log based, feedback based, authentication based and based on SLA (service level based) [15–21] but directly cannot be implemented because of distributed nature of fog. With context to fog computing, the trust model should be mutually authenticated, dynamic and distributed. Fog computing is not centralized so its security measures must be distributed, no central authority, fog nodes mutually establish trusted connection among each other, where nodes can be dynamically added and removed. The below Table 3 represents a survey on Trust Management techniques.

Existing trust model can be categorized into two types: first, trust establishment on the basis of direct interaction or direct observation and second, when there is no past interaction, node will collect local/global/community recommendations from other node in network and identify malicious node prior to interaction. Trust model based on recommendation is vulnerable because of dishonest behavior of other nodes in network and may fall prey to bad-mouthing, ballet-stuffing security attack [4]. Al-Khafajiy, Mohammed, et al. known as COMITMET, used direct observation as quality of service (QoS) and quality of protection (QoP/QoSec) along with recommendation as indirect trust parameter. Shabut, Antesar and connected too many nodes in network [10]. Alemneh, Esubalew et al. proposed two-way trust management system where service requesters and service providers check each other trustworthiness to request and response services. The system uses both QoS as direct observation and social trust as recommendation to calculate trust value of fog nodes.

Table 3 Survey on trust management techniques

Study	Trust model	Computing environment	Parameters	Results
Al-Khafajiv et al. [4]	Past-experience, Recommendation based model	Fog-fog	Experience satisfaction, Recommendation, SSLA. Response Time, Packet rate, Node service rate	This model identifies and reduces the malicious attacks/interactions among fog nodes. The accuracy of the proposed model is 66% while reducing service response time 15 s
Alemneh et al. [10]	Social-Trust, Recommendati on based model	Fog-client and fogserver	Latency, Packet Delivery Ratio, Ownership, Friendship (degree of closeness between nodes), interaction history, Honesty	Evaluation of the trust management model represents high accuracy, quick convergence and is resilient to trust-based attacks
Ghazvini et al. [23]	Feedback rating based model	Cloud	Cloud user's feedback rating	Proposed model filters the invalid feedback and sparse feedback, then it increases the quality of feedback by predicting feedback to improve feedback based trust management system
Patwary et al. [11]	Blockchain-based	Fog-fog	Location, fog device configuration detail	The proposed method met security requirement such as data confidentiality, integrity, mutual authentication, devices anonymity that was resilient against common cyber attack

(continued)

Table 3 (continued)

Study	Trust model	Computing environment	Parameters	Results
Ai-Breiki et al. [12]	Block chain based-Smart Oracles	Cloud-fog	Location, cost, availability, Response Time, Throughput, Service duration, Status, Device ID	In proposed work "Markov Fog nodes ranking model "which uses fog-cloud historical interactions to select the fog node. For trust related attribute data provider smart oracle is used. Smart contacts are written between trustor and trustee to provide distributed security and privacy. Only Smart contract time is considered for trust evaluation
Ogundoyin and Kamil [6]	AHP based framework	Fog	Qos, QoSec. Social relationships, past reputation, Recommendation	The proposed work identifies and give priorities to the trust parameters for both Service Requester (SR) and service provider (SP) For SR->SP parameters priority are (1) Qos (2) QoSec (3) Recommendation For SP->SR (1) social relationships (2) past reputation Latency is top rated parameter locally and highest ranked global in case of direct trust. Then, confidentiality, reliability, integrity
Daoud et al. [13]	User access control schema based trust model	Cloud-Fog-IOT	Access history, type of used host, users localization	This model has favorable impact on network usage and average latency that depends on user

In Ghazvini et al. [15] the trust value is calculated from cloud user's feedback and also address the problem of invalid and sparse feedback rating in feedback-based trust model. Patwary et al. [11], Al-Breiki et al. [12] address trust management in a block chain based on location parameter. These models uses ethereum IDE. Ogundoyin et al. [6] used fuzzy analytical technique to identify and priorities the trust parameters (direct and indirect) that is different for both service requestor and service provider [13]. Daoud, Wided Ben et al. proposed TACRM model which developed a clustering algorithm for security and resource allocation based upon priority.

4 Conclusions and Future Challenges

The earlier section surveys the most popular trust models and categorizes it into recommendation based, reputation based, social trust, feedback based or combination of them. These trust management techniques are assessed on the basis of trust matrices such as accuracy, scalability and reliability. Blockchain technology is also used in some research paper to address mutual authentication between fog nodes, but it may face scalability and latency issues. New techniques are needed, because fog is highly distributed and need to interact with different hardware platforms provided by different vendors. So, security and trust management must be dynamic and distributed. There are still many open challenges related to security and trust management in fog computing as follows.

In fog architecture, no mature service-level agreement (SLA) is available that can work as threshold value for comparison of result that can help out to discover misbehaving node in network.

Additionally, most of the paper focused to discover malicious node but not considered collusive attack (malicious node of collaborative frauds). It is significantly important to prevent honest fog node from frauds; otherwise, it also becomes malicious node and collectively whole network may be malicious.

Next, determination of malicious node location is another interesting question for future challenge.

To gain more clarity for trust calculation, it is important to define what behavior classifies a node as malicious node in fog computing [9]. Lastly, above hints and challenges are suggested to develop more secured and efficient trust model in fog computing.

References

1. M. Al-Khafajiy, T. Baker, H. Al-Libawy, Z. Maamar, M. Aloqaily, Y. Jararweh, (2019) Improving fog computing performance via fog-2-fog collaboration. Fut. Gener. Comput. Syst. **100**, 266–280. ISSN 0167-739X

2. P. Zhang, M. Zhou, G. Fortino, Security and trust issues in fog computing: a survey. Fut. Gener. Comput. Syst. **88**, 16–27 (2018)
3. Z. Su, et al., Toward architectural and protocol-level foundation for end-to-end trustworthiness in Cloud/Fog computing. IEEE Trans. Big Data (2017)
4. M. Al-Khafajiy, et al., COMITMENT: s fog computing trust management approach. J. Parallel Distrib. Comput. **137**, 1–16 (2020)
5. J. Guo, R. Chen, A classification of trust computation models for service-oriented internet of things systems, in *2015 IEEE International Conference on Services Computing*. (IEEE, 2015)
6. S.O. Ogundoyin, I.A. Kamil. A fuzzy-AHP based prioritization of trust criteria in fog computing services. Appl. Soft Comput. **97**, 106789 (2020)
7. https://images.app.goo.gl/gkFfkyAejGCYjvXi8
8. J. Guo, I.R. Chen, J.J.P. Tsai, A survey of trust computation models for service management in internet of things systems. Comput. Commun, **97**, 1–14 (2017)
9. T.S. Dybedokken, Trust management in fog computing. MS thesis. NTNU (2017)
10. E. Alemneh, et al., A two-way trust management system for fog computing. Fut. Gener. Comput. Syst. **106**, 206–220 (2020)
11. A.A.-N. Patwary, et al. FogAuthChain: a secure location-based authentication scheme in fog computing environments using Blockchain. Comput. Commun. **162**, 212–224 (2020)
12. H. Al-Breiki, et al., Trustworthy blockchain oracles: review, comparison, and open research challenges. IEEE Access **8**, 85675–85685 (2020)
13. W.B. Daoud, et al., TACRM: trust access control and resource management mechanism in fog computing. Human-centric Comput. Inform. Sci. **9**(1), 1–18 (2019)
14. M. Al-Khafajiy, et al., Improving fog computing performance via fog-2-fog collaboration. Fut. Gener. Comput. Syst. **100**, 266–280 (2019)
15. G.A. Ghazvini, et al., A new multi-level trust management framework (MLTM) for solving the invalidity and sparse problems of user feedback ratings in cloud environments. J. Supercomput. **77**(3), 2326–2354 (2021)
16. S. Singh, J. Sidhu, Compliance-based multi-dimensional trust evaluation system for determining trustworthiness of cloud service providers. Fut. Gener. Comput. Syst. **67**, 109–132 (2017)
17. L.H. Vu, M. Hauswirth, K. Aberer, QoS-based service selection and ranking with trust and reputation management, in *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems."* (Springer, Berlin, 2005), pp. 466–483
18. S.S. Yau, J. Huang, Y. Yin, Improving the trustworthiness of service QoS information in service-based systems, in *International Conference on Autonomic and Trusted Computing*. (Springer, Berlin, 2010), pp. 208–218
19. Q. He, J. Yan, H. Jin, Y. Yang, ServiceTrust: supporting reputation-oriented service selection, in *Service-Oriented Computing*. (Springer, Berlin, 2009), pp. 269–284
20. M.K. Muchahari, S.K. Sinha, A new trust management architecture for cloud computing environment, in *2012 International Symposium on Cloud and Services Computing*. (IEEE, 2012), pp. 136–140
21. M. Tang, X. Dai, J. Liu, J. Chen, Towards a trust evaluation middleware for cloud service selection. Fut. Gener. Comput. Syst. **74**, 302–312 (2017)
22. A.M. Shabut, et al., Recommendation based trust model with an effective defence scheme for MANETs. IEEE Trans. Mob. Comput. **14**(10), 2101–2115 (2014)
23. M. Blaze, J. Feigenbaum, J. Lacy. Decentralized trust management, in *Proceedings of the 17th Symposium on Security and Privacy*. (IEEE Computer Society Press, Los Alamitos, 1996), pp. 164–173
24. R.K. Naha, S. Garg, D. Georgakopoulos, P.P. Jayaraman, L. Gao, Y. Xiang, R. Ranjan, Fog computing: survey of trends, architectures, requirements, and research directions. IEEE Access **6**, 47980–48009 (2018)
25. R. Mahmud, R. Kotagiri, R. Buyya, Fog computing: a taxonomy, survey and future directions, in *Internet of everything*. (Springer, Singapore, 2018), pp. 103–130

26. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Personal Identification Using Fuzzy Approach and RSA Algorithm

Sharmila S. More, Bhawna Narain, and Bharat T. Jadhav

Abstract When we exchange the data via network, we need more security. Security is main part in data communication. In this paper, we have to discuss how fuzzy logic is used in RSA algorithm for securing communication. Multimodal images use the fuzzy logic FIS rules to design 64 bits blowfish algorithm which increase security and improve the performance. This algorithm helps to protect the data from unauthorized access and runs faster. The proposed algorithm is designed using MATLAB R2017a. We also discussed advantages and disadvantages of fuzzy and RSA algorithm.

Keywords Blowfish · FIS · Fuzzy logic · Cryptography

1 Introduction

We know that biometric concepts were first developed and used by Joao De Barros in China in the fourteenth century, that is, Chinese merchants stamped palmprints and children's footprints on paper with paper ink, to differentiate young children from each other [16] (Fig. 1).

Figure 1 show a block diagram of the modes of the biometric system with registration and verification/identification process. The registration process is also called the enrollment process. The enrollment or registration process means that the user has registered their data first time. Initially, the user uses biometric data obtained from biometric sensors, then we process on data and then stored in the form template. This template will be used for a subsequent authentication process.

S. S. More (✉) · B. Narain
MATS School of IT, Raipur, India
e-mail: sharmilamore22@ycis.ac.in

B. Narain
e-mail: dr.bhavana@matsuniversity.ac.in

B. T. Jadhav
Yashvantrao Chavan Institute of Science, Satara, India
e-mail: btj21875@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_10

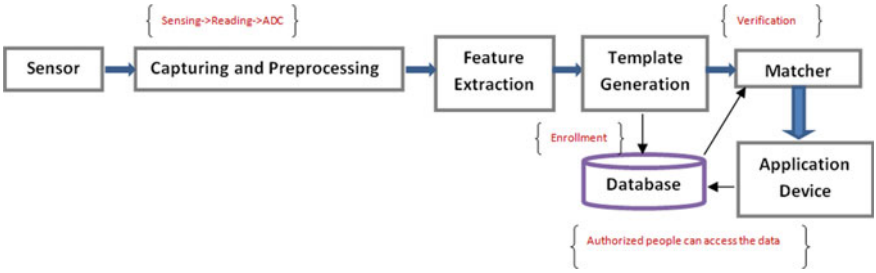


Fig. 1 Block diagram of biometric system

Fig. 2 Classification of biometric types using our dataset



1.1 Types of Biometric System

The biometric system uses the three stages namely capture, processing, and registration, but before that all these stages firstly go through verification and identification mode. Biometric techniques are classified into two classes' namely physiological and behavioral recognition systems.

Figure 2 shows the types of biometric system. As we know that biometric system is classified into two groups namely—physiological biometric recognition systems and behavioral biometric recognition systems.

1.2 Multimodal Biometrics

As we know that multimodal biometrics is actually a fusion of unimodal biometrics designed to overcome the problems of unimodality. These captured multimodal

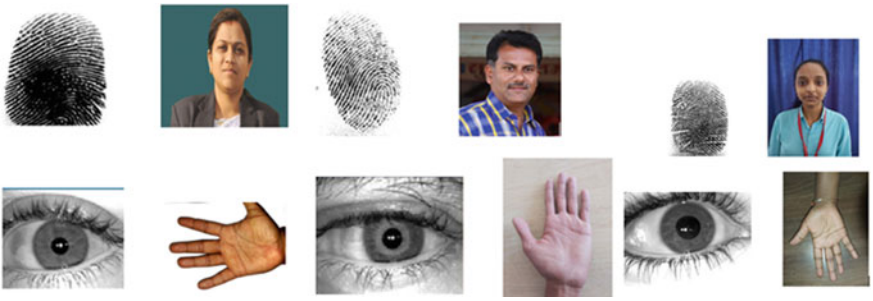


Fig. 3 Multimodal images from our dataset

biometrics are based on the combination of more than one type of biometric modalities or qualities, i.e., face, iris, fingerprint, and palmprint. As we know the multimodal biometric system¸ fusion is done in four levels such as sensor level, feature level, matching score level, and decision level. The final classification is based on the fusion of the output of the different features of captured images.

For our dataset, we are collected more than 5000 samples of multimodal images of face, iris, fingerprint, and palmprint images from school, college, and village. Figure 3 shows the face, fingerprint, iris, and palmprint dataset.

2 Fuzzy Logic

In personal identification, we use multimodal images of the iris, fingerprint, face, and palm as a dataset and by applying image processing algorithms on its fusion images. To find a precise result for our work and to minimize FAR, FRR, and FER, crisp logic has some difficulties in solving the problem of complexity, nonlinearity, precision, and ambiguity, so this is overcome by fuzzy logic optimization techniques. Specific logical concepts used with data mining, which overcome the problem of ambiguity, complexity, and nonlinearity in identification [15]. As we know that fuzzy logic contains the true or false statements, i.e., 1 or 0, it is not always possible to store precise information using only 1 or 0. Fuzzy logic is the very good approach of the control system for problem solving. It is an approach to computing based on "partial truth" or "degrees of truth," as we know that fuzzy logic concept was first introduced by Dr. Lofty Zadeh of the University of California at Berkeley in 1960 [3].

2.1 Why Fuzzy

In the fuzzy logic, fuzzy sets are suitable for recognizing shapes and classifying them. Fuzzy logic takes into account not only the value 1 or 0 but also truth values

between 0 and 1. Fuzzy logic is used to shorten the work of the system designer and calculate more accurate and time saving results [6]. Fuzzy association rules used to find an abstract co-relation between the different security features. These fuzzy association rules are easy to write and understand; so, fuzzy designer effectively describes the fuzzy system. It is very difficult to identify the extracted data, and this can be minimized by using fuzzy logic [11]. A fuzzy method requires less memory to store information and minimum time for model comparisons compared to clear logic. The fuzzy system requires fuzzy extractor, which is used to convert biometric data into random strings. These random strings easily apply on cryptographic algorithms, which are useful for the security of biometric data. They are used to encrypt and authenticate user records with biometric entries as a key. The fuzzy system requires auxiliary memory to store the bit sets. Fuzzy logic is a form of multivalued logic instead of fixed logic and process of extraction [15].

2.2 Fuzzy Logic and Mutimodal

As we know that fuzzy logic works on membership function, in digital image processing, membership function belongs to gray-level transformation. Multimodal has various digital images of biometric traits. Fuzzy logic is used to calculate intensity of pixels. Multimodal is combination of unimodal biomteric traits. We have tested the accuracy of multimodals by evaluating by the values of various parameters. Fuzzy logic is used in the evaluation process of multimodal.

3 Fuzzy Inference System for Proposed Algorithm

Figure 4 shows the fuzzy inference system (FIS) design of our new modified algorithm. Fuzzy association rules used to find an abstract co-relation between the different security features. The fuzzy association rules are easy to write and understand. It is up to the fuzzy designer to adequately describe the fuzzy system.

Figure 4 shows the fuzzy inference system design proposed algorithm rules using membership functions mf_1 and mf_2. Using above design, we are creating 19 fuzzy rules for fuzzy variable MSE, PSNR, SSIM, quality, and entropy of our proposed algorithm. These rules are defined using membership function mf_1 and mf_2. As we know that fuzzy works between 0 and 1, these membership function values are different for every fuzzy-based parameter namely MSE, PSNR, SSIM, quality, and entropy. The following table shows (Table 1).

1. For MSE parameter values, we have defined membership function mf1 between 0 and 0.5 and membership function mf2 between 0.4 and 1. The mid-values between mf1 and mf2 lie between 0.25 and 0.7, respectively.

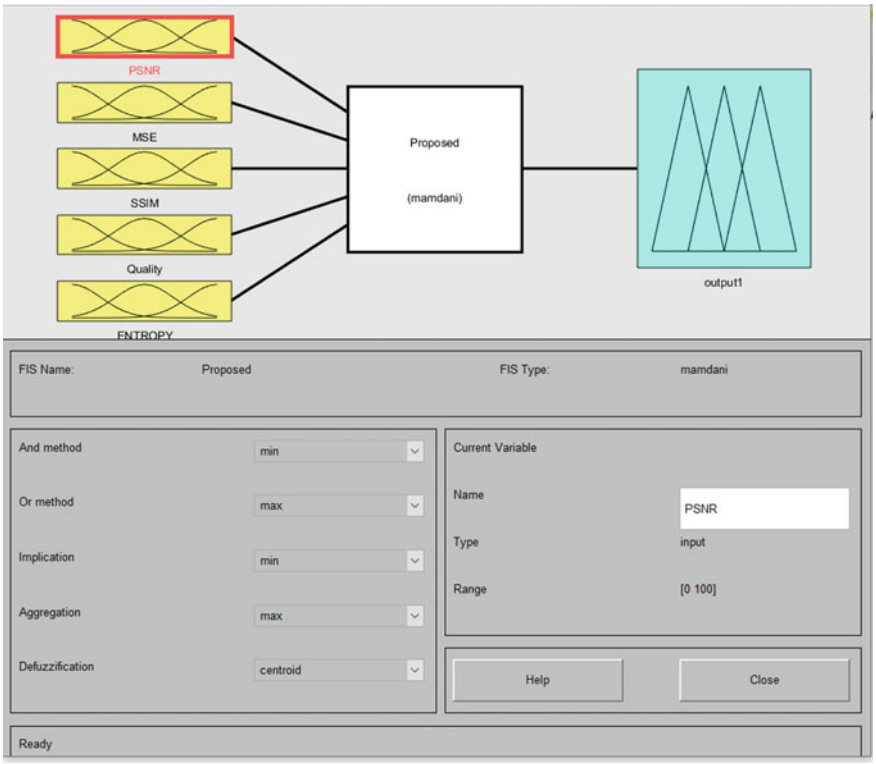


Fig. 4 Fuzzy inference system design for proposed algorithm

Table 1 Fuzzy logic parameters membership functions values

Fuzzy parameter	mf_1	mf_2	Mid-values	Result	Output
MSE	0–0.5	0.4–1	0.25–0.7	If values near to zero	Better
PSNR	0–35	35–100	17–65	If greater than 35	Better
SSIM	0–0.5	0.4–1	0.25–0.7	If greater than 1	Better
Quality	0–0.5	0.4–1	0.25–0.7	If greater than 1	Better
Entropy	0–0.5	0.4–1	0.25–0.7	If values near to zero	Better

2. PSNR parameter values—we have defined membership function mf1 between 0 and 35 and membership function mf2 between 35 and 100. The mid-values between mf1 and mf2 lie between 17 and 65, respectively.
3. SSIM parameter values—we have defined membership function mf1 between 0 and 0.5 and membership function mf2 between 0.4 and 1. The mid-values between mf1 and mf2 lie between 0.25 and 0.7, respectively.

4. Quality parameter values—we have defined membership function mf1 between 0 and 0.5 and membership function mf2 between 0.4 and 1. The mid-values between mf1 and mf2 lie between 0.25 and 0.7, respectively.
5. Entropy parameter values—we have defined membership function mf1 between 0 and 0.5 and membership function mf2 between 0.4 and 1. The mid values between mf1 and mf2 lie between 0.25 and 0.7, respectively.

These membership functions are defined according to proposed algorithm.

4 Rivest–Shamir–Adleman (RSA) Algorithm

As we know that Rivest Shamir Adleman algorithm is already developed in 1978 by three scientist Rivest Shamir Adleman. This algorithm is asymmetric algorithm means it used two different public and private keys for encryption and decryption process. We use these algorithms and evaluate these using our dataset of more than 5000 images.

4.1 Accuracy Test of Proposed Algorithms

To test the accuracy of algorithms, we have used various parameters such as sensitivity, specificity (TNR selectivity) (TPR, recall), false discovery rate (FDR), F1-score, FPR, and FNR. These parameters are used in our multimodal such as face, Iris, finger, and palmprint. The accuracy of palmprint is high, and accuracy of iris is low (Table 2).

The accuracy of palmprint is high, and accuracy of iris is low in table. Given table shows accuracy test of algorithms which we have to use to calculate various parameters such as sensitivity, specificity (TNR, selectivity) (TPR, recall), false discovery rate (FDR), F1-score, FPR, and FNR. This dataset is used in proposed algorithms for accuracy and performance evaluation.

Table 2 Accuracy testing of RSA algorithm

Accuracy	Sensitivity (TPR, recall)	Specificity (TNR, selectivity)	Precision (PPV)	False discovery rate (FDR)	F1-score	FPR	FNR	Multimodal
0.64	0	0.711111	0	1	0	0.111111	2.6	Face
0.57	−0.03226	0.644444	−0.1	0	−0.04878	0.122222	3.2	Iris
0.72	0.090909	0.777778	0.2	3	0.125	0.088889	2	Palmprint
0.6	0.03125	0.655556	0.1	2	0.047619	0.1	3.1	Finger

5 Conclusion

In this paper, we have discussed RSA algorithm related to security issues of multimodal using fuzzy logic was studied in detail. Proposed algorithm methodology and result analysis were also discussed. In this new algorithm, we found higher accuracy of encryption. In this algorithm, we have used fuzzy approach to increase the optimization for selection of personal identification. For all these processes, we have selected six parameters namely MSE, PSNR, SSIM, quality, entropy, and time complexity. Accuracy of person identification by using our algorithm was high.

References

1. A. Kumar, C. Wu, Automated human identification using ear imaging, www.elsevier.com/locate/pr. Received 3 September 2010 Received in revised form 5 May 2011 Accepted 24 June 2011
2. A. Kumar, B. Wang, Recovering and matching minutiae patterns from finger knuckle images. Pattern Recogn. Lett. (2015)
3. A. Jain, L. Hong, Y. Kulkarni, A multimodal biometric system using fingerprint
4. B. Narain, P. Shah, M. Nayak, Impact of emotions to analyze gender through speech, in *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, Solan, India (2017), pp. 31–34. https://doi.org/10.1109/ISPCC.2017.8269645
5. S.S. More, B. Narain, B.T. Jadhav, Data encryption standard algorithm in multimodal biometric image. Int. J. Comp. Sci. Eng. **6**(8), 869–874 (2018)
6. R. Fuller, Fuzzy logic and neural nets in intelligent systems (1999)
7. H.B. Kekre, T. Sarode, P. Natu, Performance comparison of walsh wavelet, kekre wavelet and slant wavelet transform in image compression. Int. J. Adv. Res. Comput. Commun. Eng. **2**(10) (2013). ISSN (Print) 2319-5940, ISSN (Online) 2278-1021, Copyright to IJARCCE www.ijarcce.com 3834
8. K. Bhargavi, S. Jyoth, An efficient fuzzy logic based edge detection algorithm. Int. J. Tech. Res. Appl. **4**(3), 194–196 (2016). e-ISSN 2320-8163, www.ijtra.com
9. S.s. More, B. Narain, B.T. Jadhav, Advanced encryption standard algorithm in multimodal biometric image, in *Advances in Biomedical Engineering and Technology. Lecture Notes in Bioengineering*, ed. by A.A. Rizvanov, B.K. Singh, P. Ganasala. (Springer, Singapore, 2021). https://doi.org/10.1007/978-981-15-6329-4_7
10. S.J. Shinde, J.G. Shinde, M.M. Kharade, H. Dhanashree, Biometrics: overview and potential use for E-governance services. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **4**(6) (2014)
11. A. Piegat, Fuzzy models, in *Fuzzy Modeling and Control. Studies in Fuzziness and Soft Computing*, vol. 69. (Physica, Heidelberg, 2001). https://doi.org/10.1007/978-3-7908-1824-6_5
12. S.S. More, B.T. Jadhav, Fuzzy logic approach for extracting biometric data, in *International Conference on Functional Materials@ Nanoscale: Concerns and Challenges*, 9–11 March 2015. ISBN 978-81-930740-0-8
13. S.S. More, B. Narain, B.T. Jadhav, Role of modified gabor filter algorithm in multimodal biometric images, in *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India (2019), pp. 1–5
14. S.S. More, B.T. Jadhav, Fuzzy logic algorithms for extracting biometric data, in *National Conference on Modern Approach for Green Electronics and Computing 2014*, p. 200. ISBN 978-81-928732-2-0

15. S.S. More, B.T. Jadhav, Overview of biometric systems, in *National conference Reflection: Emerging Drift*, in Wathar College, 27th December 2015. ISBN 978-93-85665-02-8
16. S.S. More, B.T. Jadhav, An overview on technologies used in biometric system, in *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4(2), February 2016. ISSN (Print) 2320-9798, ISSN (Online) 2320-9801, 5.618
17. S. Singh, R.K.B.S. Bansal, Comparative study and implementation of image processing techniques using MATLAB. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **2**(3) (2012). ISSN 2277 128X
18. S. Goyal, R. Wahla, A survey on image fusion. Int. J. Innov. Res. Comput. Commun. Eng. **3**(8) (2015). (An ISO 3297: 2007 Certified Organization), ISSN(Online) 2320-9801, ISSN (Print) 2320-9798
19. V. Kanhangad, A. Kumar, A unified framework for contactless hand verification. IEEE Trans. Inform. Forensics Sec. **6**(3) (2011)

ICT and Administrative Reforms: A Literature Review



Sridharan Kesavan, Aakansha Uppal, and Bhavna Pandey

Abstract This paper studies the concepts that come into play when Administrative Reform initiatives attempt to leverage ICT to meet their reform objectives. 'Grounded theory for literature review' is used as a methodology to extract the concept and their dimensions that influence the use of ICT in an Administrative reform environment. The literature review revealed that the factors affecting the ICT implementation in government have been well documented. But when ICT is used as part of an Administrative reform, consideration of factors at a project level alone was found to be insufficient. The initiatives should also consider the effect of the big picture on the projects. This consists of two important contextual concepts; ICT context and Reform context which are often ignored. In other words, why and how ICT is being used and why and how the administration is being reformed are two important questions that need to be answered by the initiative. Based on the outcomes of the review a descriptive framework consisting of four concepts and twenty-one dimensions has been theorized. This framework can be used both by the practitioners and the political/social leadership as a risk evaluation framework. This study makes an original contribution by incorporating the two macro-level concepts that affect ICT implementation in a reform environment. Thus, the model developed helps to mitigate the risks of neglecting the two critical elements of ICT-context and Reform-context.

Keywords Administrative reform · ICT · Public administration · ICT context · Reform context

S. Kesavan (✉)
Symbiosis Centre for Research and Innovation, Pune, India

A. Uppal
Symbiosis Centre for Management Studies, Noida, India

B. Pandey
Amity University, Mumbai, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_11

1 Introduction

Governments undertake various forms of reforms like social, economic, political, administrative, legal, and judicial [1–3] of which our interest is on Administrative Reforms (AR). Administrative Reform can be defined as 'the artificial inducement of administrative transformation' [1]. It also has the meaning of a major (or even radical) change introduced within the administration to improve its performance [4].

Administrations are reformed for various reasons, follow different means, produce varied outputs and achieve different outcomes [5]. Hence to understand Administrative reform as a simple change of administrative models would be erroneous. Many countries do not even change the models substantially, they are just interested in bringing about major improvements to their systems. Governments, in this context, seek to leverage ICT for Administrative reforms. Multidisciplinary fields, such as ICT for development (ICT4D), emerge due to the intersection of communication and development [6]. They develop ICT strategies, a component of which addresses ICT for improvement of administration [7]. This paper focuses on the use of ICT for Administrative Reforms.

The next section discusses some of the pertinent literature regarding Administrative reforms, followed by the methodology section, section four discusses results, and section five the summary and conclusions.

2 Theoretical Background

Administrative Reforms are carried out for various reasons like globalization, budgetary pressures, developmental or political [2, 8]. Reforms carried out for the sake of reforms themselves are seldom successful. They are effective only when associated with a major social or economic reform [1]. Thus, the overall context in which the reforms are being implemented will govern the reform process and the outcomes.

Operationally Administrative Reforms aim to change the structures, processes, and/or cultures of public sector organizations to get them to run better [2]. In some instances, governments use ICT as a strategy for Administrative reforms [9]. Viewed in that context ICT has caused a paradigm shift in the way organization are managed. This is not only applicable to the private sector but also to the public sector and government departments. Administrative reforms using ICT should take into consideration that governments are faced with the twin problem of having to modernize their organizations and also having to manage a changing society due to technical developments [10]. Thus, the overall ICT environment and direction that the government takes for the use of it become important considerations for the reform.

The concept of electronic government (e-government) is often referred to in the literature on Administrative Reform. The electronic government does not have a single definition [9] but can be conceptualized as the government's use of ICT

combined with organizational changes to improve the structures and operations of government [11]. The same concept has been expanded by Ndou [10] to say that e-government is the intersection of e-administration, e-society, and e-service/citizen [10]. The main blocks of e-government are defined in terms of relationships as; Government to citizen (G2C), Government to Business (G2B), Government to Government (G2G), Government to Employees (G2E), and Citizen to Citizen (C2C), of which most of the literature focuses on the first four [12]. Literature on e-government mainly discusses automation of simple processes and improvements at single locations. Though the lessons from these studies are valuable, they do not enhance our understanding of the role of ICT in the context of Administrative Reforms. The available literature focuses more on adoption, technology development, and citizen interface and less on sustainability, back office, ICT usage, and e-governance strategy [13]. This study is interested in understanding the concepts that come into play when ICT is used as part of Administrative Reforms.

3 Research Method

This research employed the 'grounded theory for literature review' methodology along with the concepts of open coding, axial coding, and 'concept matrix' [14, 15].

3.1 Search Strategy

This research, following the methodology suggested by Dias for the selection of databases [16] chose to use the Scopus database to retrieve the original data set. This database was used because it retrieved more entries for the intended search conditions than the other sources, thus, producing a bigger sample and also had the latest articles.

The aim was to keep the search at a certain level of aggregation by eliminating literature on non-strategic implementations. Through trial and error, the researchers arrived at the search criteria "Administrative Reform" OR "Administration Reform" OR "Public Administration Reform" OR "Government Reform" AND "ICT". Thus, eliminating literature related to e-government that was not at the reform level of aggregation. It also eliminated many articles in the technical (engineering) domain of ICT.

After having obtained the original set of 68 articles, an iterative process was employed as suggested by Wolfswinkel, et al. [14] to arrive at 53 articles for in-depth review. The last step of the iteration was identifying additional articles through forward-backward referencing. The process of iteration that was followed is shown in Fig. 1

Search based on keywords only was found to be not useful. As an example, of the original 68 articles, only 7 contained ICT as a keyword, whereas Government data

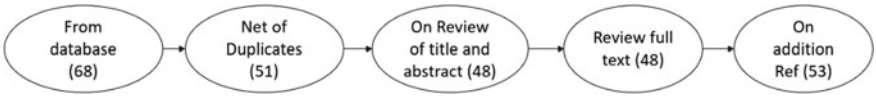


Fig. 1 Process for arriving at the sample

processing appeared in 18 of them. Hence it was concluded the nature of the article could only be ascertained after reading the abstract and the text carefully. The final list thus obtained contained articles that covered full administrative reforms or were pilots for full-fledged reforms.

3.2 Data Analysis

After finalizing the articles to be reviewed, the articles were grouped into categories for ease of reading and forward and backward referencing. Then the articles were read to identify the important concepts and dimensions emerging from them. The texts containing the dimensions were cut and pasted into a separate workbook, they were then reviewed to see if they had common threads appearing among them. Using the open coding methodology, the authors were able to get a list of codes that emerging out of the articles. Even before entering the axial coding phase, it was evident that themes or concepts were emerging from the articles even without aggregating the codes. These concepts were listed separately in a basic concept matrix and they were rationalized to produce the advanced concept matrix that mapped articles vs concepts. Parallelly the open codes were rationalized using axial coding and selective coding through an iterative process. These two parallel processes converged to produce 'concepts vs dimensions' matrix. It was found that the original concepts aligned with dimensions emerging out of the coding process. The process followed is depicted in Fig. 2.

Once the coding process was completed the articles were read again along with other reference materials to produce explanations for the concepts and the dimensions. This final analysis also produced the gaps in the dimensions, which indicated the areas for possible future research.

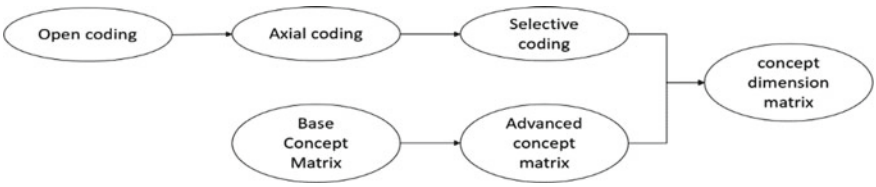


Fig. 2 Coding process

4 Results

The 53 articles were broadly categorized using two types of classifications. The first classification was based on the locations and nature of the department/agency in which the studies took place. There were three categories, 37 papers covered national department (s), 10 were from provincial structures and 6 were either from local governments or from single locations. The second classification of the same 53 articles was based on the nature of the subjects that were studied; 14 papers studied reforms across departments (multi-departments), 13 studied individual functions of the government departments (e.g., Tax collection, trade management, health system, etc.), 10 studied new channels like common service centers or other types of e-governance interfaces, 2 papers studied structural issues like introducing additional departments, 2 studied the phenomena of decentralization, 3 studied anticorruption measures, 3 studied the influence of the ICT strategy, 1 studied the phenomena of openness in government and the other 4 studied computer-science based views like database management, selection of Information System, Management Information System (MIS) and outsourcing, 1 paper studied reasons behind the effectiveness of ICT aid provided to countries to reform their administration. All the articles covered the influence of ICT on Administrative reforms. Thus, the 53 papers were not limited to any particular part of the government but covered various types of initiatives concerning ICT and Administrative reforms.

While reviewing the 53 articles it was seen that the articles broadly touched upon six concepts, with many-to-many relationship (the number in the bracket showing the number of articles); the context of ICT involvement (37), focus areas/outcomes of the intended reforms (22), what ICT was used for (19), types of ICT systems used (10), capacity building discussions (2), and factors affecting implementation (37). It was clear that the majority of the articles focused on the context of ICT implementation and the factors affecting implementation. On further analysis, it was found that the distinctions between 'What was ICT used for' and the 'type of ICT system' were blurring. Hence, they were merged as one concept. Similarly, capacity building discussions were found to be in the context of it being a factor affecting the ICT implementation. Hence the capacity concept was merged with factors affecting implementation. The concepts were then renamed for easy use. After the merger and renaming of the concepts, the numbers were; 'ICT Context' (37), 'Reform Context' (22), 'ICT Use' (21), 'Factors' (36). A concept-matric was built with concept centric approach as recommended by Webster and Watson [15]. The final concept matrix is given in Table 1.

Of the four concepts emerging, two of them, ICT context and Reform context, were at a context level and the other two, ICT use and factors, were at the project level. On further reading of the articles conducting content analysis, 222 single value dimensions were identified. 60 were listed under ICT context, 47 under Reform context, 33 under ICT use, and 82 under Factors. These single values were further organized under various dimensions. 6 dimensions emerged under each of the first two concepts, three under the third, and 17 on factors. The 17 dimensions were

Table 1 Concept matrix

Concepts	Papers addressing the concepts
ICT context	[9, 10, 17–50]
Reform context	[9, 17–19, 27, 30, 32, 42, 44, 46, 49, 51–57]
ICT use	[10, 13, 18–20, 22, 24, 28, 29, 32, 38, 43, 45, 48, 51–53, 55, 57–61],
Factors	[9, 18–36, 39, 40, 46, 47, 50, 55, 56, 58, 59, 61–66]

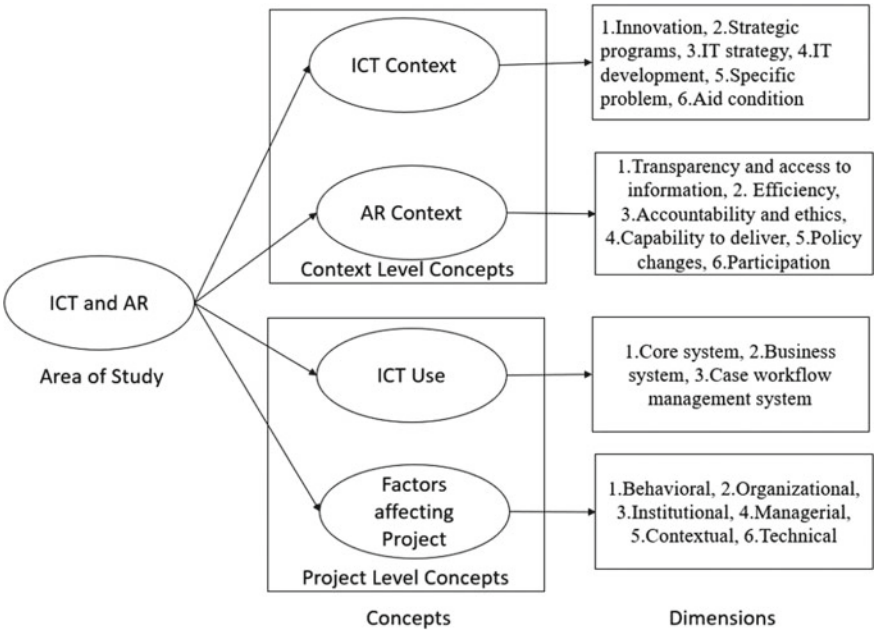


Fig. 3 Concepts for studying ICT in administration reform

further grouped into 6 dimensions. The outcome of the concepts and dimensions is depicted in Fig. 3.

4.1 Context of ICT

There are two main ways in which ICT comes into play in an Administrative Reform (AR); first, the AR is planned as a program, and ICT is integrated into the program as an enabler to achieve the program objectives. In this case, the context is that of the Administrative reform and ICT is one stream of the program [17] and ICT itself is neither a 'reform' nor an administrative model [2]. The second way is when a country formulates an ICT strategy and uses ICT in administrative Reforms within

the context of the ICT strategy. An example of such a move is the Digital-India program of the Indian government [7, 18]. Here, the context is set by the ICT strategy and administrative reforms play a role in accomplishing the ICT strategy objectives. Both of these perspectives hinge upon having an overall ICT framework to ensure effective use of ICT.

There are three other ways in which ICT can play a role in Administrative reforms. Firstly, ICT is brought in as part of an innovation drive/framework to solve operations problems. Beginning from the later part of the twentieth century innovation in government reforms was being widely used as a concept especially under the New Public Management (NPM) banner [17, 29, 39]. Secondly, ICT is brought in as and when a new ICT development happens, as in the case of, web technology, internet availability, mass data capability, etc. Examples include connecting a point-of-sale activity to the central database to improve the effectiveness of the public distribution system [62] and establishing Common Service Centers (CSC) as part of their G2C e-government program to leverage on web development [18]. Thirdly ICT is brought in to solve a specific problem in an identified area. This area could be end-to-end automation or one part of the process being automated. A case in point is using ICT to collect the property tax in Bangalore, India [63].

ICT also enters the Administrative reform domain in the context of aids being provided by outside agencies. These aids are conditional and the reform targets and strategies are stipulated by the aid providers [8, 19]. The literature review conducted has identified these six contexts in which ICT enters the AR domain.

4.2 Reform Context

The literature reviewed referred to six contexts of reforms; efficiency, accountability, transparency, participation, capability building, and policy change.

The contexts of improving efficiency and accountability were primary associated with the New Public Management (NPM) model of public administration. This model attempted to adopt business techniques to public administration. The context of transparency and participation were associated with the more recent New Public Governance model. This model attempts to democratize and decentralize public administration [67, 68]. Hence, whenever the objectives of the reforms are set within these four contexts the ICT projects will have to fit into strategic context as applicable to change of Public administration model.

There other two contexts of capability building and policy change do not intend to change the public administration model per se. Capability development could be achieved in the form of improvement to Human Resources capabilities [17] or by streamlining procedures [49]. New policy changes, mainly aiming at operational changes can be achieved by the introduction of new methods of working like providing round-the-clock service [46] or introducing new functions [29, 32].

Thus, the nature of ICT intervention in these contexts cannot be determined fully at the project level but will have to refer to a larger context.

4.3 ICT Uses in AR

The literature referred to three dimensions of ICT use in the context of Administrative reforms; core system, business systems, and case/workflow management systems.

The core systems are typically large database management systems where the core business-related information is captured stored, retrieved, and worked upon as in the case of health records or tax records [55, 63]. The business systems are used to manage the internal functions of organizations as in the case of HR or finance [32]. The Case/workflow management systems are the ones where transactions are managed. They could be integrated with the other systems or be standalone. These are the systems typically used in the Common Service Center (CSC) environment [18].

This concept is where there are significant gaps found in the literature reviewed. Although a property tax system [63], and electronic health record systems [55] were discussed there were seldom discussions about a full-fledged core system implementation. Similarly, though there were discussions about ICT use in planning, HR, and finance departments [32], there were seldom discussions about an ERP-level implementation. There seems to be a focus on the front-end systems like CSC [18] and point of sale automation [24]. There were no discussions in the selected papers on the enablement tools like analytics, document management system, etc.

This concept determines the standardization, integration, make-or-buy decisions, and leveraging the works of other parts of government. Selection of technology and tools and structure of implementations will have a long-lasting impact on the country, hence need to be carefully thought through within the ICT context and the AR context rather than at a project level.

4.4 Factors Affecting ICT and Administrative Reform

Of the four concepts that emerged out of the review, factors affecting ICT implementation is the one that has been most widely covered. 36 articles make direct reference to the factors that affect the implementation and each one of them covers multiple factors. The factors affecting implementations have been variedly categorized into success-drivers, success-enablers, failure-barriers, and failure-Inhibitors [69]; Technological, Managerial, Organizational, Institutional, and contextual [9]; Internal Service quality, External Service quality, leadership, culture, process management, employee engagement, citizen satisfaction, and Technology [13]. Some of the other factors mentioned are departmental coordination, architecture, and standards, policy parameters, resource availability, IT literacy, public awareness of services, length and breadth of services, security standards, legal and privacy matters [70]. The list of such factors can be long and can be confusing.

The 82 single values of factors obtained from the review were not entirely new. They were in line with the 25 Critical success factors of ICT projects (not limited

to government) by Ayat et al. [71] and 8 categories of factors for failure identified by Anthopoulos et al. [72]. The individual values ranged from a simple project coordination issue to a cultural issue. The 82 single variables were rationalized to 17 dimensions which were further combined to form 6 dimensions. They are described below.

Organization factors deal with the size of the organization, the people it has, the networks it employs, and the other organizational wherewithal that can support the ICT implementation. The institutional factors deal with the legal, policy, and context of the organization within the government. Managerial factors deal with the leadership aspect as well as the choice of methodologies and techniques used. Contextual factors are associated with the economic, social, and cultural aspects of society. Technical factors are associated with the hardware, software, and other technical aspects of the implementation [9]. Behavioral factors have been separated from the cultural aspect because of the multiplicity of actors in the implementation and the way each group responds to the project is important and deserves to be tracked as a separate dimension.

5 Summary and Conclusions

Based on the review of the 53 articles it can be concluded that, though most of the articles identify the factors that affect ICT implementation in government, they highlight the importance of the contextual concepts. In a study on 'ICT and Public Administration Reform', Sandor, (2012) concluded that 'technological change cannot be judged outside the social, economic and political frameworks' [50]. This study extends that conclusion to include two important concepts namely; ICT and Administrative reform contexts.

The Other aspect that plays an important role in ICT in Administrative reform is the concept of 'ICT use". In government, unlike in private industry, what ICT is used for in a project is linked to the overall big picture of the two contexts mentioned. Thus, this review has highlighted the fact that ICT implementation in an AR context can be critically affected by the overall context even if the project is well implemented within the framework of an ICT project.

Though many articles have listed and categorized the critical success factors, in the context of an Administrative Reform [35, 50, 62], they are best categorized as; Organizational, institutional, Managerial, Contextual, Technical, and Behavioral factors. This classification is helpful as it aligns well with the other three concepts of, ICT context, AR context, and ICT use. It is important to note that the institutional factors have a wider scope and are not limited to the institution as understood in the private industry.

This study has linked the two macro concepts of ICT context and Administrative Reform Context, to the two project level concepts of ICT use and Factors that affect implementation as shown in Fig. 3. These two macro contextual concepts are critical considerations for planning and implementing ICT interventions in a reform context.

In other words, studying factors affecting ICT projects alone is not sufficient in an Administrative Reform environment.

This study has its limitations, as there are two complex fields of ICT and Administrative reform that are studied using available literature. As explained by Pollitt and Bouckaert [2] study of administrative reform itself is complex and cannot be reduced to a simple frameworks. The same applies to ICT programs within a national context. Even within the cited limitations, this analysis is only applicable to the ICT implementation in the context of a larger program of administrative reform and may not be suitable for ICT implementation with a local cause.

References

1. G.E. Caiden, in *Administrative Reform* (Transaction Publishers, 2011)
2. C. Pollitt, G. Bouckaert, in *Public Management Reform: A Comparative Analysis-into the Age of Austerity* (Oxford university press, 2017)
3. K.K. Tummala, in Administrative reforms in India, in *Administrative Reform in Developing Nations,* ed by A. Farazmand (Praeger Publishers, 2002), pp. 29–48
4. L.B. Ngouo, The World Bank's approach to public sector management for 2011–2020: proposals to push forward the debate. Int. Rev. Adm. Sci. **83**(3), 541–562 (2017)
5. J.A. Halligan, J. Power, in *A Framework for the Analysis of Changes in Australian Executive Branches, In Public Administration and Public Policy,* vol. 94, ed. by A. Farazmand (2001), pp. 239–248
6. S. Song, ICTs and modernization in China, in *Handbook of Communication for Development and Social Change*,ed. by J. Servaes (2020), pp. 929–938
7. Ministry of Electronics and Information Technology, India Enterprise Architecture Framework, Government of India (2018)
8. A.B. Cheung, The politics of administrative reforms in Asia: paradigms and legacies, paths and diversities. Governance **18**(2), 257–282 (2005)
9. L. Herrera, J.R. Gil-Garcia, Implementation of e-government in Mexico: the case of Infonavit, in *Practical Studies in E-Government* (Springer, New York, 2011), pp. 29–47
10. V. Ndou, E-Government for developing countries: opportunities and challenges. Electron. J. Inf. Syst. Dev. Countries **18**(1), 1–24 (2004)
11. J.D. Twizeyimana, A. Andersson, The public value of E-Government–A literature review. Gov. Inf. Q. **36**(2), 167–178 (2019)
12. B. Gupta, S. Dasgupta, A. Gupta, Adoption of ICT in a government organization in a developing country: an empirical study. J. Strateg. Inf. Syst. **17**(2), 140–154 (2008)
13. A. Hooda, M.L. Singla, Reengineering as a strategic stance for e-governance success-mediating role of core competencies, in *Transforming Government: People, Process and Policy* (2020), pp. 205–235
14. J.F. Wolfswinkel, E. Furtmueller, C.P. Wilderom, Using grounded theory as a method for rigorously reviewing literature. Eur. J. Inf. Syst. **1**, 45–55 (2013)
15. J. Webster, R.T. Watson, Analyzing the past to prepare for the future: writing a literature review, in *MIS quarter*, pp. xiii-xxiii (2002)
16. G.P. Dias, Fifteen years of e-government research in Ibero-America: a bibliometric analysis. Gov. Inf. Q. **36**(3), 400–411 (2019)
17. C. El Ammar, C.M. Profiroiu, Innovation in public administration reform: a strategic reform through NPM, ICT, and e-governance. A comparative analysis between Lebanon and Romania, Administration & Public Management Review, p. 35, (2020)

18. K. Prasad, Capacity building and peoples participation in e-governance: challenges and prospects for digital India, in *Handbook of Communication for Development and Social Change* (2020), p. 1177
19. C.J. Schopf, Room for improvement: Why Korea's leading ICT ODA program has failed to combat corruption. Telecommun. Policy **43**(6), 501–519 (2019)
20. W. Castelnovo, M. Sorrentino, The digital government imperative: a context-aware perspective. Public Manag. Rev. **20**(5), 709–725 (2018)
21. M. Sorrentino, M. De Marco, D. Paolo, ICT policies, the Mediterranean tradition and the Italian diet of discontinuity. Telematics Inform. **34**(5), 707–716 (2017)
22. A.L. Rocca, T. Hoholm, Coordination between primary and secondary care: the role of electronic messages and economic incentives. BMC Health Serv. Res. **17**, 1–14 (2017)
23. S. Virkar, The Games people play: Exploring digital addiction within the context of the gamification of ICT project Design for Public Sector Administration Reform, in *Psychological and Social Implications Surrounding Internet and Gaming Addiction* (IGI Global, 2015), pp. 262–290
24. V. Chhabra, P. Rajan, S. Chopra, Intermediary's technology satisfaction and performance in Chhattisgarh public distribution system: Research Note, in *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development* (2016), pp. 1–4
25. S. Virkar, Wired for change?: Information and communication technologies shaping public administrative reform for development in Karnataka India. Int. J. Org. Collective Intell. **4**(1), 1–23 (2014)
26. I.S. Sodhi, E-government in China: status, challenges, and progress, in *Trends, Prospects, and Challenges in Asian e-governance* (IGI Global, 2016), pp. 36–54
27. E. Shahsavandi, G. Mayah, H. Rahbari, Impact of E-Government on transparency and corruption in Iran, in*Trends, Prospects, and Challenges in Asian E-Governance* (IGI Gobal, 2016), pp. 75–94
28. F. Contini, A. Cordella, Assembling law and technology in the public sector: the case of e-justice reforms, in *Proceedings of the 16th Annual International Conference on Digital Government Research* (2015)
29. M. Sorrentino, M. De Marco, D. Paolo, Steering the Digital Agenda at Arm's Length. All Wobble, No Spin: The Contextual Lens, Electronic Government (2015), p. 31
30. S. Virkar, Information and communication technology platform design for public administration reform: tensions and synergies in Bangalore, India, in *User-Centric Technology Design for Nonprofit and Civic Engagements* (Springer, 2014), pp. 135–169
31. A. Zardini, C. Rossignoli, L. Mola, Developing municipal e-Government in Italy: the city of Alfa case, in *International Conference on Exploring Services Science* (Springer, 2014), pp. 124–137
32. A.S. Jahangir, G. Qinghu, M.R. Alam, R.B. Roy, M. Kibria, Improved ICT grid computing model for development of the Bangladesh. Appl. Mech. Mater. **411**, 2200–2207 (2013)
33. G. Misuraca, G. Viscusi, Managing e-Governance: a framework for analysis and planning, in *Developing e-government Projects: Frameworks and Methodologie*s (IGI Global, 2013), pp. 204–224
34. D. Špaček, Information Strategies of Czech Statutory Cities and Regions: Critical Remarks. Knowl. Manag. Int. J. **3** (2013)
35. F. Bannister, Plus Ça Change? ICT and structural change in government, Innovation and the Public sector, vol 19 (2012), pp. 133–142
36. R. Chongthammakun, J. Pal, ICTs and development in the Thai bureaucracy: an examination of decentralization and organizational change, in *Proceedings of the Fifth International Conference on Information and Communication Technologies and Development* (2012)
37. G. Misuraca, G. Viscusi, E-Governance for development: Designing an operational roadmap for ICT-enabled public administration reform, in *Global Strategy and Practice of e-Governance: Examples from Around the World* (IGI Global, 2011), pp. 304–323

38. D.G. Chandra, D.B. Malaya, ICT Its Role in e-Governance and rural development, in *International Conference on Advances in Computing and Communications* (2011)
39. D. Binci, Climate for innovation and ICT implementation effectiveness: a missing link in Italian e-government projects. Int. J. Public Adm. **34**(1–2), 49–53 (2011)
40. S. Virkar, Information and communication technologies in administrative reform for development: exploring the case of property tax systems in Karnataka, India, in *ICTs for Global Development and Sustainability: Practice and Applications* (IGI Global, 2011), pp. 127–149
41. A. Cordella, F. Iannacci, Information systems in the public sector: the e-government enactment framework. J. Strat. Inf. Syst. **19**(1), 52–66 (2010)
42. F. Musella, American electronic constitution: reinventing government and neo-liberal corporatism, in *Electronic Constitution: Social, Cultural, and Political Implications* (IGI Global, 2009), pp. 54–70
43. D.C. Shim, T.H. Eom, Anticorruption effects of information communication and technology (ICT) and social capital. Int. Rev. Adm. Sci. **75**(1), 99–116 (2009)
44. T.K. Bensghir, T. Ali, An evaluation of the outsourcing IS/ICT activities in Turkish ministerial computer departments. Public Adm. Dev.: Int. J.Manag. Res. Pract. **28**(2), 94–104 (2008)
45. P. Kimberley, E-governance in trade facilitation: transparency and ICT as prerequisites for free and fair trade, in *Proceedings of the 1st International Conference on Theory and Practice of Electronic Governance* (2007)
46. K. Löfgren, The governance of e-government: a governance perspective on the Swedish e-government strategy. Public Policy Adm. **22**(3), 335–352 (2007)
47. C. Von Haldenwang, Electronic government (e-government) and development. Euro. J. Dev. Res. **16**(2), 417–432 (2004)
48. T. Cornford, E.K. Dabrowska, Telehealth technology: consequences for structure through use. Stud. Health Technol. Inf. **2**, 1140–1144 (2001)
49. L. Ma, J. Chung, S. Thorson, E-government in China: bringing economic development through administrative reform. Gov. Inf. Q. **22**(1), 20–37 (2005)
50. S.D. Şandor, ICT and public administration reforms. Transylvanian Rev. Adm. Sci. **8**(36), 155–164 (2012)
51. L. Hui, How information and communication technology promote the building of clean government: a case study of two local clean government reforms in China. Soc. Sci. China **40**(4), 85–105 (2019)
52. S.H.I.N. Sang-Chul, Z.M. Rakhmatullayev, Digital transformation of the public service delivery system in Uzbekistan, in *21st International Conference on Advanced Communication Technology* (2019)
53. A.C. Cruz, Portal for employees in the public sector: a tool for knowledge management in human resources, in *Handbook of Research on Modernization and Accountability in Public Sector Management* (IGI Global, 2018), pp. 342–362
54. V. Rakotonirina, R. Harilanto, The e-Procurement condition of sustained development: case of madagascar, in *Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance* (2016)
55. A. Zardini, C. Rossignoli, A. Suppa, F. Ricciardi, P.B. Paolo, Healthcare providers and IT-enabled organizational processes: the case of the Azienda Ospedaliera Universitaria Integrata of Verona. Int. J. Healthc. Technol. Manag. **14**(4), 272–289 (2014)
56. S. Virkar, Analysing E-government project success and failure using the design-actuality gap model, in *Encyclopedia of Information Science and Technology* (3rd Edn, Third ed., IGI Global, 2015), pp. 3219–3227
57. J. Vong, I. Song, Application of ICT to improve rural livelihood in Vietnam, in *Emerging Technologies for Emerging Markets.* (Springer, Singapore, 2015), pp. 179–204
58. A. Jansen, L. Einar, Can ICT reform public agencies? In *International Conference on Electronic Government* (2009)
59. T. Schuppan, E-Government in developing countries: experiences from sub-Saharan Africa. Gov. Inf. Q. **26**(1), 118–127 (2009)

60. R. Mahmood, Can information and communication technology help reduce corruption? How so and why not: Two case studies from South Asia, Perspectives on Global Dev. Technol. **3**(3), 347–373 (2004)
61. C. Bellamy, From automation to knowledge management: modernizing British government with ICTs. Int. Rev. Adm. Sci. **68**(2), 213–230 (2002)
62. I. Faik, M. Thompson, G. Walsham, Designing for ICT-enabled openness in bureaucratic organizations: problematizing, shifting, and augmenting boundary work. J. Assoc. Inf. Syst. **20**(6), 681 (2019)
63. S. Virkar, What's in a Game?: The Politics of Shaping Property Tax Administration in Bangalore City, India., in *International Business: Concepts, Methodologies, Tools, and Applications* (IGI Global, 2016), pp. 1913–1933
64. S. Virkar, The games people play: the politics of software platform development and ICT project design for public sector administration reform, in *Human Factors in Software Development and Design*, (IGI Global, 2015), pp. 67–91
65. G. Misuraca, G. Viscusi, E-governance for development: lessons learned and strategic principles for designing an operational roadmap. Int. J. Electron. Gov. **3**(2), 118–133 (2010)
66. J.R. Gil-Garcia, M. Flores-Zúñiga, Towards a comprehensive understanding of digital government success: integrating implementation and adoption factors. Gov. Inf. Q. **37**(4), 101518 (2020)
67. S.P. Osborne, The new public governance. Public Manag. Rev. **8**(3), 377–387 (2006)
68. A. Ingrams, Administrative reform and the quest for openness: a popperian review of open government. Adm. Soc. **52**(2), 319–340 (2020)
69. D. Gichoya, Factors affecting the successful implementation of ICT projects in government. Electron. J. e-government **3**(4), 175–184 (2005)
70. N.S. Kalsi, R. Kiran, E-governance success factors: an analysis of e-governance initiatives of ten major states of India. Int. J. Public Sect. Manag. **26**(4), 320–336 (2013)
71. M. Ayat, M. Imran, A. Ullah, C. Wook Kang, Current trends analysis and prioritization of success factors: a systematic literature review of ICT projects. Int. J. Manag. Proj. Bus. **26**(4), 320–336 (2020)
72. L. Anthopoulos, C.G. Reddick, I. Giannakidou, N. Mavridis, Why e-government projects fail An analysis of the Healthcare. gov website. Gov. Inf. Q. **33**(1), 161–173 (2016)

Analysis of Fault Tolerance Techniques in Virtual Machine Environment



Shelly Prakash and Vaibhav Vyas

Abstract Cloud computing provides various range of services over the internet such as storage services virtual servers applications infrastructure, etc. Continuously growing cloud data centers are majorly dependent on physical machines and virtualization. The reliability of cloud is calculated based on service availability of its physical and virtual servers. In this paper, a brief analysis study is done on virtualization. Firstly, the concept of failure and its types are presented. Secondly, the existing failure rectification models and strategies are studied and analyzed. Finally, a summary is presented to conclude common failure causes in virtual environment. Thereafter, it is proposed that failure detection can be improved by two-level detection strategy by introducing confidence factor, α, as a counter in heartbeat strategy for fault detection.

Keywords Virtual machine monitor · Hypervisor · Fault tolerance · Load balancing · VM (virtual machine) · PM (physical machine) · VM placement · VM replication · Deduplication

1 Introduction to Virtualization and Fault Tolerance

1.1 Virtualization

Virtualization is virtual representations of services such as memory, database, server, desktop, storage, or network virtualization. There are several advantages of virtualization such as reduced operating costs, increase in scalability, efficiency, and availability. Virtual machine (VM) is one of the several software-based components that run on a single host (physical machine, PM). Every VM functions independently and is completely unaffected by the presence of other VM's on its shared host.

S. Prakash (✉) · V. Vyas
Banasthali Vidyapith, Tonk, Rajasthan, India

V. Vyas
e-mail: vvaibhav@banasthali.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_12

The most basic problems in visualization are its backup and then the disaster recovery. Also, there is a much bigger problem with visualization which is its resource utilization. In real environments, virtualization is done on existing hardware. But many times, we go on by virtualizing whatever we can without focusing on the performance and the condition of the physical resources. Virtualization strategy will not at once make all the devices work efficiently. If the physical machine is not functioning well, then virtualization will not be efficient. Even in case of a multicore processor, if we start doing virtualizations without configuring it properly, then it will only result in clumping. Changes in the network or scaling can affect the performance of the applications virtually.

1.1.1 Hypervisor

To control and supervise virtual machines, a hypervisor or virtual machine monitor (VMM) is used, as depicted in Fig. 1. Hypervisor manages each virtual machine and operates between the physical machine and the virtual machine. The physical machine on which a hypervisor runs one or more virtual machines is known as a host machine, while each running virtual machine is known as a guest machine. The hypervisors are classified into two types (Fig. 2):

- **Type 1 or native or bare metal hypervisor**: They are installed in the operating system of host machine.
- **Native hypervisors**: Hosted type 2 hypervisors run just as other software on the host's operating system and then control the guest virtual machines.

An infected virtual machine can attack other virtual machines which are being shared on that hardware. To implement high reliability, cloud computing services rely on fault tolerance strategies at each level.

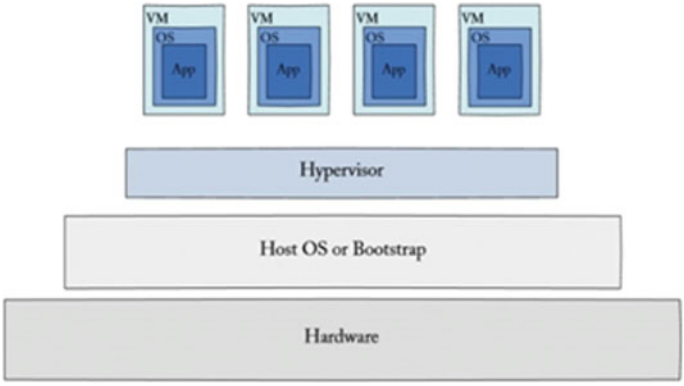


Fig. 1 Virtualization in cloud computing

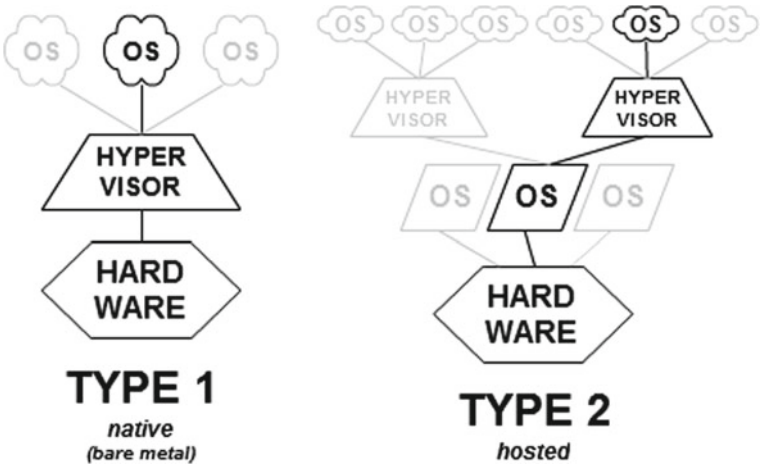


Fig. 2 Types of hypervisor

Failures in cloud environment can be in general of two types; sometimes our system behaves in an unexpected manner and produces false values. Such types of failures are known as **Byzantine failures**. However, in case of power shutdown, the whole system may abruptly stop functioning until the power resumes, such type of failures are known as **Crash failures**. The major problem with virtualization is that the failure recognition in the corresponding physical machine is difficult.

1.1.2 Challenges in Virtualization.

1. Security and Reliability: Although, different virtual machines running on the same host are unaware of each other and does not pose security threats to each other. But hypervisor interacts with virtual machines and the physical machine, causing it to be the weak point of security breach. Hyper jacking is the term used for security attack on the hypervisor. Factors affecting security in virtualized environment are:
   - VM image sharing: Malicious use of image sharing is done when an attacker steals the code from the image and determines the loose points for attack. Similarly, a user may upload a previously infected image.
   - VM isolation: Complete VM isolation is needed because communicational links between storage resources or input/output hardware may lead to intruder attack.
   - VM escape: In some cases, VM escapes from being supervised by the hypervisor, thus giving a chance to possible security threats.
   - VM migration: This is performed when fault tolerance measures are taken, or load balancing is required. During this process, all the contents of the

faulty VM are transferred to a better functioning VM which exposes all the data to the attackers.
- VM rollback: This is also a fault recovery measure. But along with necessary coding rollbacks, sometimes security patches also get removed/ disabled.
- VM sprawl: This situation arises when a large number of VMs are installed on a physical machine, while most of them are not in use. This increases unnecessary load on physical machine as well of wastage of resources.

2. Lack of control
3. Performance unpredictability
4. Software licensing
5. Data lock in
6. Reliability
7. Downtime
8. Implementing reliability by using Microservices: (Khan [11]) Simple way to eliminate such problems is to host small applications in the network. These applications are wrapped in a module. This service is known as container service and microservices. The design of microservices leaves least inter dependency among services. Only the necessary part of API is exposed to the user, and rest is hidden in that container. Before deployment, critical testing of security should be employed in each part of the application software. Rather than being attacked from outside attack, the service is most vulnerable when there is a loose patch in its own security service. Next thing which can be done to eliminate the threat of network security is to differentiate the management API and the user application. The controlling code should not be in easy access by the users and the outsiders. Therefore, it should be put in separate containers.
9. Resource allocation and Load Balancing: Resource management involves collection of resources, its allocation to the virtual machines and then monitoring. Firstly, all the resources are discovered which will be used in cloud computing. According to the usage and demand of resources, they are allocated to virtual machines, and after that, the monitoring is done using the load balancing technique. We can manage the resources in our environment based on two methods that is knowledge-based method and knowledge-free method.

1.2 Failure Management

Alharbi et al. [1] evaluated energy efficiency of VM placement in intra-data center networks, along with inter-VM traffic and live user traffic (Fig. 3). Mixed integer linear programming. (MILP) model has been used to optimize VM placement in corresponding scenario.

Kamaludin et al [10] evaluated the efficiency of a group of virtual machines based on CPU utilization, speed, and memory consumption by using Oracle VirtualBox. It was revealed in this paper that usually the utilization of the host OS is directly proportional to the memory allocated to it.

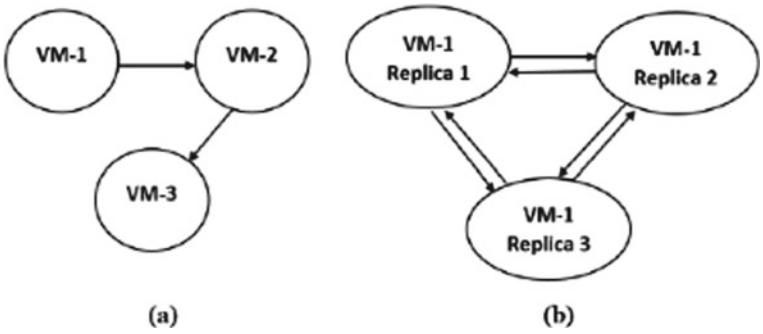


Fig. 3 **a** VM–VM coordination. **b** VM replica synchronization Alharbi et al. [1]

Memory resource sharing between different virtual machines on the same host can cause leakage of information as a threat to security. Memory deduplication is used to efficiently utilize memory by combining similar pictures of different virtual machines. To secure this process, Lindemann [15] proposed a model which performs timing-based side channel attack which is further used to identify software running on the virtual machines on the same host. After multiple repetitions of this process, it was proved that this process can identify similar pages between the VMs.

Virtual machine consolidation is a widely trending topic in the field of research. It includes consolidation of several VMs over a single host so that the resources of physical machine are efficiently utilized. But this process may compromise quality of service and may increase overload on the physical machine. Khan [11] analyzed and suggested various meta-heuristic algorithms to solve this NP-hard problem (Fig. 4).

VM placement is a process which curates the mapping of virtual machines on physical machines, along with improving energy efficiency and balancing VM migrations. While VM selection is a process which is associated with task assignment and load balancing to the VM's. Mann [20] experimented to conclude that VM selection largely affects VM placement (Fig. 5). While assigning load to the VMs, the storage and resource limit of the host physical machine should be taken care of to avoid overloads.

To tackle with the issues of reliability and downtime in virtualization, Ghazi [3] suggested proactive VM fault tolerance algorithm. A model is proposed in this paper which dynamically determines threshold for the parameters such as CPU utilization, usage, temperature, bandwidth, and memory. The dynamic behavior of this algorithm is also helpful in resource utilization.

Resource allocation affects the performance, energy consumption and reliability of the virtual machine. Liu [16] developed a deployment model for the virtual machine which provides the best physical configuration according to the user's dynamic requirements. This feedback virtual machine is experimented to meet the users customized fault tolerance demands.

Li et al. [14] proposed a model to improve reliability of virtualization in cloud by reducing the task response time. VM workload consolidation strategy is considered

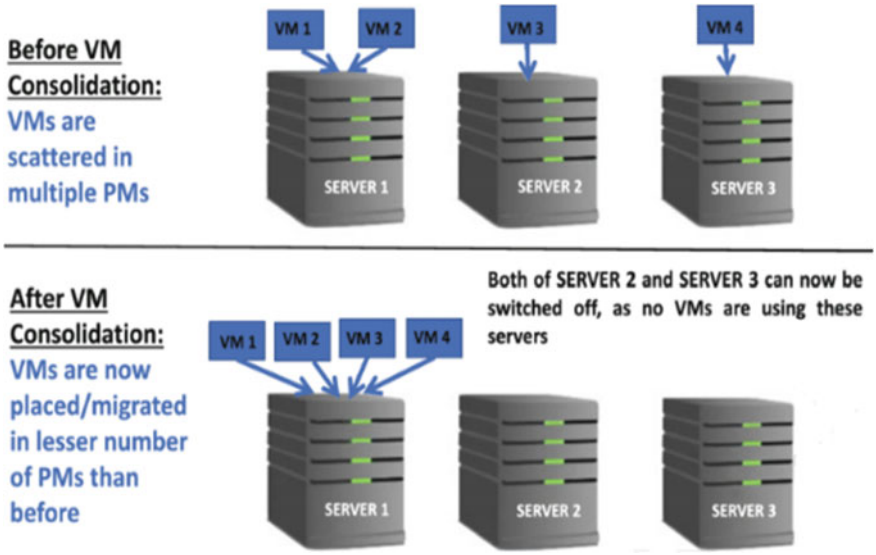


Fig. 4 Multiple VM's hosted on single physical machine (Khan [11])

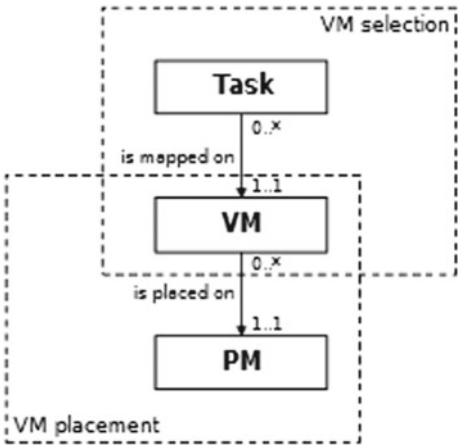


Fig. 5 VM placement and selection Mann [20]

to manage fault tolerance. When overload is exceeded beyond a preset value, then fault tolerance strategies are started.

Gilles [5] in their paper focused on energy saving in scheduling of tasks by Green Energy Aware Scheduling Problem (GEASP) for virtualized data centers. In this process, brown energy consumption is lowered for batch applications and not for active applications. Renewable green energy is then significantly introduced in the system while maintaining the quality of service and availability of services for users.

Zhou [30] focused on virtual machine replication process to overcome the loss from node failure so that the virtual machine recovers its processes without adjusting reliability of services. In this paper, it is mentioned that K-fault tolerance technique, for replication does not handle switch failure. They have proposed (m, n) fault tolerance virtual machine placement algorithm to solve this issue. Their work is aimed to eliminate inter traffic, service complexity and improving service reliability by handling an edge switch failure. The process is to discover services or host servers which are not critical and does not require startup in failure recovery process. This majorly contributes toward effective energy usage.

Zhou [29] in their paper proposed a technique to handle virtual machine placement issue reactively. The focus here was on the efficient network resource consumption while VM replication is performed. Firstly, network topology is studied and the host servers are shortlisted accordingly. The primary and backup virtual machines are placed optimally, and reassignment of tasks is then solved as an optimization problem. This overall improves network issues in VM replication phase of fault recovery.

Slimani [23] VM replication is also a common fault tolerance technique used to ensure service availability. This replication can be done in two ways, service-oriented replication (SOR), and data-oriented replication (DOR). Proactive and reactive replication approaches and their dynamic or static placement are also discussed in this paper.

Bharany [2] worked on detecting unhealthy virtual machines by measuring their temperature variations. The main focus of this paper was to incorporate live migrations for energy efficient fault tolerance. In this approach, firstly CPU utilization, power consumption, fan speed, and temperature is measured. If any of this rises or falls across a set threshold value, then the VM is declared to be near to failing. Proceeding further, live VM migration is carried out by selecting new healthy VMs whose power consumption is least at that moment and then the load is transferred to it. This energy-aware fault tolerance system (EAFT) was proposed to visibly save energy.

Li [13] focused on strengthening networking because a small failure in network may lead to failure of several virtual machines on that network. Before failure, backup network path needs to be determined and after failure, primary paths are linked to the backup network. **Online Backup and Fast Backup** techniques are employed to lower allocation of resources to be used for backups before failures. The fast backup is time saving and efficient in computing primary paths. Fast backup method predetermines primary paths and is suitable for a network with a lower rate of change in it.

However if the network's rate of change is high, then this method will be doing repetitive precomputing at the time of every change. Online backup method is proposed to be better here.

In Table 1, some of the existing fault analysis techniques are summarized based on different parameters.

Table 1 Review of existing failure analysis techniques in virtualized cloud computing

Reference	Main issues	Target objectives	Proposed approach	Parameters/conclusions
Alharbi et al. [1]	VM placement	Energy efficiency	Mixed integer linear programming model (MILP)	Focused on intra-data center networks, inter-VM traffic and live traffic
Kamaludin et al [10]	VM efficiency	CPU utilization, speed and memory consumption	Evaluate crucial basic parameters using Oracle Virtual Box	Concluded that the utilization of host operating system is directly proportional to memory allocated to it
Lindemann and Fischer [15]	Memory deduplication	Effective memory utilization	Timing based side channel attack on various VM's on the same host	Concluded that this process can identify similar pages in various VM's on the same host
Khan Anit [11]	VM consolidation	Consolidation of many VM's over single host for effective resource utilization of PM	Analysis of various meta heuristic algorithms	Concluded this to be a NP-Hard problem, which can be solved using this algorithm
Mann [20]	VM placement	VM selection affects VM placement	The VM selection is proposed to be done ideally also focusing on health and basic parameters of the host	Proposed that the storage and resource limit of host PM should be focused before loading VM over it
Li [14]	VM reliability	VM workload consolidation	VM fault tolerance model	Proposed to check overload and activate fault tolerance model if overhead exceeds certain threshold
Ghazi and Meenakumari [3]	VM reliability	Resource utilization, reliability and downtime management	Proactive VM fault tolerance algorithm	Parameters like CPU utilization, usage, temperature, bandwidth, and memory are monitored
Liu et al. [7]	VM Reliability	Resource allocation, performance, energy efficiency	Deployment model for VM to provide better physical configuration according to dynamic service requirement	Feedback VM is experimented to handle user's customized fault tolerant demands

(continued)

Table 1 (continued)

Reference	Main issues	Target objectives	Proposed approach	Parameters/conclusions
Gilles et al. [5]	Green energy	Energy Efficiency in Task Scheduling	Green Energy Aware Scheduling Problem (GEASP) for virtualized data centers	Proposed to increase Green energy usage, QOS and availability of services
Zhou [30]	VM replication	Inter-VM traffic service complexity, reliability, edge switch failure	(m,n) Fault Tolerance Placement Algorithm	Proposed to monitor critical and non-critical services before replication
Zhou [29]	VM placement (reactive fault tolerance)	Efficient network resource consumption, VM replication	Primary and backup VM, reassignment of services, solved as an optimization problem	Improves network issues in VM replication in fault tolerance
Slimani [23]	VM replication	Service-oriented replication (SOR) and dynamic-oriented replication (DOR)	Proactive/reactive replication approach, dynamic and static placement techniques	Proposed to solve trivial queries of fault recovery, i.e., when to replicate, which services to replicate, where to replicate, and how many replications are needed
Bharany [2]	Live VM migration	Detection of unhealthy VM, energy efficient VM fault tolerance	Energy-aware fault tolerance system (EAFT)	Proposed to monitor temperature variations, utilization, power consumption and fan speed of the VM
Li et al. [14]	Network reliability	Network fault tolerance	Online backup, fast backup	Analyzed online and fast backup

1.3 Conclusion

In our proposed methodology, we introduce a tracker, confidence factor, α, to supervise faults in heartbeat messages reception by VMs. Upon significant rise in this trackers value, the VM is discarded and marked for failure recovery procedures to be taken thereafter.

Levels of virtualization, its challenges, and related work toward fault tolerance are discussed in this paper. It has been observed that virtualization has its pros and cons, but with efficient management of resources, security and reliability, its challenges can be overcome. In this paper, we have analyzed several works related to faults and

better practices related to virtual machines and presented a summary of comparison between them.

References

1. H. Alharbi, T. El-Gorashi, A. Lawey, J. Elmirghani, The impact of inter-virtual machine traffic on energy efficient virtual machines placement (2019). https://doi.org/10.1109/STICT.2019.8789381
2. S. Bharany, Proactive detection of deteriorating node based migration for energy-aware fault tolerance. Think India J. **22**(16), 2256 (2019) ISSN: 0971-1260
3. S. Ghazi, J. Meenakumari, Virtual machine (VM) earlier failure prediction algorithm. Int. J. Appl. Eng. Res. **12**, 9285–9289 (2017)
4. S.S. Gill, R. Buyya, Failure management for reliable cloud computing: a taxonomy, model and future directions. Comput. Sci. Eng. pp 1–1 (2018). https://doi.org/10.1109/MCSE.2018.2873866
5. G.M. Wamba, Y. Li, A.-C. Orgerie, N. Beldiceanu, J.-M. Menaud. Green energy aware scheduling problem in virtualized datacenters. ICPADS 2017 (Shenzen, China, 2017), pp.648–655. ⟨hal-01582936⟩
6. H.S. Priyanka, M. Cherian, A Review on VirtualMachine Migration, Resource Management and Challenges (2019)
7. M. Hairy, A. Abdullah, S. Subramaniam, M. Hussin, A survey on resource allocation and monitoring in cloud computing. Int. J. Mach. Learn. Comput. (IJMLC). **4**, 31 (2014). https://doi.org/10.7763/IJMLC.2014.V4.382
8. A. Hosni, Cloud computing virtualization challenges. Int. J. Adv. Res. **5**, 1754–1758 (2017). https://doi.org/10.21474/IJAR01/4598
9. https://www.w3schools.in/cloud-computing/cloud-virtualization/
10. H. Kamaludin, M. Jamal, N. Ab Rahman, N. Mohd Safar, S. Abd Ishak, Implementing virtual machine: a performance evaluation (2020) https://doi.org/10.1007/978-3-030-36056-6_35
11. M. Khan, A. Paplinski, A. Khan, M. Murshed, R. Buyya, Dynamic virtual machine consolidation algorithms for energy-efficient cloud resource management: a review (2018). https://doi.org/10.1007/978-3-319-62238-5_6
12. P. Kumari, P. Kaur, A survey of fault tolerance in cloud computing. J King Saud Univer—Comput. Inf. Sci. (2018)
13. S. Li, Survivable services oriented protection level-aware virtual network embedding. Comput. Commun. (2020)
14. Z. Li, L. Liu, Z. Tong, Study on Fault Tolerance Method in Cloud Platform based on Workload Consolidation Model of Virtual Machine (2017)
15. J. Lindemann, M. Fischer, A memory-deduplication side-channel attack to detect applications in co-resident virtual machines (2018), pp. 183–192. https://doi.org/10.1145/3167132.3167151
16. J. Liu, Using proactive fault-tolerance approach to enhance cloud service reliability. IEEE Trans. Cloud Comput. **6**, 1191–1202 (2018)
17. S. Liu, W. Jia, X. Pan, Fault-tolerant feedback virtual machine deployment based on user-personalized requirements. Front. Comput. Sci. **12**, 682–693 (2018). https://doi.org/10.1007/s11704-017-6422-0
18. M. Maurer, I. Brandic, R. Sakellariou, Adaptive resource configuration for Cloud infrastructure management. Futur. Gener. Comput. Syst. **29**(2), 472–487 (2013)
19. S.S. Madani, S. Jamali, A comparative study of fault tolerance techniques in cloud computing. Int. J. Res. Comput. Appl. Robot. 7–15 (2018)
20. Z. Mann, Interplay of virtual machine selection and virtual machine placement (2016). https://doi.org/10.1007/978-3-319-44482-6_9

21. C.C. Marahatta, Energy-aware Fault-tolerant Scheduling Scheme based on Intelligent Prediction Model for Cloud Data Center, in *2018 Ninth International Green and Sustainable Computing Conference (IGSC)* (Pittsburgh, PA, USA, 2018), pp. 1–8
22. A. Miklosik, E. Hvizdová, Knowledge base cloud—a new approach to knowledge management systems architecture. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis **60**, 267–280 (2012). https://doi.org/10.11118/actaun201260040267
23. S. Slimani, Service-oriented replication strategies for improving quality-of-service in cloud computing: a survey. Cluster Comput. (2020)
24. D. Sullivan, Managing Virtual Machines (2019), pp 117–144. https://doi.org/10.1002/9781119564409.ch6
25. Y. Tang, Z. Qin, S. Yi, Q. Li, Virtual machine migration for IoT applications (2019) 437–442. https://doi.org/10.1145/3318216.3363383
26. A. Tomsic, P. Sens, J. Garcia, L. Arantes, J. Sopena, 2W-FD: a failure detector algorithm with QoS (2015), pp. 885–893. https://doi.org/10.1109/IPDPS.2015.74
27. R. Turchetti, D. Elias, L. Arantes, P. Sens, A QoS-configurable failure detection service for internet applications. J. Internet Ser. Appl. **7**, 9 (2016). https://doi.org/10.1186/s13174-016-0051-y
28. X. Zang, W. Chen, J. Zou, S. Zhou, H. Lisong, L. Ruigang, A Fault Diagnosis Method for Microservices Based on Multi-Factor Self-Adaptive Heartbeat Detection Algorithm (2018), pp. 1–6. https://doi.org/10.1109/EI2.2018.8582217
29. A. Zhou, Cloud service reliability enhancement via virtual machine placement optimization. IEEE Trans. Ser. Comput. 1–1 (2016)
30. A. Zhou, Virtual machine placement with (m, n)-fault tolerance in cloud data center. Cluster Comput. **22** (2019)

Analysis of Symmetric and Asymmetric Key Algorithms



Jitaksh Kapoor and Divyansh Thakur

Abstract Our world is making way towards complete digitalization, with more and more of data going to Internet. Thus, security of this data has become one of our utmost responsibilities. In 2018, 30 million cyber-attacks occurred all over the world costing $3.86 million on an average. With the statistics getting worse every year, it is very important to invest more in securing the data and more importantly design modern cryptographic techniques that are capable of mitigating modern adversaries. In this paper, we study different cryptographic algorithms that were designed after 1970 and are being used till date, and which were adopted and trusted to secure the data across the globe. Comparisons between different algorithms are being done on basis of flexibility, resistance against common attacks, execution speed, memory utilization, applications and the conclusion on best-suited encryption/cryptographic algorithms for securing our data is drawn. The study and comparisons of various algorithms have shown that asymmetric key encryption is far more secure than symmetric key encryption because of the application of two keys in place of one key and the algebraic complexity of their algorithms. Comparative analysis between symmetric key algorithms concluded that AES is the most versatile, secure and efficient algorithm. Comparative analysis between asymmetric key algorithms reveals that elliptical curve cryptography (ECC) is very secure due to its algebraic structure dependency on finite fields and elliptic curves.

Keywords Cryptography · Encryption · Key · Symmetric key algorithms · Asymmetric key algorithms · AES · ECC

1 Introduction

Cryptography or "secret codes" are a primary information security tool. Cryptography has large-scale applications which include offering secrecy and reliability,

J. Kapoor (✉) · D. Thakur
School of Computing, Indian Institute of Information Technology Una, Himachal Pradesh, India

D. Thakur
e-mail: divyansh@iiitu.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_13

among other vital information security purposes. The original unencrypted data is known as plaintext [1], and the result of encryption is ciphertext [2]. From the historic times, certain cryptographic techniques have been deployed to send messages from one person to others. Most historic simple substitution cipher [3] in which each alphabet of plaintext is substituted by an alphabet n (key) places ahead of the current one; double transposition cipher [4] in which the plaintext is converted into an array of a given size and the rows and columns are permuted according to specified permutations; Vernam Cipher [5] in which mapping between letters and binary representation of letters occurs; Vigenere Cipher [6] in which alphabetic text undergoes polyalphabetic substitution using a keyword, and many more such cryptographic algorithms and cipher were used. Our modern-day encryption algorithms are categorized into two categories: symmetric key encryption algorithms and asymmetric key encryption algorithms.

Symmetric key encryption algorithms [7] or private key encryption algorithms use one key (a secret key) for each encryption and decryption process. Data is encrypted to a form that is not recognizable or under stable to anyone who does not have the key to convert it back to original message. Once the anticipated receiver has the key and the encrypted text, the decryption algorithm, he/she does their action to convert back the encrypted text to its original plaintext form. Some of these algorithms are: DES [8], Blowfish [9], RC5 [10], RC6 [11], AES [12], and many more. This type of cryptography is largely used in applications for payment such as card transactions, database encryption, and hashing. The symmetric key algorithms have some weak points that resulted in them being over taken by new category of cryptographic algorithms. Apart from their large-scale applications, these algorithms had certain flaws; thus, a new category of encryption algorithms was designed which overcame the shortcomings of these algorithms.

Asymmetric key encryption algorithms [13] or public key encryption algorithms use a duo of encryption keys (one is private, one is public) to encrypt and decrypt the data. The sender and the receiver both have their own pair of public and private keys. In the first step, the sender obtains the receiver's public key. In the next step, the plaintext is made to undergo encryption by the sender with the help of receiver's public key; this results in conversion of plaintext to ciphertext. The ciphertext is then sent via a network to the receiver, who applies decryption algorithm on the ciphertext with the private key they possess and converts it back to original plaintext. If the encryption is carried out using public key, then the decryption process is completed using the private key; and vice versa is also true. The private key and public key are mathematically related to each other. Some of these algorithms are: Diffie–Hellman [14], RSA [15], elliptical curve cryptography [16], and many more. These algorithms are used for encrypting mails, Bitcoin, and other cryptocurrencies, making SSL/TLS cryptographic protocols, etc.

2 Motive of Survey

The motive of this survey is to get the answer of following research question:

2.1 Research Questions

The motive of this article is to find out the solutions of following research questions:

(RQ1) Which Cryptographic technique is better: Asymmetric key cryptography or Symmetric key cryptography?

(RQ2) Which Symmetric key encryption algorithm is the best algorithm in terms of flexibility, resistance against different types of Attacks, execution speed, versatility, etc.?

(RQ3) Which Asymmetric key encryption algorithm is the best algorithm in terms of flexibility, resistance against different types of Attacks, execution speed, versatility, etc.?

3 Related Work

This section of paper catalogues the literature survey of various research articles/papers covering the topics of symmetric and asymmetric encryption key algorithms. This section includes various techniques/algorithms, their encryption–decryption methods for securing information and overview of their applications in the real digital world. The literature survey is divided into two categories. These categories are:

- Symmetric key cryptography
- Asymmetric key cryptography

3.1 Symmetric Key Cryptography

In the work "A study and analysis of Symmetric Cryptography", Chandra et al. [17] proposed the comparative study between different mechanisms built on symmetric key cryptography or private key cryptography on basis of essential characteristics like advantages, drawbacks and applications of several algorithms like DES, Blowfish, 3DES, digital watermarking scheme, etc. The authors concluded that digital watermarking scheme and revocation are realized to be very effective because it is established on steganographic systems. Coppersmith et al. [18] proposed the system with DES and has more secure system thus reduced the chances of breaking into

the system using cryptanalysis. The author concluded that DES requires at least 1015 bytes of plaintext to be broken by Biham and Shamir's attack. Han et al. [19] implemented enhanced DES alongside high-order discrepancy power investigation in smartcards. The author implemented the improved DES to protect beside high-order DPA attacks and find the minimum requirements of DES to defend against the DPA attack. The author concluded that masking is a very effective and easily executed process to respond the DPA attack. The author also concluded that minimum of three random 32-bit masks and six additional S-Boxes are the nominal requirement for a DES implementation concealing all results of the S-Boxes over sixteen rounds to be secure against high-order DPA attacks. McLoone et al. [20] proposed high functioning implementation of DES using FPGAs. The author also proposed to compare the security and data rates of FPGAs implementation and software implementation. The author concluded that 16-stage pipeline DES algorithm implementation on single-chip FPGA can encrypt and decrypt data block at a rate of 3.87 Gbits/sec which is 27 times quicker than current software design. In the work of Johnson et al. [21], the authors introduced a new mode of multiple encryption—Triple DES. The aim of the work is to provide high protection against certain attacks which exploit the DES by using three keys for data encryption. The author concluded that triple DES is modified version of DES where we use several independent keys so as to achieve strength against key exhaustions attacks, dictionary attacks and matching ciphertext attack. Jun et al. [22] designed and implemented a high-speed 3DES algorithm system. The author proposed to do implementation of 3DES algorithm on FPGA, and its design must use pipeline technology and only one S-box. The author concluded that using pipeline technology helped the system to achieve the goal of high speed and also use of one S-box in place of original 8, significantly reduced the circuit size thus resulting in reduction of power consumption. In the work "Data encryption performance based on Blowfish", Mousa et al. [23] proposed that the performance indices for blowfish algorithm are the security and speed of the algorithm tested upon different types of data: text, sound, image. For each case, the key length and file size are improved to observe changes in the performance. The author concluded that speed of execution is directly affected by size of plaintext but not by varying key length and it is an important index to determine performance of Blowfish. Suresh et al. [24] implemented the Blowfish algorithm in IoT for secure data transmission using FPGA. The author proposed that the algorithm must be modified by changing its function module, and later comparisons are made between original and modified algorithms to find the efficient algorithm for IoT. The author concluded that modified algorithm showed enhancement in encryption time by 16.9% and output by 18.7%; as a result, improved Blowfish algorithm is more efficient for IoT environment. Kaur et al. [25] proposed a random selective block encryption technique for secure image cryptography using Blowfish algorithm. The author studies the encryption and decryption of the proposed technique and compared it with standard techniques on the basis of image security during transmission. The author concluded that the developed technique works effective and faster as associated to standard encryption algorithm. To analyse the Cast—256 cipher, Adams et al. [26] scrutinize the cryptographic security of Cast—256 symmetric block cipher algorithm which has been designed for 128-bit

block size and variable key sizes of up to 256 bits to ensemble AES requirements. The author concluded from the analysis that with reverence to cipher properties such as information theoretic characteristic and attacks like related-key attack, higher-order differential attack and linear-differential attack, this cipher is secure. Majeed et al. [27] implemented an enhanced CAST block algorithm to encrypt big data. The author proposed to analyse the original and primitive CAST-256 and its modified and new version with the assistance of modified S-Box and key generator. The author concluded that unlike the original CAST-256 which uses six S-boxes, the modified CAST algorithm works by utilising the generating keys, compression algorithm, and just one S-box which results in reduced execution time. Modified algorithm added much fewer overhead data and provided right protection; as a result it was concluded to be more favourable for encrypting big data. To introduce two-fish key algorithm, Schneier et al. [28] proposed that Twofish, a block cipher with a block size of 128-bit, works for different key length of 128, 192 or 256 bits. He also proposed to review the structure of Twofish, key schedule and its resistance to attack. The author concluded that related-key attacks failed against the full Twofish; also Twofish is appropriate to be used as a hash function to provide more security with 128-bit keys and 256-bit keys despite the fact that it slows the hash function by an approximate factor of two. Gulsezim et al. [29] proposed two-factor authentication technique for secure communication using Twofish algorithm and visual cryptography. The author implemented TEVC which used technique of predicting the correct graphical password. The author concluded that TEVC required arranging the particles of graphical password in correct manner which harder as compared to traditional alphanumerical password system, thus making it more reliable and less time consuming. As a result, TEVC is concluded to be more secure as compared to traditional system. Avila et al. [30] introduced the Rijndael block cipher (AES). The author proposed to analyse the structure and design of AES based upon criteria such as resistance against known attacks, design simplicity, speed and code compactness. In this work, author investigated advantages of AES over DES and T-DES. The author concluded that AES has advantages over DES and T-DES because it practically eliminates (a) the weak and semi-weak key and (b) linearity of key expansion. The AES provides these advantages by consuming computer cost of same order as T-DES. Jain et al. [31] introduced new algorithm AES 512 consisting of input block of 512 bit and key 512 bit. The author proposed to compare the security, memory and processor utilization of AES 512 and traditional AES for communication purposes. The author concluded that AES 512 has about 230% throughput compared to traditional AES and due to increased key size from 128 to 512 bit; the security increased significantly. With high level of security and high throughput, AES 512 is concluded to be ideal for multimedia communications. Sachdev et al. [32] proposed an algorithm for enhancing of cloud computing security using AES algorithm. The authors implemented a simple data protection model where data is encrypted using AES before it is launched in cloud storage. The author concluded that implementing AES for security of cloud data results in less memory consumption, less computation time and higher security as compared to other algorithms. Verma et al. [33] introduced enhanced RC6 block cipher algorithm and made contrast of enhanced RC6 with RC5

and RC6. The author proposed that RC6 is designed for 256-bit plaintext block with increased performance due to usage of eight registers and improved security. The author concluded that enhanced RC6 (RC6e) is 1.335 times quicker than RC5 and 1.212 times quicker than RC6 in terms of execution time, and the application of two-variable algebraic expressions and 2 Box-Types operations provide high security and CPU usage of RC6e is approximately same as that of RC5 and RC6 but uses little more memory. Mohamed et al. [34] implemented RC5 and RC6 block cipher algorithms to digital images. The author proposed to use RC5 and RC6 encryption to digital images and including them to statistical and differential analysis so as to investigate the errors and ambient noise. The author concluded that due to efficient retransmitting of defective packets and larger difference in two encrypted images (98.56%), RC6 is considered to be more favourable for encryption of digital images. Introducing the MARS encryption algorithm, Burwick et al. [35] proposed to analyse the structure and performance of MARS symmetric key encryption algorithm which supports 128-bit blocks and a variable key size. The proposed algorithm is supported in today's computers thus taking advantage of advanced performance to increase its performance and security. The author concluded that MARS is speedy and very secure symmetric-key-based block cipher with a very miscellaneous structure. Code for MARS is astonishingly compact, making it more suitable for limited-resource usage environments such as the smartcard. The grouping of high security, high speed, and tractability makes MARS a brilliant choice for the encryption. Shah et al. [36] implemented RGB image encryption using modified and improved SERPENT algorithm. The author proposed that improved version of SERPENT algorithm was less time-consuming which depends upon chain ring-based substitution boxes (S-boxes) dealing with 8-bit vector instead of 4-bit for RGB image encryption. The author concluded that due to execution of algorithm using chain ring-based constructed S-boxes, there was an improvement in time execution efficiency. Also, with the use of 8-bit block, the algebraic complexity of the algorithm increased leading to an increase in the algorithm's security. Zhang et al. [37] proposed a comparative study of DES and Blowfish encryption algorithm. The author proposed to study and analyse the security of both algorithms. The author evaluated performances in terms of execution speed based on diverse memory sizes. The author concluded that both algorithms provide enough security to tackle discrepancy and linear cryptanalysis attacks, but Blowfish overpowers DES in terms of faster execution speed. But DES proves better than Blowfish in terms of memory utilization as it desires much less memory for sub-key and S-boxes initialization than Blowfish. Mandal et al. [38] proposed performance evaluation of cryptographic algorithms: DES and AES. The author proposes to implement these using MATLAB software, and these techniques are compared on the basis of Avalanche effect due to one-bit variation in plaintext keeping the key constant, one-bit variation in key keeping the plaintext constant, memory utilization and simulation time required. The author concluded that DES required 43.3 KB of more space, whereas in AES, avalanche effect is very high. Thus, AES is ideal for encryption of messages or for anything involving monetary transactions.

3.2 Asymmetric Key Cryptography

Li et al. [38] made a proposal for Diffie–Hellman key exchange protocol. Diffie–Hellman protocol enables two users to swap a secret key securely but is easily strike down by man-in-the-middle attack thus author proposed an better-quality key exchange schema based on hash function. The author concluded that upgraded Diffie–Hellman key exchange protocol is resistant to replay attack, impersonation attack and man-in-the-middle attack. Also, the schema has low computing quantity and faster computing speed. Sujatha et al. [39] implemented combined DSA and multiple DES algorithms for secure Internet voting system. The author proposed to use DSA for digital signature generation that will be used for authorizing the person, and DES is applied random number of times to gain multi-fold encryption for increased security. The author concluded that digital signatures helped to authorize the correct users to ensure fair voting and the votes saved in database were highly encrypted by the multiple DES; thus, correctness of the data was ensured. Taneja et al. [40] proposed to implement dual security using DSA and audio steganography. The author aimed to provide the dual security by encrypting data through DSA and hiding the encrypting data beneath another medium (sound) for secure transmission. The author concluded that there was huge change in the security as it was nearly impossible to extract the data during transmission. As a result, data integrity, confidentiality and performance were enhanced. Tianhuang et al. [41] used digital signatures for e-commerce security. The author proposed to implement digital signatures generated from DSA to address key problems of security in e-commerce and also research for an improvement in the algorithm. The author concluded that use of digital signatures in e-commerce increased security immensely, as it denied the unauthorized users to do malicious acts. Though there is scope of improvement in this technique also, it is still very efficient in providing security. Tang et al. [42] studied the RSA public key algorithm and proposed to implement it practically for encryption and decryption both. The author stated that the security of algorithm is dependent on rigour of mathematics involved and also highlighted the importance of key confidentiality. The author concluded that RSA's security is dependent on the inconvenience of large integer factorizations, thus is used for data encryption and digital signatures. Wang et al. [43] proposed file encryption and decryption system using RSA algorithm. The author used C + + class library to develop the algorithm. The author concluded that RSA algorithm used in file encryption is very convenient to communicate and manage. This also brings scope of reusability and efficiency. Nibouche et al. [44] implemented high-speed RSA encryption algorithm using FPGA. The author proposed that the structures on which RSA is implemented are built using a modified Montgomery modular multiplier. The author concluded that the proposed architecture achieves twice the throughput rate of traditional RSA. Also, area-efficient RSA structure results in high clock frequency also. Zhao et al. [45] designed RSA-based digital image encryption algorithm for wireless sensor networks. The author implemented this new algorithm to deal with the weakness of limitations in WSN's transmission strategy. The author concluded that the proposed algorithm of RSA-based digital image encryption is highly secure

and faster in grey scaling images for encryption. This improves the security and speed of transmission process in WSN. Mundra et al. [46] proposed enhancement of data security of cloud using digital signatures and RSA algorithm. The proposed technique aimed to improve data security by implementing to cloud over a network. The author concluded that the proposed technique increases security of data in cloud significantly and makes it even more efficient for enterprise use. Kaur et al. [47] introduced a hybrid algorithm using DSA, RSA and MD5 for wireless devices. The author proposed to implement the hybrid algorithm on MANET to test the security level of the algorithm. The author concluded that the algorithm provided better response time, less network delay and best throughput. As result, this algorithm can be implemented to mobile nodes for security purposes. Gupta et al. [48] introduced a hybrid algorithm that is combination of Diffie–Hellman and RSA. The proposed algorithm had been implemented to provide more security for Internet and network applications. The author concluded that use of Diffie–Hellman for key generation and ciphertext, and generation of prime number using RSA makes it impossible to find the key. As a result, increase in security is observed. In the implementation of DES and RSA-based hybrid algorithm for Bluetooth communication, Ren et al. [49] proposed that the new algorithm will replace traditional 128-bit symmetric stream cipher for data transmission in a Bluetooth connection. The author concluded that the hybrid algorithm requires far more time complexity ($\gg$O (264)) than traditional cipher to be broken under certain circumstances. As a result, the hybrid algorithm is relatively more secure and easier to achieve in Bluetooth transmission. Mahalle et al. [50] proposed a hybrid algorithm using RSA and AES for enhancing the data security in cloud. The use of three keys will be done in this algorithm for encryption and decryption purpose, and two keys are used for secure upload and download of the data. The author concluded that each key generation takes place in a unique way; thus, there is no chance of correlation or redundancy in the keys. The use of unrelated and multiples keys increased security multiple times, thus making cloud secure in every aspect. Koblitz et al. [51] studied the use of the discrete logarithm in public key cryptography and specifically in elliptical curve groups. The author proposed that implementation of discrete logarithm on elliptical curve groups must provide high security, high speed and relatively small block size. The author concluded that selecting an appropriate elliptic curve for implementation is very important and is dependent on where it has to implement. Proper implementation helps to use its security to the fullest.

4 Conclusion

In this article, fifty paper/articles have been studied and they have been arranged into two different categories, i.e. symmetric key cryptography and asymmetric key cryptography. The motive behind this survey article is to obtain the answers of research questions mentioned in Sect. 2.1. The followings are the answers: **(RQ1)** From literature, it can be understood that symmetric key algorithms use one key for encryption

and decryption, whereas asymmetric key algorithms use two related secret keys for encryption and decryption. The use of two keys increases security significantly, and asymmetric key algorithms being new and latest do not depend on number theory rather depend upon more complex concepts like logarithms, curves, signatures, etc. Thus, it can be concluded that asymmetric key algorithms are far more secure and efficient compared to symmetric key algorithms. **(RQ2)** From literature, we have studied the comparisons among different symmetric key algorithms on the basis of their performance, security, flexibility, etc. From the comparisons, it can be concluded that AES is the best encryption algorithm because of its higher security, lesser memory usage, faster execution and more applications in the real world. **(RQ3)** From literature, we have studied the comparisons among different asymmetric key algorithms on the basis of their performance, security, flexibility, etc. From the comparisons, it can be concluded that ECC is the best encryption algorithm because of its higher security, faster execution, complexity due to use of logarithms and curves and its compatibility with other cryptographic algorithms.

References

1. N. Mairs, *Plaintext* (University of Arizona Press, 1992)
2. J. Katz, Y. Lindell, *Introduction to Modern Cryptography* (CRC Press, 2014)
3. R.S. Ramesh, G. Athithan, K. Thiruvengadam, An automated approach to solve simple substitution ciphers. Cryptologia **17**(2), 202–218 (1993)
4. W. Stallings, *Cryptography and Network Security: Practice and Principles* (1998)
5. S.M. Bellovin, Frank Miller: inventor of the one-time pad. Cryptologia **35**(3), 203–222 (2011)
6. Q.A. Kester, A cryptosystem based on Vigenère cipher with varying key. Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **1**(10), 108–113 (2012)
7. M. Agrawal, P. Mishra, A comparative survey on symmetric key encryption techniques. Int. J. Comput. Sci. Eng. **4**(5), 877 (2012)
8. F. Pub, Data Encryption Standard (DES). *FIPS PUB* (1999), pp. 3–46
9. B. Schneier, Description of a new variable-length key, 64-bit block cipher (Blowfish), in *International Workshop on Fast Software Encryption* (Springer, Berlin, Heidelberg, 1993), pp. 191–204
10. R.L. Rivest, The RC5 encryption algorithm, in *International Workshop on Fast Software Encryption*. (Springer, Berlin, Heidelberg, 1994), pp. 86–96
11. S.H. Abdullah, J.A. Mahdi, A.T. Hashim, A proposed 512 bits RC6 encryption algorithm. Iraqi J. Comput., Commun. Control Syst. Eng. **10**(1), 11–25 (2010)
12. D. Joan, R. Vincent, The design of Rijndael: AES-the advanced encryption standard, in *Information Security and Cryptography* (Springer, 2002)
13. B.A. Forouzan, *Cryptography & network security* (McGraw-Hill, Inc., 2007)
14. U.M. Maurer, S. Wolf, The Diffie-Hellman protocol. Des. Codes Crypt. **19**(2–3), 147–171 (2000)
15. R.A. Mollin, *RSA and Public-Key Cryptography* (CRC Press, 2002)
16. J. Lopez, R. Dahab, An overview of elliptic curve cryptography (2000)
17. S. Chandra, S. Bhattacharyya, S. Paira, S.S. Alam, A study and analysis on symmetric cryptography, in *2014 International Conference on Science Engineering and Management Research (ICSEMR)* (IEEE, 2014), pp. 1–8
18. D. Coppersmith, The Data Encryption Standard (DES) and its strength against attacks. IBM J. Res. Dev. **38**(3), 243–250 (1994)

19. J. Lv, Y. Han, Enhanced DES implementation secure against high-order differential power analysis in smartcards, in *Australasian Conference on Information Security and Privacy* (Springer, Berlin, Heidelberg, 2005), pp. 195–206
20. M. McLoone, J.V. McCanny, A high performance FPGA implementation of DES, in *2000 IEEE Workshop on SiGNAL PROCESSING SYSTEMS. SiPS 2000. Design and Implementation (Cat. No. 00TH8528)* (IEEE, 2000), pp. 374–383
21. D. Coppersmith, D.B. Johnson, S.M. Matyas, A proposed mode for triple-DES encryption. IBM J. Res. Dev. **40**(2), 253–262 (1996)
22. Y. Jun, L. Na, D. Jun, A design and implementation of high-speed 3DES algorithm system, in *2009 Second International Conference on Future Information Technology and Management Engineering* (IEEE, 2009), pp. 175–178
23. A. Mousa, Data encryption performance based on Blowfish, in *47th International Symposium ELMAR, 2005* (IEEE, 2005), pp. 131–134
24. M. Suresh, M. Neema, Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Things. Procedia Technol. **25**, 248–255 (2016)
25. A. Kaur, G. Singh, A random selective block encryption technique for secure image cryptography using blowfish algorithm, in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)* (IEEE, 2018), pp. 1290–1293
26. C. Adams, H.M. Heys, S.E. Tavares, M. Wiener, An analysis of the CAST-256 cipher, in *Engineering Solutions for the Next Millennium. 1999 IEEE Canadian Conference on Electrical and Computer Engineering (Cat. No. 99TH8411)*, vol. 1 (IEEE, 1999), pp. 361–366
27. F.A. Kadhim, G.H. Abdul-Majeed, R.S. Ali, Enhancement CAST block algorithm to encrypt big data, in *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)* (IEEE, 2017), pp. 80–85
28. B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, On the twofish key schedule, in *International Workshop on Selected Areas in Cryptography*. (Springer, Berlin, Heidelberg, 1998), pp. 27–42
29. D. Gulsezim, S. Zhansaya, A. Razaque, Y. Ramina, F. Amsaad, M. Almiani, A. Oun, Two factor authentication using twofish encryption and visual cryptography algorithms for secure data communication, in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)* (IEEE, 2019), pp. 405–411
30. C. Sanchez-Avila, R. Sanchez-Reillol, The Rijndael block cipher (AES proposal): a comparison with DES, in *Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No. 01CH37186)* (IEEE, 2001), pp. 229–234
31. R. Jain, R. Jejurkar, S. Chopade, S. Vaidya, M. Sanap, AES algorithm using 512 bit key implementation for secure communication. Int. J. Innov. Res. Comput. Commun. Eng. **2**(3), 3516–3522 (2014)
32. A. Sachdev, M. Bhansali, Enhancing cloud computing security using AES algorithm. Int. J. Comput. Appl. **67**(9) (2013)
33. H.K. Verma, R.K. Singh, Enhancement of RC6 block cipher algorithm and comparison with RC5 & RC6, in *2013 3rd IEEE International Advance Computing Conference (IACC)* (IEEE, 2013), pp. 556–561
34. A.B. Mohamed, G. Zaibi, A. Kachouri, Implementation of RC5 and RC6 block ciphers on digital images, in *Eighth International Multi-Conference on Systems, Signals & Devices* (IEEE, 2011), pp. 1–6
35. C. Burnwick, D. Coppersmith, The Mars Encryption Algorithm. IBM, August, **27** (1999)
36. T. Shah, T.U. Haq, G. Farooq, Improved SERPENT algorithm: design to RGB image encryption implementation. IEEE Access **8**, 52609–52621 (2020)
37. T. Nie, T. Zhang, A study of DES and Blowfish encryption algorithm, in *Tencon 2009–2009 IEEE Region 10 Conference* . (IEEE, 2009), pp. 1–4
38. N. Li, Research on Diffie-Hellman key exchange protocol, in *2010 2nd International Conference on Computer Engineering and Technology*, vol. 4. (IEEE, 2010), pp. V4–634
39. K. Sujatha, A.A. Rao, L.V. Rajesh, V.V., Raja, P.N. Rao, Secured internet voting system based on combined DSA and multiple DES algorithms. In *ICT and Critical Infrastructure: Proceedings*

of the 48th Annual Convention of Computer Society of India-Vol II (Springer, Cham, 2014), pp. 643–650
40. N. Taneja, P. Gupta, Implementation of Dual security through DSA and audio Steganography, in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (IEEE, 2015), pp. 1349–1352
41. C. Tianhuang, X. Xiaoguang, Digital signature in the application of e-commerce security, in *2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT)*, vol. 1 (IEEE, 2010), pp. 366–369
42. X. Zhou, X. Tang, Research and implementation of RSA algorithm for encryption and decryption, in *Proceedings of 2011 6th International Forum on Strategic Technology* vol. 2 (IEEE, 2011), pp. 1118–1121
43. S. Wang, G. Liu, File encryption and decryption system based on RSA algorithm, in *2011 International Conference on Computational and Information Sciences* (IEEE, 2011), pp. 797–800
44. O. Nibouche, M. Nibouche, A. Bouridane, High speed FPGA implementation of RSA encryption algorithm, in *10th IEEE International Conference on Electronics, Circuits and Systems, 2003. ICECS 2003. Proceedings of the 2003*, vol. 1 (IEEE, 2003), pp. 204–207
45. G. Zhao, X. Yang, B. Zhou, W. Wei, RSA-based digital image encryption algorithm in wireless sensor networks, in *2010 2nd International Conference on Signal Processing Systems*, vol. 2 (IEEE, 2010), pp. V2–640
46. U. Somani, K. Lakhani, M. Mundra, Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing, in *2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010)* (IEEE, 2010), pp. 211–216
47. K. Kaur, E. Seema, Hybrid algorithm with DSA, RSA and MD5 encryption algorithm for wireless devices. Int. J. Eng. Res. Appl. **2**(5), 914–917 (2012)
48. S. Gupta, J. Sharma, A hybrid encryption algorithm based on RSA and Diffie-Hellman, in *2012 IEEE International Conference on Computational Intelligence and Computing Research* (IEEE, 2012), pp. 1–4
49. W. Ren, Z. Miao, A hybrid encryption algorithm based on DES and RSA in bluetooth communication, in *2010 Second International Conference on Modeling, Simulation and Visualization Methods* (IEEE, 2010), pp. 221–225
50. V.S. Mahalle, A.K. Shahade, Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm, in *2014 International Conference on Power, Automation and Communication (INPAC)* (IEEE, 2014), pp. 146–149
51. N. Koblitz, A. Menezes, S. Vanstone, The state of elliptic curve cryptography. Des. Codes Crypt. **19**(2–3), 173–193 (2000)

A Hybrid Approach for Retrieving Geographic Information in Wireless Environment Using Indexing Technique



Prashant Vats, Zunaid Aalam, Satnam kaur, Amritpal kaur, and Neha Gehlot

Abstract The wireless data transmission has emerged as a residential data distribution process which is nowadays used for dissemination of public users in order to cater a large integer of mobile users. In this research paper, we have proposed a hybrid indexing schemes for data transmission which is based on the dispersion of indexing using hash table with Huffman-tree index coding. In the proposed work, we have theoretically explained the performance of existing indexing scheme using a detailed study and afterward have compared their performances. In our proposed approach we have used an indexing technology for retrieving geographic information in Wireless Environment. The proposed technology has been evaluated in terms of efficiency and time difficulty and proved to be very efficient during our experimental analysis.

Keywords Data radio casting · Tuning time · Indexing scheme · Access latency

1 Introduction

In the field of wireless transmission the area that has received a lot of attention in the area of GIS (Geographic Information system). Recent advancements in the communication hardware have made possible the accomplishment affordability of these types of systems for many broadcasting organizations. In the wireless sensor, networking organization efforts have been given in making possible that many public broadcasting organizations are working on the development of the spatial data-based communication infrastructures that will make possible for them to share their geographical-based informational data. Many of the data chronicles that are stored in

P. Vats (✉)
Fairfield Institute of Management and Technology, GGSIPU, New Delhi, India

Z. Aalam · S. kaur · A. kaur · N. Gehlot
SGT University, Gurugram, Haryana, India
e-mail: amritpal_fet@sgtuniversity.org

N. Gehlot
e-mail: neha_fet@sgtuniversity.org

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_14

electronic libraries and record archives incorporate geographic innuendo within their texts. For example, newscast documents depict the spot where the incident occurred and sometimes the place where the document has been produced. Geographical location innuendo can also be affixed to Internet pages by using details from the location of the webpage text, web server, and many other webs-based informational elements. However, the geographic location plugs of these Internet documents are scarcely used in the geographical informational recuperation systems. Few geographical informational recuperation algorithms or index structures include the spatial nature of geographic innuendo entrenched within these documents. The pure expurgated textual indexing techniques concentrate only on the phonological pragmatics of the documents and pure spatial techniques concentrate only on the topographical aspects of the Internet base documents. Not any of them are appropriate enough as a combined approach to the process of Internet-based geographical information retrieval because they totally ignore the other type of informational structures. Consequence to which, there is a total paucity of system architectures, index structures, and query languages that includes both types of gens.

In recent years, wireless data transmission has become more popular due to its scalability and elasticity to distribute public users in turn to a large numeral of mobile users with common interests because it can accommodate all awaiting requirements for same data in a comeback. Customers in the efficient area can access the broadcast channel, investigate for compulsory data item and wait for the data item to appear before downloading it [1]. In fact, many practical applications use data broadcast technology, where movable clients have a frequent attention in certain data groups [2]. Since most mobile devices have incomplete battery power or limited life, access delay and adjustment time are the two main criteria for evaluating the presentation of data transmission systems. In this research paper, we have proposed hybrid indexing schemes for data transmission which is based on the dispersion of indexing using hash table with Huffman-tree index coding. In the proposed work, we have theoretically explained the performance of existing indexing scheme using a detailed study and afterward have compared their performances. In our proposed approach we have used an indexing technology for retrieving geographic information in Wireless Environment which is based on wavelet wood data structure for text indexing or spatial indexing thereby establishing a new evaluation strategy.

2 Some of the Wireless Indexing Techniques

Indexing technology has been used to condense the tuning time of data transmission systems. An index is an explicit data arrangement that contains position in order for data elements. Indexing technology has evolved rapidly in current years or it is fair or just to choose the most advanced design for assessment. To trounce above shortcomings, we strive to compare the presentation of unusual indexing techniques in all possible situations. In general, indexing system can be divided into 3 categories,

namely Hashing schemes, B + tree-based schemes and Huffman wood compression-based schemes.

2.1 Hash-Scheme

This scheme uses less power, has a shorter transmission or a shorter access time. It can also connect errors flexibly. In the case where most customers need short comeback time or minimal power consumption, the hash method is the best choice because hash method can achieve almost the best adjustment time. It works better in scheme that does not involve frequent updates because it may take some time to construct a broadcast sequence. Similarly, the hash function may need to be further modified for dissimilar datasets.

2.2 B + Tree-Based Schemes

In the implementation of database indexes, a B + contains pointers to lower level nodes in the tree and an ordered list of keys. To insert an element search for or search for element into the tree, one must loads up the root node, based on searched-for value in between try to find the adjacent keys, and follows to the next node in the tree using the corresponding pointer the tree.

2.3 Huffman Wood Compression-Based Schemes (H.T.D.)

The Huffman-tree is a small index tree that considers the potential for data entry, where the more popular data has a shorter path from root to path, thus reducing the moderate adjustment period. It works better in search, above all for datasets with high contact probability and small index boxes. It has flexibility, short transmission or best time effectiveness, uses less energy and can sometimes connect faults flexibly. When mainly clients need the shortest comeback time or lower energy expenditure, the service provider should consider the Huffman-tree schema, especially when the data element has a rather skewed access probability in dataset. Though, when the dataset needs to be updated frequently, this may not be a good choice.

3 Related Work

In this section of the paper, we have carried out a literature review on the work related to the indexing technology for retrieving geographic information in Wireless Environment.

Sun et al. [3] have presented a new proposal for two-dimensional spacing, which can provide the general status of the files placed in server, which is useful for retrieving XML data in of the request mode. Firstly, they have proposed cutting method or double arrangement greatly condense size of the index. Secondly, their two-tier system allows the client to implement an effective access protocol, which can further reduce correction time during index indexing.

Dimitrios et al. [4] have proposed their work for energy saving and access efficiency are two key goals competing with non-functioning communication networks. To address the energy loss caused by queuing searches, they have recommended adjusting the indexes and data. While there is a significant contribution to indexing, indexing has one or more of the following issues. First, they all consider the complete arrangement between the broadcast data, and none of them consider the partial subscription case in general. Second, they are balanced systems and do not fit into "linear (one-dimensional) system" of wireless media, where an unbalanced structure can provide obvious advantages. Third, they do not consider the reduction of access patterns that hinder greater profits.

Ping et al. [5] have proposed their work on broadcasting in an effectual way of distribute information to many consumers using mobile devices in a wireless world. This requires customer to actively listen to the channels to get information that interests them, which will increase battery consumption. However, so far, the battery of the mobile device is still a container, which limits size of mobile application. In their proposed work, they have presented a specific measurement conversion strategy (PFInd), which can be used to adjust the exchange between access competence or power savings according to customer supplies. Experimental results show that this process has better presentation or efficiency compared to some of latest indexes.

Chinmayananda et al. [6] have addressed the problem of a dual sender unicast account that has two senders, and each sender has a different message. Some messages may be similar to two senders. Each recipient needs a unique message or has a message piece called a sub-message. The sender uses the knowledge of all recipient margins to send a coded message so that all recipients can solve their needs. The goal is to find the total number of opt-in senders for the length of the message (also known as maximum number of messages sent with a limited number of messages), and the value of limit if message lengths tend to be unlimited (also known as good audio transmission rate). It also provides the best coding system.

Zhu et al. [7] have considered the characteristic properties of variable data sizes across multiple channels, by offering a recording technique using a reference tree to reduce the average time and average correction time. The results show that programmatic programs can have a high quality index and are very effective in transmitting heterogeneous data.

Yon et al. [8] have presented a naming scheme for the efficient processing of energy saving and the delay of full text search on wireless radio stations. Although many access methods and indexing arrangement for full text search have been proposed in the past, they are all targeted to the data in disk archive, rather than to non-broadcast channels. In order to perform a full text search on a wireless radio station, they have introduced the naive list operation method, in which the list goes before the data in wireless channel. To reduce the waiting time header, they have offered two-level indexing, which adds another index structure to the index style list.

Kuvano et al. [9] have presented their work on JoyTV, which is PC-based PC-watching software. They have automatically noticed the changes and the music on stage and accepted superimposed text on television broadcasts. It uses the function of images to connect TV content and Web sites.

4 Proposed Work

Huffman-tree indexing is an efficient indexing technique for the wireless broadcast environment because when we are constructing and codes the Huffman-tree it takes into account how much is the user access probability is there for an Internet data items. When we start the Huffman-tree traversing from the root, in Huffman-tree we place the popular page of data over the Internet with highest probability which lives in closer to the root, that is results in reduction of the search time for a popular Internet data page over the web using mobile data network. Further considering the flat broadcast, we have found that to a Huffman-tree-based broadcasting scheme over the wireless network, the distributed method can be extended over and applied to the base stations that is a very innovative idea and can be taken into consideration as an efficient index technique for the wireless indexing schemes. In this section, we have discussed the architectural configuration of data bucket and index bucket in H.T.D. is as similar as in a BTD. The first step is to bit by bit gradually create a Alphabetic Huffman-Tree that is k-ary-based, catalyzed by the following steps which are being introduced during the construction and development process that is based on the access frequency of datasets of the Internet clouds in Fig. 1. An Alphabetic Huffman-Tree would be raised up further to prepare and composing the formalized earth base station access frequency in a integrated uniform manner as shown in Fig. 2. In this, following algorithm would be used to construct this H.T.D.

Data Item Key	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Frequency	23	4	12	10	17	31	15	21	29	19	7	12	16	14	20	48

Fig. 1 Given dataset of H.T.D. index

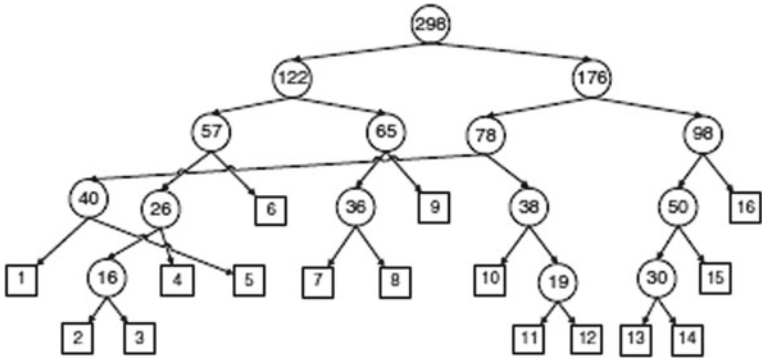


Fig. 2 Construction of Huffman code-based tree

Stage 1: Let us consider a Binary Huffman-tree data nodes → di, dj as nodes as candidates to be unified. we will create a new index node-based tree di with a data frequency which would be equal to the total sum of the nodes di's and dj's data item frequencies, and will replace the data item nodes di, dj with a new data node d'i during the construction sequence H.T.D. Index.

Stage 2: When there would be no leave nodes among them, At stage 2, For every data di note and observe the level of each leaf data node of T0. The root node would be at level 1. Considering from bottom level to the root level H.T.D. Index, for each level rearrange the pointers in such a way that the leftmost two nodes of Huffman-Tree would then have the same parent, and so on then the next two and soon. In this way, alphabetic Huffman-Tree T would be generated, without altering the level of each node in tree T0, as shown in Fig. 3

Stage 3: The sum of the Nodal frequencies would be minimum, Now we will cut the final Huffman-tree T at level l after generation of the alphabetic Huffman index tree T based on the mobile index bucket information, and we will perform a distributed traversal final Huffman-tree T as stage 4 (Fig. 4).

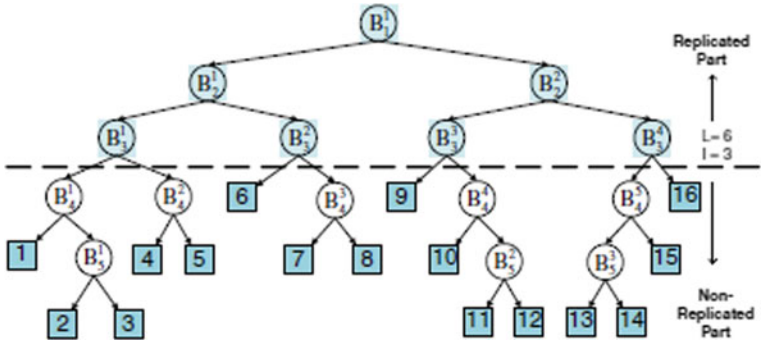


Fig. 3 The Huffman coded-tree index T

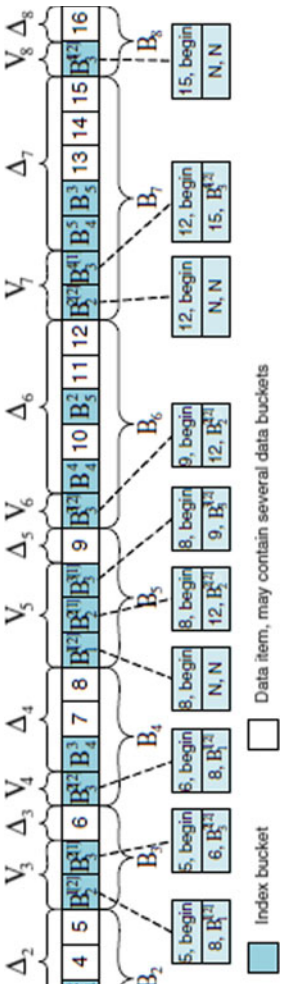


Fig. 4 Huffman-tree-based index-based broadcast bucket sequence

```
Input→ keyreqd , {Where Input id the key value of request data is
equal to dreq}
Output:→dreq .
Do the Access →in a randomized order on to the broadcast
channel;
Declare the value of B0 is equal to current bucket;
if (B0 is equal to data bucket &&  B0 .bId is equal to (keyreq, 1,
sreq )) then declare
{
 Download data dreq ;
 } end if;
else if  (B0.bType  is equal to control) then
{
Doze B0.bOffset time till the next control index;
B0 → current bucket;
} end if
Follow B0's control table and go to the pointed bucket;
Download data dreq ;
```

Fig. 5 Algorithm for retrieving data from The broadcasting sequence of a Huffman-tree-based index

Stage 4: Let di, dj → would be the left most nodes available among all candidates. During stage 4 when we are searching in a Huffman-tree *T* control table, the client check the first node record entry in the control table with using the key value of a request data packet; algorithm which is given in Fig. 5. will be used for while retrieving the indexing data from the broadcast sequence of a Huffman-tree-based index as shown in Fig. 5

5 Experimental Results

In this section, we have used experimental miniature simulation for obtaining the results for evaluating the actions of the indexed H.T.D. Index Scheme. We have implemented our system is on an AMD Ryzen computer with 8 GB memory using Java NetBeans, and Windows 10 v6.1 operating system.

5.1 Experimental Settings

While using a single broadcast communication channel we have simulated a base station which is broadcasting a data collection archive with 10,000 data items [9], where a series of multiple clients are based on these mobile stations that are requesting

various sets of data items depending upon the user need which is having a varying size as shown in Fig. 6.

5.2 *Simulation Results*

From Fig. 7, we can see and analyze that the results for evaluating the actions of the indexed H.T.D. Index Scheme and can conclude that: (1) It reduces response time significantly, and (2) it is more energy efficient.

6 Conclusion

In this research paper, we have proposed hybrid indexing schemes for data transmission which is based on the dispersion of indexing using hash table with Huffman-tree index coding. In the proposed work, we have theoretically explained the performance of existing indexing scheme using a detailed study and afterward have compared their performances. In our proposed approach we have used an indexing technology

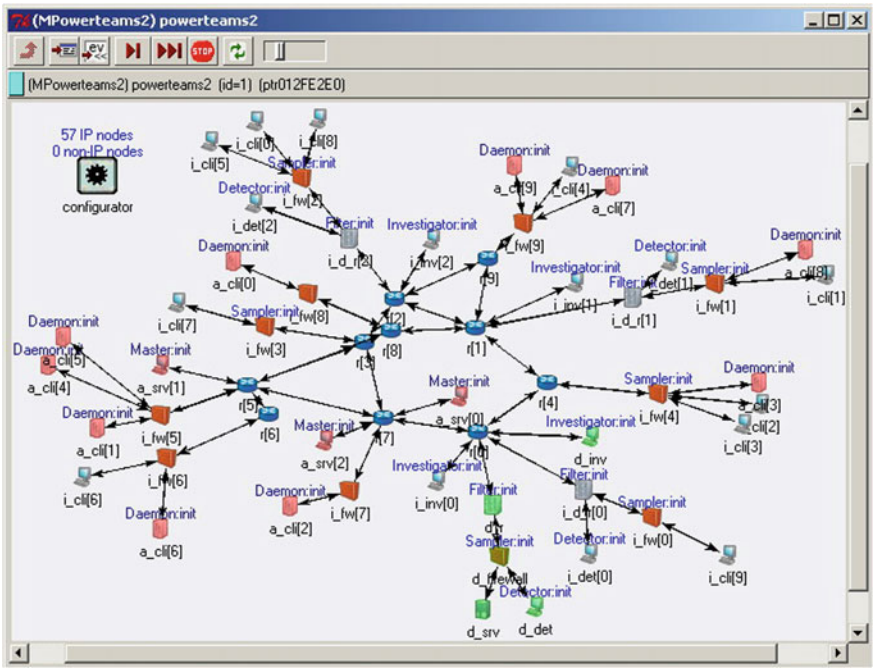
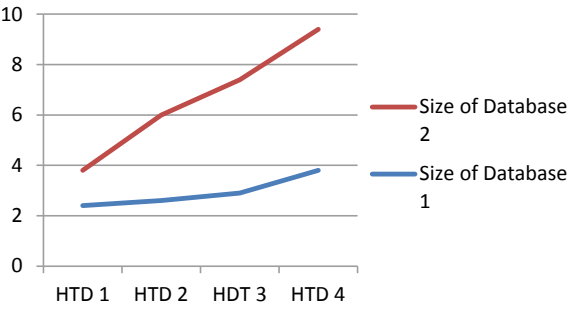


Fig. 6 To show a base station which is broadcasting if done using Huffman indexing

Fig. 7 AAL w. r. t. |*D*|



for retrieving geographic information in Wireless Environment which is based on wavelet wood data structure for text indexing or spatial indexing thereby establishing a new evaluation strategy. After by analyzing each scheme under the controlled environment and with selected criteria, our simulation results show two major advantages of the proposed H.T.D.: (1) It reduces response time significantly, and (2) it is more energy efficient.

References

1. Y.B. Kim, M. Shibata, T. Ehara, Agent-based broadcasting with video indexing. IEEE Trans. Broadcasting **42**(3) (1996). https://doi.org/10.1109/11.536583
2. J. Almeida, M. Narvekar, Review of techniques for data dissemination in broadcast environment, in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)* (2017). https://doi.org/10.1109/I-SMAC.2017.8058237
3. W. Sun, P. Yu, Y. Qing, Z. Zhang, B. Zheng, Two-Tier Air Indexing for On-Demand XML Data Broadcast, in*29th IEEE International Conference on Distributed Computing Systems* (2009). https://doi.org/10.1109/ICDCS.2009.42
4. D. Katsaros, N. Dimokas, Y. Manolopoulos, Generalized indexing for energy-efficient access to partially ordered broadcast data in wireless networks, in *2006 10th International Database Engineering and Applications Symposium (IDEAS'06)* (2006). https://doi.org/10.1109/IDEAS.2006.26
5. P, Yu, W. Sun, B. Shi, A parameterized flexible indexing scheme for data broadcast in wireless mobile environments, in *The Sixth IEEE International Conference on Computer and Information Technology (CIT'06).* https://doi.org/10.1109/CIT.2006.22
6. C. Arunachala, V. Aggarwal, B. Sundar Rajan, Optimal linear broadcast rates of some two-sender unicast index coding problems. IEEE Trans. Commun. **67**(6) (2019). https://doi.org/10.1109/TCOMM.2019.2907538
7. C.H. Chu, M.S. Chen, Y.F. Chen, On the energy efficiency for heterogeneous data broadcasting, in *2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware* (2009). https://doi.org/10.1109/MDM.2009.20
8. Y.D. Chung, S. Yoo, M.H. Kim, Energy- and latency-efficient processing of full-text searches on a wireless broadcast stream. IEEE Trans. Know. Data Eng. **22**(2) (2010). https://doi.org/10.1109/TKDE.2009.67
9. H. Kuwano, Y. Taniguchi, K. Minami, M. Morimoto, H. Kojima, A smart TV viewing and Web access interface based on video indexing techniques, in *2002 Digest of Technical Papers.*

International Conference on Consumer Electronics (IEEE Cat. No.02CH37300) (2002). https://doi.org/10.1109/ICCE.2002.1013993

A Survey on Human Action Recognition and Detection Techniques



Shankargoud Patil and Kappargaon S. Prabhushetty

Abstract The recognition and detection of activities of human have gathered a significant research importance in the field of computer vision. In the current paper, a performance evaluation on various techniques of Human Action Recognition (HAR) is carried out in detail. The applications of HAR are widespread and they range from Security Surveillance to Patient Health Monitoring Systems, Human-to-Computer interaction to Robotics, etc. In the recent past, many research articles have been published on HAR systems and HAR system is broadly divided into Pre-processing stage, Segmentation stage, Feature extraction stage, Action classifier stage and Action identification stage. The goal of the paper is to consider different stages of HAR system and to compare various algorithms used in these stages for input video datasets.

Keywords Human action recognition (HAR) · Computer vision · Feature extraction · Action classifier · Video datasets

1 Introduction

The analysis and recognition of human body movements from input video is a burgeoning area for researchers because of its widespread applications ranging from simple human–computer interaction to complex military operations [1]. The analysis of human motion can be divided into identification of actions and activities. Human actions are simple and periodic, such as hand gestures, laying, sitting, walking, running, and jumping. Human activities are complex and usually non-periodic, such as playing, fighting, and interaction in group.

Nowadays, CCTV cameras are deployed almost everywhere for the purpose of security, mainly to monitor human activities. Hence, the security surveillance systems are divided as three types. (i) Non-autonomous (ii) Partial autonomous and (iii)

S. Patil (✉)
S.G. Balekundri Institute of Technology, Belagavi, Karnataka, India

K. S. Prabhushetty
Veerappa Nisty Engineering College, Hasanapur, Shorapur, Yadgir, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_15

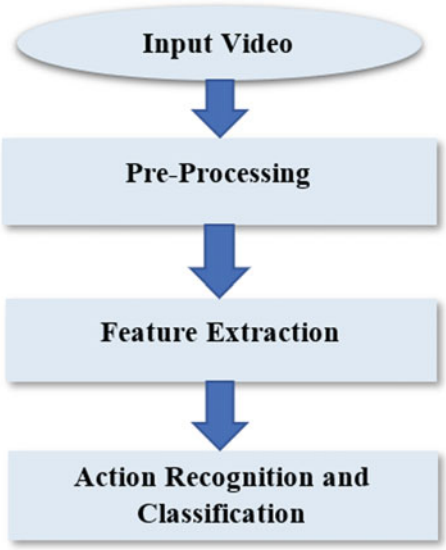


Fig. 1 Stages of HAR system

Autonomous. In non-autonomous system of video surveillance, the task of recognition and analysis is performed manually demanding the continuous monitoring of video by human. In partial autonomous system of video surveillance, human is also a part of video analysis. Lastly, in autonomous system of video surveillance, machine learning algorithms perform the function of processing, analyzing and recognizing with no intervention of human. The Human Action Recognition (HAR) system is broadly classified into three main stages and is shown in Fig. 1.

(i) Pre-processing (ii) Feature Extraction and (iii) Action Recognition and Classification [2]. In pre-processing, various tasks like conversion of video into frames, noise reduction and background subtractions are performed [1, 2, 4]. In feature extraction, the identification of object and extraction of its features is carried out with various algorithms being used, such as artificial neural networks, histogram of oriented gradients, data fusion techniques, Harris algorithm, Gabor algorithm, and one-dimensional CNN-based algorithm [1–8]. In action recognition and classification, the human action is recognized and classified into various types. The algorithms being used are Back Propagation Neural Networks, Mahalanobis distancing, Support Vector Machine algorithm, etc. [2–4, 8].

The input is taken from the available video datasets. Various video datasets are (i) CAVIAR, (ii) IXMAS, (iii) i3DPost, (iv) KTH, (v) Weizman, (vi) PETS, etc. [9–17]. The rest of the paper is organized as follows: A detailed and comprehensive survey of the existing literature is done along with performance evaluation in Sect. 2. The inferences drawn from the survey done are discussed in Sect. 3 while highlighting the work to be carried out in future.

2 Literature Survey

Babiker et al. [1] carried out a work on human activity recognition for video surveillance using neural network. The work was carried out in an indoor environment and a static camera was used to capture the mundane activities of human. In the stage of pre-processing, background subtraction algorithm is used, wherein, the video is converted into frames. The first frame is named as a reference frame and is subtracted from a foreground image frame, resulted in a human body. Next, in the stage of feature extraction, artificial neural network is used to extract the features of human activities. The collected samples are divided to train, test and validate the results. Lastly, a graphical user interface is provided to monitor the entire system. The coding was done in Matlab 2014. The five activities of human considered are, walking, laying, hand waving, boxing and sitting down. Toward the end a confusion matrix is constructed for training stage, testing stage and validation stage and an overall performance of 94, 93.3 and 94% was achieved in each stage. The limitation of the research is, the work carried out in an indoor environment with a static camera. Table 1 summarizes the performance of the system for the five human activities.

A system is proposed by Sehgal [2] for Human Activity Recognition using Histogram of Oriented Gradients (HOG) and Back Propagation Neural Network (BPNN) techniques. The experiment was conducted on a Weizman video dataset. The HAR system is broadly categorized into three main stages: Human detection, Feature extraction and Activity classification. In the stage of human detection, the background modeling is done in the first step to subtract the background image and to identify the human image present in it. If the result is not satisfactory, then it is suggested to use the morphological operations to remove the fallacious blobs. In the feature extraction stage, a technique of HOG is proposed that uses the feature descriptors. In the stage of activity detection, a multi-layered BPNN was adopted. The algorithm was implemented in three different steps: Feed-forwarding, calculation of error and updating the weights. The video comprises of nine different human activities got considered. Lastly, a confusion matrix was constructed showing an accuracy of 99.7% The limitations of the research are: (i) Consideration of a static background and (ii) A delay in the output due to BPNN classifier. In future, a dynamic background may be considered and an advanced classifier may be used to get the accurate output with no delay.

Karali and ElHelw [3] have done a research on Human Action Recognition using data fusion techniques. The proposed algorithm uses IXMAS and i3DPost datasets

Table 1 Performance of the system

Stages	Rate of recognition (in %)
Training	94
Testing	93.3
Validation	94
Overall performance	94

Table 2 Comparison of accuracy for IXMAS datasets

Techniques	Accuracy (in %)
MHSV/LDA	82
MHSV/MAH	84
TCBV/LMT	79
Data fusion	88

Table 3 Comparison of accuracy for i3DPost datasets

Techniques	Accuracy (in %)
MHSV/LDA	84
MHSV/MAH	78
TCBV/LMT	78
Data fusion	89

as input videos. The algorithm is classified into two stages. (i) Extraction of features and (ii) Classification of actions. In case of extraction of features, calculation of motion history and temporal change is carried out for skeletal volumes and bounding volumes respectively. Feature vector is formed by using Fourier Transform based on cylindrical coordinates to get the proper alignment. Later, the classification of action is done using the method of Mahalanobis distance and linear discriminant analysis. Toward the end, a table of comparison is formed to show the accuracy of individual techniques with fusion techniques for IXMAS and i3DPost datasets. Tables 2 and 3 depict the same.

The algorithm showed better results for fusion techniques compared to individual techniques.

A method is suggested for activity recognition of human, making use of spatio-temporal techniques by Mohana and Mahantesha [4]. The system being proposed is broadly classified into the stages of: (i) Pre-processing (ii) Feature extraction (iii) Action recognition and (iv) Performance measurement. In the first stage of pre-processing, the input videos are converted into frames and the noise present in the frames is reduced with the application of median filter. The pixel with the noise is detected by the median filter and is later replaced by the average value of adjacent pixels. In the second stage of feature extraction, three different extraction techniques have been proposed. (a) Harris technique (b) Gabor technique and (c) HOG technique. Harris algorithm adopts a technique of finding the corner in every pixel and later a mechanism of intensity variation is used to detect the object present in a frame. Gabor algorithm is used to find the object in a video by making use of Gabor wavelet and by finding the features of Gabor filter. Later, HOG is also used for detection of object that in-turn makes use of feature descriptors. A 3-Dimensional image of HOG feature extraction is plotted. In the third stage of action recognition, SVM algorithm is used for the purpose of action recognition. In the fourth and last stage of performance measurement accuracy, sensitivity and specificity of HAR system are estimated and is shown in Table 4.

Table 4 Performance measurement of HAR system

Parameters	Rate of recognition (in %)
Accuracy	95.3125
Sensitivity	92.5
Specificity	100

Table 5 Accuracy of the algorithms

Algorithm	Accuracy (in %)
Proposed	92.7
Random forest	89

Lee et al. [5] have proposed 1-dimensional CNN-based system to recognize the human activities using accelerometer. The input data was collected from the smartphones of users. HAR system was broadly classified into two types. (i) Gathering of input data (ii) Feature extraction. In the stage of gathering of input data, the data is collected from users' smartphones and is named as triaxial accelerometer data and is processed later. In the stage of feature extraction, one-dimensional CNN-based algorithm is used which consists of a convolution layer, a pooling layer, a fully connected layer and a soft-max layer. The three human activities such as walking, running and staying still are recognized through the proposed system. Toward the end, it is shown with the result that the proposed algorithm outperformed the random forest algorithm in terms of accuracy. Table 5 depicts the same.

Stefan Oniga and Jozef Suto presented a research in the field of health monitoring by recognizing the activities of a human [6]. A prototype was built consisting of smartwatch, microcontroller, accelerometer sensor, heart beat sensor and IoT. The proposed algorithm is classified into two types. (i) Input data acquisition and (ii) Action recognition. In the stage of input data acquisition, data is acquired from the prototype built. In the second stage of action recognition, the gathered data is used to train the artificial neural networks and a total of ten postures of human are recognized such as, standing, supine, left lateral recumbent, right lateral recumbent, prone, walking forward, walking backward, running forward, running backward and seating. The prototype is tested for different arm postures and body postures provided the recognition rate of 90% accuracy. In the future work, new sensors can be added to monitor the prototype. Advanced activity recognition techniques such as data fusion and fuzzy logic can also be used to improve the performance.

Jie Yang et al. proposed a novel model for the recognition of human activities. The input data was collected from CAVIAR video dataset [7]. HAR system is classified into three stages. (i) Feature extraction (ii) Feature modeling and (iii) Activity recognition. Prior to the above-mentioned three stages, adaptive background subtraction algorithm is used to remove the background image and to identify the foreground human present in the frame. In feature extraction stage, an adaptive Gaussian mixture technique is used. Author believed that color videos were not reliable hance videos got converted into gray colored videos and then processed. In feature modeling,

Table 6 Rate of recognition

Algorithm	Accuracy (in %)
CNN + MLP	99.40
CNN + LSTM	91.56
CNN + SVM	99.92
Overall	96.33

Expectation Maximization and Minimum Description Length principle are adapted. Finally, action recognition is done to classify the action by checking the Mahalanobis distance between test feature point and mean of Gaussian mixture. Lastly, a confusion matrix is constructed to compare the results with P. Ribeiro's method [7].

Basly H et al. have done the research work on human action recognition using CNN model and SVM classifier and the architecture was tested for MSR daily activity 3D dataset [8]. The proposed architecture is broadly divided into (i) CNN model and (ii) SVM, MLP and LSTM classifier. The input video got converted into frames are the inputs to the CNN model. The extracted spatial and temporal features act as inputs to the three different classifiers SVM, MLP and LSTM, the actions are identified and classified. A good recognition performance is achieved and is also compared with six existing technologies and outperformed the rest. Table 6 shows the recognition rate for the three different classifiers.

3 Conclusion and Future Scope

A comprehensive survey is done in the current paper on the techniques of recognition and detection of human actions by considering various renowned literatures in the field of computer vision. Researchers have proposed different machine learning algorithms in the stages of pre-processing, feature extraction and action classification for the input video datasets. The inferences drawn from this survey are listed below and they also serve as mere guidelines for the work to be carried out in future by researchers.

First, a thorough and deep understanding of the video dataset is very essential and a proper input dataset must be chosen for the research work to be carried out. Due to widespread availability of many standard datasets, it is challenging to choose the apt datasets as few are dedicated for single human action recognition and others are dedicated for group activity detection.

Second, un-processed videos will hamper the performances of algorithms used in feature extraction stage and that of a classifier stage as well. Knowledge of noise reduction techniques, background subtraction, etc. is essential to process the videos and make them available for next stages.

Third, a variety of questions remain unanswered in the stage of feature extraction as to choose the existing techniques or to develop novel approaches to extract the

features of an object. However, data fusion techniques and neural networks have shown better performance over individual techniques.

Finally, to classify actions, a suitable classifier must be used in action classifier stage depending on the ease of implementation and computational time requirements (Table 7).

Table 7 Comparative analysis with future scope of various algorithms used for HAR

Ref. No. and authors	Year and publication	Algorithms used	Input video datasets	Results	Future scope
Mohanad Bibiker et al. [1]	2017 IEEE	Background subtraction, artificial neural network	Videos from indoor environment	Overall performance of 94% is achieved	Standard video datasets can be used
Sonia Sehgal [2]	2018 IEEE	Background subtraction, histogram of oriented gradients and back propagation neural network	Weizman video dataset	For a static background an accuracy of 99% is achieved but resulted in delay due to BPNN classifier	A dynamic background can be considered and advanced classifiers may be used
Abubakrelsedik and Mohammed ElHelw [3]	2013 Springer	Motion history of skeletal volumes, temporal changes in bounding volumes and mahalanobis distancing	IXMAS and i3DPost video datasets	Fusion techniques showed better performance over individual techniques	Different algorithms can be considered for the Fusion techniques
H. S. Mohana et al. [4]	2021 Springer	Harris algorithm, Gabor algorithm, HOG and SVM algorithm	– –	GUI is provided and performance measurement of various parameters is done	Advanced techniques for feature extraction may be used
Song-Mi Lee et al. [5]	2017 IEEE	1-dimensional CNN-based algorithm	Users' Smart phones	Proposed technique showed better performance over Random Forest technique	Different human activities may be considered

(continued)

Table 7 (continued)

Ref. No. and authors	Year and publication	Algorithms used	Input video datasets	Results	Future scope
Stefan Oniga and Jozsef Suto [6]	2014 Proceedings of the 15th international carpathian control conference	Artificial neural networks	From prototype	Prototype is tested for different arm and body postures	Different human activities may be considered
Jie Yang et al. [7]	2009 IEEE	Background subtraction, adaptive Gaussian mixture technique	CAVIAR video dataset	Proposed algorithm outperformed P. Ribero's method	Advanced techniques for feature extraction may be used
Basly H. et al. [8]	2020 Springer	CNN model, SVM, MLP, LSTM classifiers	MSR daily activity 3D dataset	Overall performance of 96% is achieved	Suggested to use combination of genetic algorithms

References

1. M. Babiker, O. Khalifa, K. Htike, A. Hassan, M. Zaharadeen, Automated daily human activity recognition for video surveillance using neural network, in *IEEE 4th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA)* (Putrajaya, Malaysia, 2017)
2. S. Sehgal, Human activity recognition using BPNN classifier on HOG features, in *International Conference on Intelligent Circuits and Systems* (IEEE, 2018)
3. A. Karali, M. ElHelw, Motion history of skeletal volumes and temporal change in bounding volume fusion for human action recognition, in *MPRSS 2012, LNAI7742, 2013*, eds. By F. Schwenker, S. Scherer, L.-P. Morency (Springer-Verlag Berlin Heidelberg 2013), pp. 79–87
4. H.S. Mohana, U. Mahantesha, Human action recognition using STIP evaluation techniques, in *Progress in Advanced Computing and Intelligent Engineering, Advances in Intelligent Systems and Computing*, eds. by C. R. Panigrahi et al. (Springer Nature Singapore Pte Ltd., 2021)
5. S. Lee, S.M. Yoon, H. Cho, Human activity recognition from accelerometer data using convolutional neural network, in *IEEE International Conference on Big Data and Smart Computing (BigComp)* (IEEE, 2017)
6. S. Oniga, J. Suto, Human activity recognition using neural networks, https://www.academia.edu/15439945/Real_time_human_activity_monitoring. Last accessed 18 Apr 2021
7. J. Yang, J. Cheng, H. Lu, Human activity recognition based on the blob feature, in *IEEE International Conference on Multimedia and Expo* (IEEE, 2009)
8. H. Basly, W. Ouarda, F.E. Sayadi, B. Ouni, A.M. Alimi, CNN-SVM learning approach based human activity recognition, in *Image and Signal Processing. ICISP 2020. Lecture Notes in Computer Science,* vol. 12119, ed. by A. El Moataz, D. Mammass, A. Mansouri, F. Nouboud (Springer, Cham, 2020). https://doi.org/10.1007/978-3-030-51935-3_29
9. R.S. Rakibe, B.D. Patil, Background subtraction algorithm based human motion detection. Int. J. Sci. Res. Publ. **3**(5), 2250–3153 (2013)
10. N. Ravi N. Dandekar, P. Mysore, M.L. Littman, Activity recognition from accelerometer data, in *AAAI* (2005), pp. 1541–1546

11. V. Khong, T. Tran, Improving human action recognition with two-stream 3D convolutional neural network. 978-1-5386-4180-4/18/$31.00 (2018)
12. M.B. Rasheed, H.B. Raja, T.A. Alghamdi, Evolution of human activity recognition and fall detection using android phone, in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications* (IEEE, 2015)
13. W. Ding, K. Liu, F. Cheng, J. Zhang, Learning hierarchical spatio-temporal pattern for human activity prediction. J. Vis. Commun. Image Represent. **35**, 103–111 (2016)
14. M.S. Ryoo, Human activity prediction: early recognition of ongoing activities from streaming video. Iccv (2011), pp. 1036–1043
15. A. Eweiwi, C. Cheema, C. Thurau, C. Bauckhage, Temporal key poses for human action recognition, in *Proceedings of IEEE International Conference on Computer Vision* (2011), pp. 1310–1317
16. R. Kaur, S. Singh, Background modelling, detection and tracking of human in video surveillance system, in *Computational Intelligence on Power, Energy and Controls with their impact on Humanity (CIPECH), 2014 Innovative Applications* (IEEE, 2014), pp. 54–58
17. H. Wang, L. Shi, Foreground model for background subtraction with blind updating, in *IEEE International Conference on Signal and Image Processing (ICSIP)* (IEEE, 2016), pp. 74–78

Parallel Algorithm to Efficiently Mine High Utility Itemset



Eduardus Hardika Sandy Atmaja and Kavita Sonawane

Abstract Finding high utility itemset (HUI) from transactional databases like customer transaction data is not an easy task. The generated HUI should represent the real-world condition which contains set of items that likely to be purchased together and also has high profit. Many algorithms have been introduced to overcome that issue. Parallelism is one of the good architectures that can be adapted for mining algorithms, and it is rarely used for HUI Mining. The basic idea that can be adapted is by dividing the mining process based on subsearch spaces in concurrent time to boost the performance. This paper proposed two new frameworks that adapted parallel mining namely CLB and PLB which are extension of ULB-Miner algorithm. CLB is hybrid algorithm from CTU-PRO and ULB-Miner, and PLB is proposed because of inefficient process in CLB. From the experimental evaluation, PLB outperforms ULB-Miner in all cases regarding execution time.

Keyword High utility itemset · Data mining · Parallel processing · CLB · PLB

1 Introduction

Market basket analysis is a common instance of frequent itemset mining (FIM) which specifically deals with transactional databases such as customer purchase history. FIM helps to reveal products that are likely to be purchased together by analyzing customer buying habit. This technique commonly used by retailers to increase sales. They can optimize product bundling, placement, and recommendation and offer special deals to get customer satisfaction. Agrawal and Srikant [1] introduced FIM along with apriori as the algorithm that can efficiently discover

E. H. S. Atmaja (✉) · K. Sonawane
St. Francis Institute of Technology, Mumbai, India
e-mail: eduardus@student.sfit.ac.in

K. Sonawane
e-mail: kavitasonawane@sfit.ac.in

E. H. S. Atmaja
Sanata Dharma University, Yogyakarta, Indonesia

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_16

interesting patterns. There are several algorithms that were introduced afterward [2–4]. FIM uses minimum support threshold to identify which itemset is interesting or has high frequency in the database. This condition makes the interesting patterns become less meaningful in real-world situation. For example, tea and sugar are items that are likely to be purchased together but they give less profit when compared to washing machine.

To solve problem in FIM algorithms, high utility itemset mining (HUIM) was introduced. To find the profitable patterns, HUIM uses additional parameter such as quantity and profit. HUIM uses minimum utility threshold to decide whether an itemset is interesting or not. In HUIM, every item is not seen as equal like in FIM because every item has their own weight. That is the reason why HUIM is more complex thus designing efficient algorithm is very important. HUIM has been studied by many researchers, tree structure [6, 9, 10, 17] and utility list-based structure [7, 11–14] are the most interesting extensions because it has efficient data structure and also has efficient mining algorithm. Hybrid implementation [15, 16] is also done to combine advantages from different data structures to improve the performance. Moreover, computation technology such as multicore processor can be used as a powerful infrastructure to execute many tasks in a concurrent time that leads to efficient mining process [17–19].

In this paper, two frameworks are proposed for HUIM. The first framework is by combining utility list and tree-based algorithm to get advantages of them and applying parallel processing to the mining process. The second framework is by creating new parallelism framework to improve efficiency of ULB-Miner [7] algorithm.

2 Literature Review

FIM has been studied by many researchers, and apriori [1] is the first algorithm to solve FIM that introduces downward closure property. It means that for every itemset that has support below the minimum support threshold, all of its superset is infrequent, thus can be removed from the search space. This apriori idea greatly reduces the search space by removing unnecessary candidates. UMining and UMining_H [5] are extension of apriori to solve HUIM. It is designed more efficient than apriori but it may discover incomplete HUIs; moreover, it also does not satisfy downward closure property. Two-phase [8] is then introduced that applies downward closure property. Transaction weighted utilization (TWU) is the upper-bound to identify the unpromising item by applying transaction weighted downward closure (TWDC) strategy. All itemsets that have TWU below the minimum utility threshold can be pruned, thus a complete HUIs can be discovered. This concept is used by many tree-based algorithms [6, 9, 10]. CTU-PRO [6] has efficient tree structure called CUP-Tree. It is more compressed than the other above trees structures that makes the algorithm efficient.

The main problem in tree-based algorithm is that when the number of transaction is large then it becomes inefficient because more memory and time are needed to build

and mine the tree. Utility list-based algorithm is then introduced. HUI-Miner [11] is the first algorithm inspired by ECLAT [2]. The mining process works by combining itemsets within the utility list. This combination procedure is costly when there are too many items. FHM [12] solved the problem by developing Estimated Utility Co-Occurrence Structure (EUCS) and Estimated Utility Co-occurrence Pruning (EUCP) as the pruning strategy. This concept is used by many researchers to efficiently prune the search space. Some other utility list-based algorithms are [7, 13, 14], and ULB-Miner [7] has utility list buffer (ULB) that works like memory pipeline which reuses data segments whenever it is no longer needed thus makes efficient in memory consumption.

mHUIMiner [15] and UFH [16] are hybrid algorithms that combine tree and utility list-based algorithms. The tree structure is used to generate candidate itemset and helps to prune the low utility itemsets, and the mining process is done by utility list based. With this strategy, the search space can be reduced so it can reduce the memory usage and running time. Parallelism can be used to improve the performance of HUIM algorithms. Since the search space is independent, parallel mining is possible to do. The basic idea is by dividing the search spaces that can be mined concurrently. CHUI-Mine [17], pEFIM [18], and MCH-Miner [19] are algorithms that implemented parallel processing to mine HUI. pEFIM which is extension from EFIM [20] and MCH-Miner which is extension from iMEFIM [21] are the efficient two that apply simple load balancing to manage the resources. This strategy is efficient to boost the original algorithm performance.

3 Problem Statement

From a dataset, let $I = \{i_1, i_2, i_3, \ldots i_n\}$, where I is list of distinct items from dataset. Let $D = \{T_1, T_2, T_3, \ldots T_n\}$, where D is list of transactions from database. Each transaction has an id called T_{id}. Each item i in T_i has a quantity that represents how many i appeared in T_i. Every item $i \in I$ is related to a profit $p(i)$. Table 1 shows example of D, and Table 2 shows example of profit.

Problem Statement: Let D is transactional database and $minutil$ is minimum threshold of utility given by the user, then the problem in HUIM is that performs efficient mining process to reveal itemsets that have utility higher than $minutil$.

Table 1 Example of database

Tid	Transaction (item: quantity)	tu
T_1	(a:4), (b:1), (c:2)	9
T_2	(c:1), (d:3)	13
T_3	(a:2), (d:3)	14
T_4	(a:2), (b:3), (c:2), (d:1)	17
T_5	(b:1), (c:5), (e:3)	14

Table 2 Example of profit

Item	Profit
a	1
b	3
c	1
d	4
e	2

4 Proposed Algorithm

This research work presents two strategies being proposed and experimented namely hybrid framework termed as CLB and parallel framework termed as PLB. The pseudocode for CLB and PLB is given in Algorithm 1 and 2.

4.1 Hybrid Algorithm: CLB (ULB-Miner with CTU-PRO)

The hybrid idea of CLB is by modifying CUP-Tree [6] and combining with ULB-Miner [7]. The proposed data structure namely CLB-Tree, a modified version of CUP-Tree is constructed to maintain the database, reduce transactions, and manage parallel mining. The CLB-Tree construction is similar to CUP-Tree, and the differences are: (1) Every node maintains items, TWU, and utilities from similar transactions. It supports parallel processing by saving time to traverse all descendant nodes. (2) Every node contains calculated utilities so that there is no need to do repeated calculations. The CLB mining process occurs during the tree construction with a specific condition based on step 3c and 3d [17] in Algorithm 1.

Figure 1 illustrates CLB-Tree after inserting T_4. From our running example, T_1 is mapped into {(1:2), (3:3), (4:4)} and inserted into the tree. The count of these items is deducted by 1 so that the new set of count is Count = {3, 3, 2, 2}. T_2, T_3, T_4 are inserted in the same way and Count = {1, 0, 1, 0}. Count of item {d} and {a} is 0 so we can do local mining immediately using concurrent process for prefix 2 and 4.

Algorithm 1: CLB	**Algorithm 2**: PLB
Input: database `D`, minimum utility threshold `minUtil` Output: high utility itemset $HUIs$	

(continued)

(continued)

Algorithm 1: CLB	**Algorithm 2**: PLB
Step 1:Construct global item table **Step 2**:Initialize CLB-Tree **Step 3**:For each t ∈ D a. Revise and map t b. Insert t and update items, TWU and utilities for each node i ∈ t c. Reduce i.count ∈ t in global item table by 1 d. If i.count = = 0 then retrieve all node i and do parallel mine using ULB-Miner **Step 4**:Collect all HUIs	**Step 1**:Scan D to find promising items I where TWU(i ∈ I) ≥ minUtil and sort I into TWU ascending order **Step 2**:Scan and revise D to construct global ULB **Step 3**:Set n = number of CPU cores and create n empty local ULB **Step 4**:For each task i ∈ I do parallel: a. If no local ULB available then wait. Else, b. Assign and mine task i using available local ULB c. Release local ULB and notify main thread **Step 5**:Collect all HUIs

The next proposed strategy is that we distribute the search space based on prefix tree, and overall step 3 in Algorithm 1 explains this condition. Figure 2 shows enumeration tree for the search space. For local mining prefix 2 which is item {d}, the mining process only does task 3. Similar to prefix 4 which is item {a}, it only does task 1. The last strategy is by ordering the items. CLB-Tree uses TWU descending order but ULB-Miner uses TWU ascending order. This leads to incorrect calculation of remaining utilities. The order of the items is incorrect, and the distribution of the data from CLB-Tree is also incorrect. Then, items in CLB-Tree are sorted into TWU descending order and for same TWU value it is lexicographically sorted into descending order. In ULB-Miner, we sort them into ascending order. With this strategy, the order of the data is correct either for ascending or descending task.

4.2 Extended ULB-Miner: PLB (ULB-Miner with Parallel Framework)

PLB is proposed to improve performance of ULB-Miner [7] by applying parallel processing along with load balancing and more efficient memory management. Step 2 in Algorithm 2 is the same process as ULB-Miner to build global ULB. Based on the running example, Fig. 3a shows the global ULB.

Instead of exploring the search space sequentially like the original ULB-Miner, PLB explores it in parallel guided by enumeration tree in Fig. 2. The mining process in ULB-Miner uses the ULB as a memory pipeline. The explored data is inserted as a new data segment in the last index + 1 of UTLBuf and SULs from main ULB. This data segment can be reused when it is no longer needed. This strategy cannot

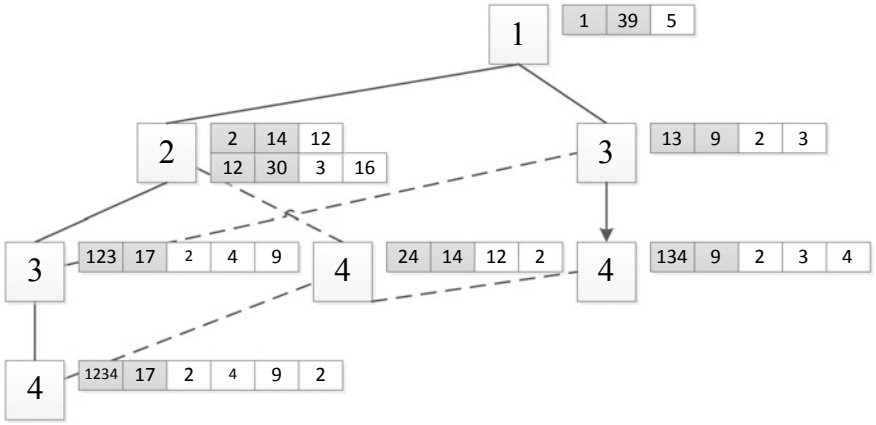


Fig. 1 CLB-tree after inserting T_4

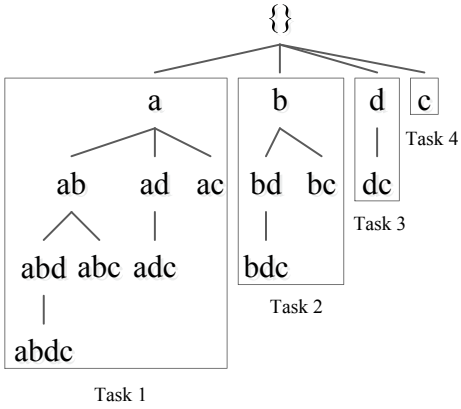


Fig. 2 Enumeration tree distribution

be applied to PLB because it causes collision and synchronization problem between threads. PLB introduces new strategy by applying load balancing and more efficient memory management. PLB limits the number of task pool based on the number of available processors [19]. It also creates and limits the number of local ULB to improve the memory efficiency during exploration. Step 3 and 4 in Algorithm 2 explain this strategy. Figure 3a and b also show illustration of the above explanation. For example, task 1 (item a) is explored by thread 1 and task 2, 3, and 4 are explored by thread 2, 3, and 4, respectively. Suppose we have extra item {e} that is executed through task 5, then it waits until any thread finished. Suppose thread 4 is finished and released its local ULB then task 5 is executed and reuses local ULB from task 4.

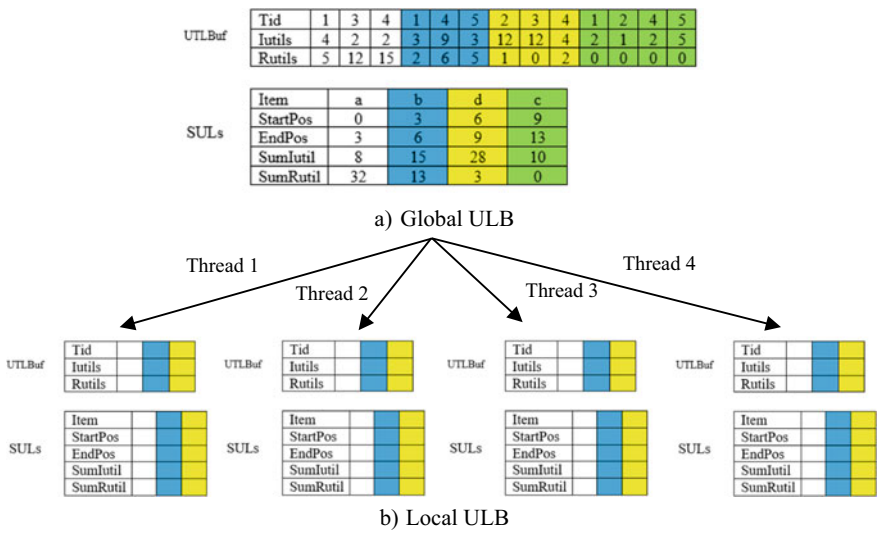


Fig. 3 PLB mining strategy

5 Results and Discussion

5.1 Experimental Setup

The experiments used three datasets, two standard benchmark structured datasets retail and kosarak available in SMPF Web site [22] and a real-world customer transaction dataset namely real retail from a store in Malang Indonesia. Retail and kosarak were chosen because these two datasets are complex with many transactions and many distinct items. Table 3 shows the datasets in details. The algorithms were evaluated based on minimum utility, memory usage, and the running time. For each algorithm, it was executed using the same minimum utility varied from 0.02–0.1% for retail, 1.5–3.,5% for kosarak, and 0.78–0.82% for real retail, then the results are compared. For the implementation, Java Netbeans IDE 8.2 was used. The experiments were performed on a personal computer equipped with fourth-generation Intel Core i5-4210U processor @1.7 GHz (4 logical CPUs), DDR3 8 GB RAM, and running Windows 10 Pro.

Table 3 Datasets details

No	Dataset name	Distinct items	Transactions count	Avg. length
1	Retail	16.470	88.162	10
2	Kosarak	41.270	990.002	8
3	Real retail	3.114	24.511	3

Table 4 Comparative analysis (ULB-Miner, CLB and PLB)

Dataset	ULB-Miner (Avg)		CLB (Avg)		PLB (Avg)	
	Runtime (s)	Memory (MB)	Runtime (s)	Memory (MB)	Runtime (s)	Memory (MB)
Retail	13.234	245.026	13.331	679.711	8.284	254.441
Kosarak	24.119	647.525	96.474	1.897.213	22.758	693.611
Real retail	0.892	23.960	0.772	34.184	0.762	25.234

Observations: Best cases runtime (PLB-0.762 s) and memory usage ULB-Miner-23.960 MB, PLB-25.234 MB)

5.2 Results and Analysis

Table 4 shows comparison for CLB and PLB with ULB-Miner performances which clearly states that CLB is not contributing positively with the intended objectives. For large database, it is inefficient because it needs more memory and time to build the tree, moreover creating many ULB for each local mining is inefficient. However, the proposed parallel framework named PLB is performing quite better in terms of running time as compared to CLB and the existing ULB-Miner algorithm.

5.2.1 Runtime

The experiments were done by setting the maximum task pool number to 4 since the processor has 4 cores. Figure 4 shows the results of the running time. It is clear that PLB has better performance than the ULB-Miner for all cases. The PLB running time is up to two times faster than ULB-Miner. For each dataset, let X be ULB-Miner runtime and Y be PLB runtime. For retail dataset $X = 1,5Y$, kosarak $X = 1,06Y$ and real retail $X = 1,2Y$ in average case. The results of retail dataset are the best and the results of kosarak are not significant but still better than ULB-Miner. Different dataset has different results because there are some factors that affect the performance, viz. distinct item count, transaction count, and transaction length. The distinct item count is the most affecting factor because it increases the search space. From the overall results, we can conclude that PLB can efficiently mine HUIs by applying parallel processing framework. It outperforms ULB-Miner which uses sequential process.

5.2.2 Memory Usage

The experiments were also conducted to compare the memory usage. Figure 5 shows the memory usage results. It is clear that in almost cases, ULB-Miner consumes less memory than PLB. It is reasonable because in parallel processing each thread need memory allocation to maintain their data. Instead of creating one local ULB for each subsearch space, PLB allocates only four local ULB to maintain data from

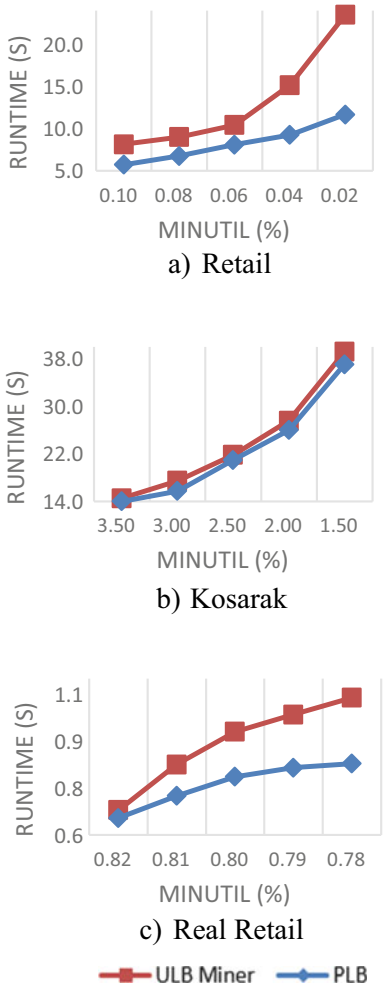


Fig. 4 Execution time for three datasets

its subsearch spaces. These local ULB are reusable, since every subsearch space is independent and can be overwritten. This approach can minimize the memory usage. This is the reason why even PLB has higher memory usage but the difference is not significant.

6 Conclusion

We have proposed two new frameworks to extend the original ULB-Miner to efficiently mine HUI namely CLB and PLB. CLB has a great concept to combine tree-based and utility list-based algorithm but the performance is relatively poor even it

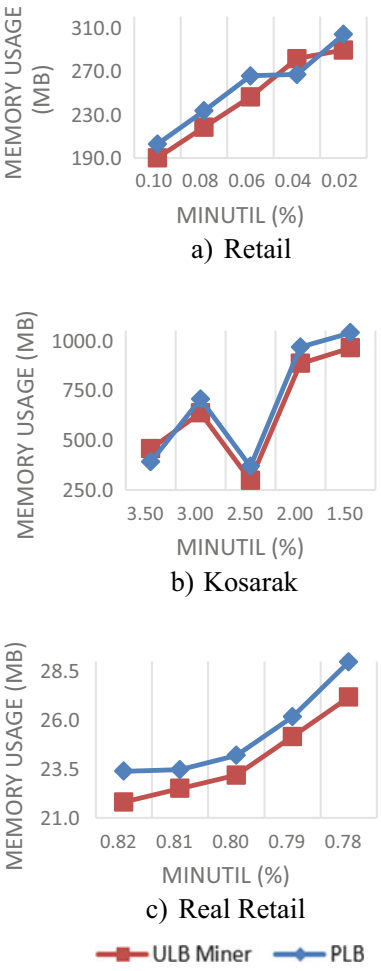


Fig. 5 Memory consumption for three datasets

can discover the correct HUI. The worst case is in large databases because it needs more memory and time to build the tree and creating individual ULB for all search spaces. PLB which is extension of ULB-Miner is proposed. Parallel processing, load balancing, and more efficient memory management are implemented to improve the efficiency. The results show that PLB outperforms ULB-Miner by up to two times faster. The drawback of PLB is that it consumes more memory to store the data for each active thread. This problem can be investigated in the future work by finding a way to do efficient memory management for parallel processing.

References

1. R. Agrawal, R. Srikant, Fast algorithms for mining association rules, in *20th International Conference on Very Large Data Bases* (Morgan Kaufmann, San Francisco, 1994), pp. 487–499
2. M.J. Zaki, Scalable algorithms for association mining. IEEE Trans. on Knowl and Data Eng **12**(3), 372–390 (2000). https://doi.org/10.1109/69.846291
3. J. Han, J. Pei, Y. Yin, Mining frequent patterns without candidate generation, in *2000 ACM SIGMOD Int. Conf. on Management of Data* (Association for Computing, New York, 2000), pp. 1–12. https://doi.org/10.1145/335191.335372
4. Y.G. Sucahyo, R.P. Gopalan, CT-PRO: a bottom-up non recursive frequent itemset mining algorithm using compressed fp-tree data structure, in *IEEE ICDM Workshop on Frequent Itemset Mining Implementations* (2004)
5. H. Yao, H.J. Hamilton, Mining itemset utilities from transaction databases. Data & Knowl. Eng. **59**(3), 603–626 (2006). https://doi.org/10.1016/j.datak.2005.10.004
6. A. Erwin, R.P. Gopalan, N.R. Achuthan, A bottom-up projection based algorithm for mining high utility itemsets, in *2nd Int. Workshop on Integrating Artificial Intelligence and Data Mining,* (Australian Computer Society, Australia, 2007), pp. 3–11
7. Q.H. Duong, P.F. Viger, H. Ramampiaro, K. Norvag, T.L. Dam, Efficient high utility itemset mining using buffered utility-lists. Appl. Intell. **48**, 1859–1877 (2018). https://doi.org/10.1007/s10489-017-1057-2
8. Y. Liu, W. Liao, A. Choudhary, A two-phase algorithm for fast discovery of high utility itemsets, in *9th Pacific-Asia Conf. on Knowl. Discovery and Data Mining* (Springer, Berlin, 2005), pp. 689–695. https://doi.org/10.1007/11430919_79
9. V.S. Tseng, B.E. Shie, C.W. Wu, P.S. Yu, Efficient algorithms for mining high utility itemsets from transactional databases. IEEE Trans. on Knowl. Data Eng. **25**(8), 1772–1786 (2013). https://doi.org/10.1109/TKDE.2012.59
10. Z.H. Deng, An efficient structure for fast mining high utility itemset. Appl. Intell. **48**, 3161–3177 (2018). https://doi.org/10.1007/s10489-017-1130-x
11. M. Liu, J. Qu, Mining high utility itemsets without candidate generation, in *21st ACM Int. Conf. on Information and Knowl. Management* (Association for Computing Machinery, New York, 2012), pp. 55–64. https://doi.org/10.1145/2396761.2396773
12. P.E. Viger, C.W. Wu, S. Zida, V.S. Tseng, FHM: faster high-utility itemset mining using estimated utility co-occurrence pruning, in *21st Int. Symp. on Methodologies for Intell. Systems* (Springer, Cham, 2014), pp. 83–92. https://doi.org/10.1007/978-3-319-08326-1_9
13. P.F. Viger, Y. Zhang, J.C.W. Lin, D.T. Dinh, H.B. Le, (2018) Mining correlated high-utility itemsets using various measures. Logic J. Interest Group Pure Appl. Logics (IGPL). **28**(1), 19–32 (2018). https://doi.org/10.1093/jigpal/jzz068
14. C.W. Wu, P.F. Viger, J.Y. Gu, V.S. Tseng, Mining compact high utility itemsets without candidate generation, in *High-Utility Pattern Mining: Theory, Algorithms and Applications* (Springer, Cham, 2019), pp. 279–302. https://doi.org/10.1007/978-3-030-04921-8_11
15. A.Y. Peng, Y.S. Koh, P. Riddle, mHUIMiner: A fast high utility itemset mining algorithm for sparse datasets, in *21st Pacific-Asia Conf. on Knowl. Discovery and Data Mining* (Springer, Cham, 2017), pp. 196–207. https://doi.org/10.1007/978-3-319-57529-2_16
16. S. Dawar, V. Goyal, D. Bera, A hybrid framework for mining high-utility itemsets in a sparse transaction database. Appl. Intell. **47**, 809–827 (2017). https://doi.org/10.1007/s10489-017-0932-1
17. W. Song, Y. Liu, J. Li, Mining high utility itemsets by dynamically pruning the tree structure. Appl. Intell. **40**, 29–43 (2014). https://doi.org/10.1007/s10489-013-0443-7
18. T.D.D. Nguyen, L.T.T. Nguyen, B. Vo, A parallel algorithm for mining high utility itemsets, in Proc. 39th Int. Conf. on Information System Architecture and Tech., vol. 853 (Springer, Cham, 2019), pp. 286–295. https://doi.org/10.1007/978-3-319-99996-8_26
19. B. Vo, L.T.T. Nguyen, T.D.D. Nguyen, P.F. Viger, U. Yun, A multi-core approach to efficiently mining high-utility itemsets in dynamic profit databases. IEEE Access. **8**, 85890–85899 (2020). https://doi.org/10.1109/ACCESS.2020.2992729

20. S. Zida, P.F. Viger, J.C.W. Lin, C.W. Wu, V.S. Tseng, EFIM: a fast and memory efficient algorithm for high-utility itemset mining. Knowl. Inf. Syst. **51**(2), 595–625 (2017). https://doi.org/10.1007/978-3-319-27060-9_44
21. L.T.T. Nguyen, P. Nguyen, T.D.D. Nguyen, B. Vo, P.F. Viger, V.S. Tseng, Mining high-utility itemsets in dynamic profit databases. Knowl. Based Syst. **175**, 130–144 (2019). https://doi.org/10.1016/j.knosys.2019.03.022
22. P.F.Viger, SPMF : An open source data mining library (2008–2021). http://www.philippe-fournier-viger.com/spmf/

A Review on Insulators in Transmission Line—Progress and Comparative Studies



Keka Mukhopadhyaya

Abstract Electrical insulation is the most important component in generation, transmission and utilization of electrical energy. Progress in this domain is interrelated with the advancement in material sciences. This paper has incorporated detailed view of the research carried out over the last half century that has contributed to the progress of high-voltage transmission in a broad sense. The paper further explores thoroughly the attention needed to improve the characteristics of dielectric materials so that their range of applications can be expanded. The article also highlights some gaps and suggests some future areas of research.

Keywords Ceramic · Porcelain · Polymer · Nanofillers · Sustainability

1 Introduction

An insulator maintains distance between lines from ground. This clearance depends upon the following factors: system voltage, safety margin and contamination, etc. Insulator also withstands all kind of mechanical, electrical and environmental stresses. Static, compression and dynamic load are example of mechanical stresses. Electrical stresses on insulator are mainly system voltage or electric field and over voltage. Temperature variation, contamination, pouring and ultraviolet ray are the example of environmental stresses. At different voltage level, different factors play the dominant role. At lower level of voltage transmission, mechanical clearances, corona and surges are important design factors. As the voltage level increases, main concentration moves toward lightning and switching surges. For very high voltages 765 to 1500 kV, contamination is the main factor for design consideration. Electrical equipment performs mainly based upon by the characteristics of its dielectric materials.

The voltage level for transmitting electricity from the generating station to load center is increasing on an average rate of 3% per year. In 1900, the voltage level

K. Mukhopadhyaya (✉)
CMR Institute of Technology, Bengaluru, India
e-mail: keka.m@cmrit.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_17

was around 100 kV, whereas in the year of 2017–18 the maximum value reached to 1200 kV. Voltages chosen for transmitting of bulk power have to follow international specifications standard. The maximum nominal voltage of a power system is 1150 Kv, and maximum operating voltage for the same level of transmission is 1200 kV. It is important that maximum operating voltage specified should not exceed at any part of the system, since level of insulation all equipment is chosen as per this level. Power transmission from generating stations to load centers through overhead lines greatly depends upon design and choice of materials of insulators. Design and choice of insulators greatly depend upon ambient temperature and overvoltage condition. It also depends on length of transmission line.

The first-generation insulating materials are mainly mica, rubber, marble and pitch; all of them are natural substances but having very poor insulating properties, viz. low resistivity and low breakdown strength. Therefore, they can only be applied for the low power levels of electrical equipment. Growth in global economy necessitates more electric power and therefore, insulator industries shifted toward synthetic insulating materials such as dielectric varnishes, resins, composites and impregnated dielectric fibers. Polymeric materials are the second generation of dielectric materials with better electrical properties. Their properties can be varied with chemical composition and molecular structure. The development of polymeric insulating materials is highly successful; however, with the continuation of increased voltage level, application of polymers insulating materials became limited. Some of the drawbacks of polymer insulating materials are accumulation of space charge, aging, flashover due to pollution and reversal of polarity in resultant field which became crucial factors for their applications [1]. Also, the power generation is moving toward the solar, tidal, wind and nuclear energy sources; therefore, it became obvious to search of materials that could be used in these environments of renewable energy sources. The different factors responsible for rapid growth in insulating materials properties are research toward renewable energy sources generation, introduction of extra and as well as ultra-high-voltage power generation and third to reduce adverse environmental effects at the time of producing, manufacturing, applying and recycling of insulating material to fulfill huge requirement of sustainable and environmentally friendly technology means. Thus, insulating materials based on nanodielectrics evolved in twenty-first century as third generation.

Section 2 of this paper highlights in detail the different types of insulators, whereas Sect. 3 deals with different important properties of dielectric materials that need to be addressed during their performance analysis. Section 4compares the performance of polymer and ceramic insulators. Section 4 discusses on simulation-based approach and defect detection. Section 5 emphasized that polymer insulator and nanocomposites are new-generation dielectric.

2 Type of Insulators

2.1 Ceramic and Porcelain Insulator

The significant progress in ceramic-type dielectric materials was observed after the First World War. It boosted the simultaneous development of the electrical and as well as electronic industries, as research moved toward betterment of the characteristics of the ceramic-type insulators as per application-specific requirements. The important properties of ceramic insulators need to concentrate are dielectric strength, power factor, resistivity and the impact of temperature and frequency on the performance of the insulators. Generally, ceramic insulator with dielectric constant with an average value of 5.5–6.5 is most common. Ceramics have power factors in between 0.004 and 0.0005 and resistivity in between 10^{10} and 10^{12} ohmmeter at room temperature. Dielectric strength ranges between 7.48–13.7MV/m at room temperature. It can be employed at 200 °C and above maintaining a good insulating property. But at high frequency, operation of ceramic insulator loss factor increases. The high stability of ceramic insulator is due to the strong ionic bond and high packing density of the constituting atoms of ceramics. A strong ionic bond is formed between oxygen and silicon in silica and silicates which results in a stable structure and, therefore, ceramic housing does not degrade because of environmental stresses like, UV radiation, humidity or any other electrical activity. Though it exhibits excellent radiation properties, some temporary lowering of electrical properties under high-intensity radiation occurs but with no permanent effect and, therefore, recovery is very fast. All ceramics are brittle in nature, low tensile and high compressive strengths. They are having chemical stability even at high temperature. They are good in thermal shock resistance because of low thermal coefficients of expansion and low thermal conductivities. The significant mechanical strength of the ceramic material is due to its rigid nature. Insulators can be designed for cantilever loads and tension. Therefore, the porcelain housing can be used for surge arresters, bushings and termination of cables without any other supporting materials. Low costs for raw materials are another advantage for ceramic insulator. Manufacturing process of porcelain insulators with larger housings is time-consuming because of prolonged time needed to thrust out core water content before shaping and firing. The major features of ceramic and porcelain insulator are their use at all voltage level, and it can withstand strong compressive force and high degree of standardization. Application of porcelain is mainly to produce pin and cap suspension units, hollow and solid core posts, multi-cone and long rod insulators, and housings of bushing. The major drawback with porcelain or ceramic insulator is their careful handling while transportation; the extensively damaged insulator can be easily identified, but minor crack or internal damage can be difficult to identify.

2.2 Glass Suspension Insulator

The glass insulators have higher breaking resistant in comparison with ceramics-type insulators. Compressive strength and dielectric strength are greater than ceramics. Relative deformation of glass insulator is very less with temperature change because of its low value of thermal expansion coefficient. Application of glass insulator is restricted to multi-cone posts and cap and pin suspension. Any defect during manufacturing such as any crack or hole can easily be identified in the glass insulators, but not in ceramic. Due to transparency, some sun rays travel through the glass insulator and reduce the degradation of insulator. But the major drawback is its low resistance toward bending forces than that of ceramics. A sudden strong impact can cause all glass insulators to break simultaneously. Impurities in composition or wide variations of temperature either during storing or operation can cause damage to the glass insulators. Absorption of contaminations of the glass insulators much easier than any other varieties of insulators. The moisture distills on the glass insulators' surface with much ease. But these insulators are more attractive to shoot as the shell explodes which is a major safety hazard. Manufacturing of glass insulators constitutes of many steps as ceramic insulators. Damaged glass insulator can be spotted easily. Nowadays, glass insulators are mainly used thermally treated glass, which resists formation of crack. Few disadvantages of glass insulator are heavy, it is fragile in nature and more attractive to vandalism. Glass insulators are completely crushed before cracking; therefore, faulty insulators can easily be detected.

2.3 Non-ceramic Insulators

This kind of insulators introduced in 1970s. The major advantages are it can be used for wide range of voltages, it is very light weighted and having high strength-to-weight ratio. The following sections discussed different insulators under this category.

2.4 Silicone Rubber

Application of silicone rubber (SiR) is mainly to coat porcelain and glass insulators. The main functional performance criteria for coatings are ice-phobic or hydrophobic, self-cleaning, durability, cost-effectiveness and ease of application. SiR is having better resistance to contamination, temperature, high elasticity and good electrical insulation property. It is widely used in insulators and accessories of cable in the high-voltage DC transmission lines [2]. Major disadvantages of SiR are its low thermal conductivity and having adverse effects on environment. Because of low thermal conductivity of SiR, accumulation of heat occurs around the area of discharge and

cannot dissipate readily. This causes the deterioration of SiR with time and may further causes tracking and as well as erosion [3] which ultimately leads to less longevity. It has been observed under DC voltage, degradation of SiR with more contaminants is more severe because of high conductivity and leakage current. Laboratory tests also confirmed the fact that at high temperature, the erosion and tracking phenomenon becomes prominent under the influence of positive DC voltage than AC voltage in vulcanized SiR insulators. The void, impurities or irregularity in shapes of insulators are the point of maximum stress and thereby initiation of electrical tree starts. Electrical trees even can cause permanent breakdown of insulation. It is understood that blends of SiR with other polymers like EPDM can provide improved flashover performance of the new insulating materials [4].

2.5 Polymer Insulator

Polymers have come out as the materials which can fulfill the high power level requirements at the best. To increase the breakdown strength of polar polymer materials are used which can trap electrons and thereby increases strength. As with increase in molecular weight, crystallinity decreases, therefore higher the dielectric strength. Cross-linked polymer has high dielectric strength because of high melting point. Polymers' complex formulation, the presence of impurities, defects or contaminants during processing increase dielectric losses and ionic conduction. Enhanced research of chemical and physical properties of insulating materials helped in production of huge numbers of plastic materials, viz. polyethylene terephthalate, polycarbonate, polystyrene used in thin film capacitor applications at high electrical stresses with minimal dielectric thickness. Polyethylene-insulated are in use from 1950s up to 15 kV voltage level. The 1960s experienced a quantum leap in the advancement of polymeric insulation for use under higher voltage. Two important applications found are extruded polyethylene used for HV cable, and thin polypropylene films introduced in capacitors. Then started the progress with synthetic insulation in HV domain and LV domain as thin film capacitor. Many challenges arose in the course of this expansion. In particular, it was realized that the electrical properties strongly depend on chemical and physical factors, which therefore provide two ways of tailoring the properties. In MV, HV and extra high-voltage applications, XLPE cables are considered as better choice due to its superior voltage endurance, thermomechanical performance very low losses and above all, easy manufacturability and jointing technology [5].

2.6 Nanodielectrics

They are manufactured by incorporating specific nanoscale fillers into the matrix of polymer which leads to improved electrical, mechanical and thermal characteristics.

Different characteristics such as breakdown strength and temperature resistance can be raised to a very high value with the help of proper pretreatment and proper choice of fillers. These even help for space charge reduction. The breakdown strength of composite dielectric depends on various factors, for example, properties at interface, particle dispersion and compatibility of filler and matrix. Nanosized SiO particles filled in cross-linked polyethylene (XLPE) composites have a high breakdown strength. Development of new electrical equipment causes improvement in insulating materials [6]. Han et al. studied trap energy density in the LDPE/ZnO nanocomposite materials and found two different energy trap distribution relating to the depth of the traps [7]. The introduction of trichlorodiphenyl as insulating oil improved the energy storage/unit volume capacity of capacitors. But this is injurious to human being and so changed with other alternating insulating liquid. Instead of silicon carbide nonlinear resistors, usage of zinc oxide varistor improved the coefficient of nonlinearity and surge energy absorption capability of insulators greatly.

3 Properties for Performance Analysis

The various properties which are extremely important for performance analysis of insulators are discussed below. Figure 1 highlights different types of materials used

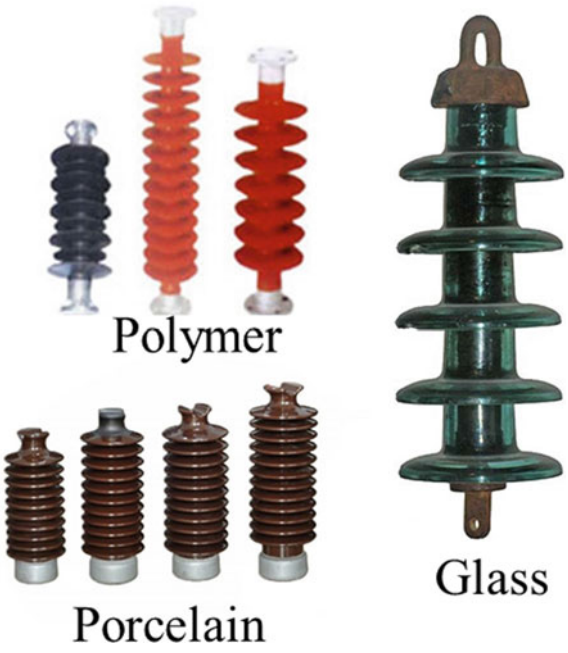


Fig. 1 Different types of electrical insulators

Table 1 Comparison of performance ceramic and polymer insulator

Parameters	Ceramics	Polymers
Weight	Heavier	Lighter
Fragility	Least shock absorption	Highly shock absorption capability
Vandalism	Prone to vandalism	Least prone to vandalism
Breakdown strength	Reduces with time	Longevity high
Hydrophobicity	Non-hydrophobic, degradation happened faster	Hydrophobicity of SiR forms beads of water and showed improved performance
Pollution performance	Inferior performance	Superior performance
Frosty climatic condition Performance	Better	Not satisfactory

for electrical insulators. The comparison of different properties is summarized in Table 1.

3.1 High Thermal Conductivity

Higher the thermal conductivity lesser the working temperature and heat accumulation; therefore, durability of insulator increases. In case of polymer insulators, heat conduction happens through the atomic vibrations and phonon. Factors which impact the thermal conductivity of insulating materials are free electrons, lattice structure, dipolar polarization, the number of polar groups, cross-linking and orientation. To enhance thermal conductivity of nanocomposite, designer need to change the type, content, and require to modify the surface. Surface modification helps to increase dispersion and particles combination inside a matrix [8]. Metal as a filler in polymer dielectric can exhibit high thermal conductivity, but the effect becomes prominent when the amount of filler is sufficiently high [9, 10] so that it can provide a continuous path. Therefore, metal powder as a filler is not a good choice.

3.2 Heat Resistance

High heat resistance is an important property to ensure minimum degradation of insulating material at high operating temperature. The materials are prone to undergo through different chemical reactions such as ozonization, hydrolysis and above all oxidation; these lead a remarkable change in the density, state, mobility, impurity, charge transport and thermal degradation of insulating material. Polymers with

aromatic rings have high resistance of heat because of strong bonds and rigid molecular chains. Adjustment of the molecular structure of polymers can improve the thermal properties of insulating materials.

3.3 Low-Temperature Resistance

The abrupt movement of the atoms and molecules reduces at low temperature, the internal configuration of materials tends to become in order, and the carrier density and mobility reduce drastically. This decreases the thermal conductivity and thermal expansion coefficient, whereas tensile and compression strength, dielectric loss increase, which ultimately leads to increased breakdown strength under AC voltage. Therefore, research is moving in the direction of developing materials which will exhibit improved mechanical and thermal properties of dielectric materials at low temperature. To improve the mechanical properties of insulating materials at reduced temperatures, increase in elongation percentage and tensile strength is important [11].

3.4 Water Absorption

Absorption of water from environment is a serious threat to film as it deteriorates electrical properties of polymer. Therefore, it is necessary to ensure production of high-quality polymers. Films with less water absorption are needed to ensure to decrease the impact of water.

3.5 Corona Resistance

Corona discharge is an inherent phenomenon associated with HVDC transmission lines even with properly designed insulators; therefore, there is a possibility of charge injection into the insulator surface and which can ultimately deteriorate the insulator [12]. Charge injection phenomenon depends on the initial external distribution of field [13]. In case of DC voltage, the charge accumulation on the insulator surface occurs because of constant electrostatic field which is not the case for the AC voltage. Duration of retention of charges on it for certain duration decided by the rate of decaying. The presence of surface charges causes early dielectric failure much before than predicted time and one of the factors for producing flashover [14]. Pollutant accumulation rate of DC voltage under the same electric field situation is 1.2–1.5 times more than that of AC voltage [15]. Longevity of electrical equipment depends on corona resistance of insulating materials. An improved corona resistance can be obtained by optimizing the dielectric system of the device, decreasing the distortion of electric field, controlling the accumulation of space charge, coating of semiconducting

materials on the device surface and inorganic nanofillers to the polymer [16–21]. There are many systematically placed spherulite structures around the nanoparticle-doped polymers which resist electric erosion and hence polymers show improved performance for partial discharge and corona [22, 23]. A small amount of titanium oxide-based nanoparticles can enhance the resistance toward corona of epoxy resin as they make the inner field uniform. Suitable methodology to manufacture thin and uniform films having high value of corona resistance is difficult [24]. Last half century has experienced a remarkable progress in this area. During 1960s, the natural insulating materials such as mica sheets were able to sustain a field of 10 MV/m approximately for 10 h. Inorganic insulating oxides exhibit higher thermostability, less oxidizability and better shielding of ultraviolet radiation. Incorporating inorganic oxides in nanoscale inside the polymer, better insulating performances with respect to space charge diffusion, charge distribution and increased corona resistance are observed. Kachi et al. observed that the corona discharge onset voltage and the current voltage characteristics are highly dependent on the nature and thickness of the dielectric layer [25], especially the ionic content is strongly affected by the materials homogeneity. Elastic mica tape exhibits more ordered structure with nanofillers and can withstand corona discharge for more than 200,000 h. Sometimes, dielectric materials work in very strong fields and therefore, easily discharge. Improving the dispersion of nanofillers and importing films with minimum defects can extend the films lifetime considerably during corona discharge in a field of the order of 40 MV/m [26]. It is also observed that SiR insulators when exposed to humid weather and severe pollutants, the hydrophobic nature of SiR can be hampered which will form a film of conduction on the surface of insulator. As a consequence, dry band arcing starts which in turn produces a large amount of heat.

4 Comparison of Ceramic and Polymer Insulating Materials

This section has compared different important characteristics parameters of ceramic and polymer insulator. The comparative studies reveal that ceramic insulator is disadvantageous with respect to weight, fragility than polymer. Its breakdown strength and non-hydrophobicity reduce drastically compared to polymer insulator. Ceramic material has high surface free energy because of strong ionic bonds, thereby there is a surface adhesion of pollutants. Because of high value of free energy of surface, porcelain gets easily wetted. Surface water readily forms filaments. These kinds of materials are hydrophilic in nature. The surfaces do not exhibit good insulating properties under polluted environment. This is because the conductive pollutant dissolves in water filament, thereby reduces the surface resistance of the insulator by forming a conductive continuous path of electrolyte. This path initiates flashover at lower voltage level. Polymer materials are by nature hydrophobic because of their low

surface energy, which generally used for outdoor insulating applications. But retention of hydrophobicity when exposed is of great importance. Water accumulates on hydrophobic substance in the form of bead; therefore, the conductive pollutant also dissolves within the water beads which is discontinuous in nature rather than forming a film. It results in less value of leakage current and less dry band formation probability; therefore, flashover can cause only by a high value of voltage.

Compared with porcelain, some polymer materials typically have much better flashover resistance, even when aged. Insulating materials working in moist, polluted, outdoors environments suffer from corrosion [27, 28] and form tracks for carrier's conduction, go along with the production of organic semi-conductive materials by the method of carbonization, and graphitization at the surface of the materials. Spark discharge is the main reason behind causing these conducting tracks at surface. The amount discharge current is more than partial discharge but less than arc discharge. Reduction of the surface tracks in insulating materials can be done by weakening the oxidation rate and suppressing the formation of a dry zone. Other significant method for this purpose is to enhance tracking resistance of insulating materials by reducing the number of benzene rings and groups, as they are easy to oxidize; by introducing polymers with low pyrolysis rate and producing few conjugated systems; producing new materials with less surface energies; preventing the formation of a continuous water film at the surface of materials; and suppressing the current at the materials surface. Nanofillers with crystallized water when used to dope polymers can decrease tracking. The reason behind this is the nanofillers get oxidized during spark discharge and as a result remove the free carbon at the surface. When crystallized water inside the composites is released, it flushes out the carbon granules over the material and reducing surface tracking. Ceramic insulator exhibits exceptionally better performance in frosty climate.

5 Discussion

Nowadays, improvement of various properties of silicon rubber is done by using the nanocomposite. Venkatesulu and Thomas et al. in their research highlighted improved resistance in tracking, and erosion of nanocomposites is because of compatibility between the main insulator and the filler nanoparticles [29, 30]. Research also highlighted that nanoparticles have a high impact on behavior of surface charge. Kumara et al. [31] noticed that flashover voltage changes proportionally with charge deposition irrespective of nature of charge. Degradation of material depends upon leakage current magnitude and duration of dry band arcing remains in a specific point [32, 33]. In coastal area, reason for SiR insulator degradation is thermal depolymerization triggered by electrical discharge. Different researcher studied the effect of composites in SiR insulators. Erosion resistance of composites of SiR, along with alumina trihydrate or silica as filler, greatly depends on thermal conductivity of the composite insulator [34]. Similarly, the study of electrical treeing by Chen et al. revealed that the starting time of tree of pure epoxy increases with incorporation of nanoparticles [35]. Tanaka

et al. even concluded that alumina as nanofillers is extremely beneficial in controlling both tree actuation and propagation through insulator [36]. Recently, advanced processing techniques, like additive manufacturing, have been used to study novel materials and their electrical performances under different environmental conditions to predict material behaviors for real-time performance [37].

Simulations can provide valuable insight into the insulator surfaces and their performance [38]. Potential and electric field values are critical parameters for designing and choosing the polymeric or ceramic insulators for transmission lines and substations. Nia et al. [39] compared different insulators under various conditions and voltages. They concluded that the all insulators have their advantages and disadvantages, and design modifications can be adjusted to address such specific features. Defect identification in insulators is currently dependent on manual investigation and time consuming. Fan et al. [40] have a proposed a convolutional neural network (CNN) method to detect defects in insulators as well as the location of defects. The efficiency of such deep learning methods has improved significantly. Recently, Choi et al. [41] also reported the use of machine learning tools for diagnosis of defects in a consistent and accurate manner.

6 Conclusions

Over the last century, the insulating materials used in transmission lines moved from porcelain, ceramic, glass to finally polymeric and nanocomposites and each category are having their own advantages and disadvantages. Recent research shows that the degradation of polymeric insulators depends on the type of electric stress, outdoor environmental stresses and is judged through loss of hydrophobicity, increase in leakage current, loss of fillers, depolymerization, surface cracking, chalking, discoloration, reduction in mechanical properties, tracking and erosion of shed materials. Nanocomposites showed better performance than regular composites under stressed indoor studies; however, mechanisms of nanoparticles doping on enhancing the properties of polymeric insulation material need some highlights, as well as the long-term operation characteristics of nanodielectrics. We significant gap exists in the intrinsic breakdown strengths. This gap can be bridged by taking advantages of the new-generation analytical tools, probes with spatial resolutions in the nanometer level. Further, simulation methods should also be used to predict insulation behaviors based on the real-time performances. The future research needs to be particularly focused on: the effect ambient temperature, electric field, space charge and volume resistivity under various fields.

References

1. Q. Lei, in *Recent progress of engineering dielectrics*, 1st edn. (Science Press, Beijing, 1999)

2. Z.D. Jia, S. Fang, H.F. Gao, Z.C. Guan, L.M. Wang, Z.H. Xu, Development of RTV silicone coatings in China: overview and bibliography. IEEE Electr. Insul. Mag. **24**(2), 28–41 (2008)
3. S.H. Kim, E.A. Cherney, R. Hackam, K.G. Rutherford, Chemical changes at the surface of RTV silicone rubber coatings on insulators during dryband arcing. IEEE Trans. Dielectr. Electr. Insul. **1**(1), 106–123 (1994)
4. S. Khatoon, A.A. Khan, S. Singh, A review of the flashover performance of high voltage insulators constructed with modern insulating materials. Trans. on Electr. Electron. Mater. **18**(5), 246–249 (2017)
5. A. Madonia, E.R. Sanseverino, P. Romano, I. Troia, S.F. Bononi, M. Albertini, S. Giannini, G. Mazzanti, Wireless partial discharge tracking on cross-linked polyethylene MV and HV cables. IEEE Electric. Insul. Mag. **34**(6), 8–17 (2018)
6. A.R. Said, A.G. Nawar, A.E. Elsayed, Enhancing electrical, thermal, and mechanical properties of HV cross-linked polyethylene insulation using silica nanofillers. J. of Mater. Eng and Perform **30**, 1796–1807 (2021)
7. Y. Han, S. Li, D. Min, Trap energy distribution in polymeric insulating materials through surface potential decay method. IEEE Trans. Dielectr. Electr. Insul. **25**(2), 639–648 (2018)
8. S. Wu, Q. Burlingame, Z. Cheng, Strongly dipolar polythiourea and polyurea dielectrics with high electrical breakdown, low loss, and high electrical energy density. J. Electron. Mater. **43**(12), 4548–4551 (2014)
9. J. Zeng, R. Fu, Y. Shen, High thermal conductive epoxy molding compound with thermal conductive pathway. J. Appl. Polym. Sci. **113**(4), 2117–2125 (2009)
10. M. Kozako, Y. Okazaki, M. Hikita, Preparation and evaluation of epoxy composite insulating materials toward high thermal conductivity, in *10th IEEE International Conference on Solid Dielectrics* (2010), pp. 1–4
11. J. Wang, L. Zhong, S. Li, in *Handbook of Electrical and Electronic Insulation Technology*, 1st edn. (CMP, Beijing, 2008)
12. B.X. Du, Y. Liu, H.J. Liu, Y.J. Yang, Recurrent plot analysis of leakage current for monitoring outdoor insulator performance. IEEE Trans. Dielectr. Electr. Insul. **16**(1), 139–146 (2009)
13. S. Kumara, S. Alam, I.R. Hoque, Y.V. Serdyuk, S.M. Gubanski, DC flashover characteristics of a polymeric insulator polymeric materials under different neutralization surface charges. IEEE Trans. Dielectr. Electr. Insul. **19**(3), 1084–1090 (2012)
14. B.X. Du, J.W. Zhang, Y. Gao, Effects of TiO2 particles on surface charge of epoxy nanocomposites. IEEE Trans. Dielectr. Electr. Insul. **19**(3), 755–762 (2012)
15. T.C. Cheng, C.T. Wu, Contamination flashover of HVDC insulators, Research Project 848–1, Final report (EPRI, 1981)
16. C. Calebrese, L. Hui, L.S. Schadler, A review on the importance of nanocomposite processing to enhance electrical insulation. IEEE Trans. Dielectr. Electr. Insul. **18**(4), 938–945 (2011)
17. I. Ramirez, E.A. Cherney, S. Jarayam, Comparison of the erosion resistance of silicone rubber and EPDM composites filled with micro silica and ATH. IEEE Trans. Dielectr. Electr. Insul. **19**(1), 218–224 (2013)
18. Y. Hu, R.C. Smith, J.K. Nelson, Some mechanistic understanding of the impulse strength of nanocomposites, in *IEEE Conf. on Electrical Insulation and Dielectric Phenomena* (2006), pp. 31–34
19. L. Liu, H. Shi, L. Weng, The effects of particle size on the morphology and properties of polyimide/nano-Al composite films. Polym. Polym. Compos. **22**(2), 117–121 (2014)
20. R.C. Smith, C. Liang, M. Landry, The mechanisms leading to the useful electrical properties of polymer nanodielectrics. IEEE Trans. Dielectr. Electr. Insul. **15**(1), 187–196 (2008)
21. Z. Han, C. Diao, Y. Li, Thermal properties of LDPE/silica nanocomposites, in *2006 IEEE Conerence. on Electrical Insulation and Dielectric Phenomena* (2006), pp. 310–312
22. P. Maity, S. Basu, V. Parameswaran, Degradation of polymer dielectrics with nanometric metal-oxide fillers due to surface discharges. IEEE Trans. Dielectr. Electr. Insul. **15**(1), 52–62 (2008)
23. M. Kozako, R. Kido, N. Fuse, Difference in surface degradation due to partial discharges between polyamide nanocomposite and microcomposite, in *Electrical Insulation and Dielectric Phenomena Annual Conference* (2004), pp. 398–401

24. T.C. Chang, C.W. Yang, K.H. Wu, Organic-inorganic hybrid materials Characterization and degradation of poly (imide–silica) hybrids doped with LiCF3SO3. Polym. Degradation Stab. **68**(1), 103–109 (2000)
25. M. Kachi, A. Nadjem, A. Moussaoui, L. Dascalescu, N. Zouzou, Corona discharge as affected by the presence of various dielectric materials on the surface of a grounded electrode. IEEE Trans. Dielectr. Electr. Insul. **25**(2), 390–395 (2018)
26. H. Li, L. Guo, B. Liu, A study of dielectric properties of polyimide/nano-titanium/dioxide composites films. Insul. Mater. **6**, 30 (2005)
27. H. Li, G. Liu, B. Liu, Dielectric properties of polyimide/Al hybrids synthesized by in-situ polymerization. Mater. Lett. **61**(7), 1507–1511 (2007)
28. V. Rajini, K. Udayakumar, Degradation of silicone rubber under AC or DC voltages in radiation environment. IEEE Trans. Dielectr. Electr. Insul. **16**(3), 834–841 (2009)
29. B. Venkatesulu, M.J. Thomas, Corona aging studies on silicone rubber nanocomposites. IEEE Trans. Dielectr. Electr. Insul. **17**(2), 625–634 (2009)
30. B. Venkatesulu, M.J. Thomas, Erosion resistance of alumina-filled silicone rubber nanocomposites. IEEE Trans Dielectr Electr Insul **17**(2), 61–624 (2010)
31. S. Kumara, B. Ma, Y.V. Serdyuk, S.M. Gubanski, Surface charge decay on HTV silicone rubber: effect of material treatment by corona discharges. IEEE Transactions on Dielectrics and Electrical Insul. **19**(6), 2189–2195 (2012)
32. R.S. Gorur, E.A. Cherney, R. Hackam, T. Orbeck, The electrical performance of polymeric insulating materials under accelerated aging in a fog chamber. IEEE Trans Power Deliv **3**(3), 1157–2114 (1988)
33. L.H. Meyer, S.H. Jayaram, E.A. Cherney, Correlation of damage dry band arcing energy, and temperature in inclined plane testing of silicone rubber for outdoor insulation. IEEE Trans. Dielect. Elect. Insul. **11**(3), 424–432 (2004)
34. L. Meyer, S. Jayaram, E.A. Cherney, Thermal conductivity of filled silicone rubber and its relationship to erosion resistance in the inclined plane test. IEEE Trans. Dielectr. Electric. Insul. **11**(4), 620–630 (2004)
35. Y. Chen, T. Imai, Y. Ohki, T. Tanaka, Tree initiation phenomena in nanostructured epoxy composites. IEEE Trans. Dielectr. Electr. Insul. **17**(5), 1509–1515 (2010)
36. T. Tanaka, A. Matsunawa, Y. Ohki, M. Kozako, M. Kohtoh, S. Okabe, Treeing phenomena in epoxy/alumina nanocomposite and interpretation by a multi-core model. IEEJ Trans. Fundam. Mater. **126**(11), 1128–1134 (2006)
37. O. Sefl, P. Vesely, J. Minar, K. Dusek, Novel Electrical Insulation Materials—Photodegradation Endurance of 3D Printed Polylactic Acid, in *2020 International Conf. on Diagnostics in Electrical Engineering, Czech Rep* (2020), pp. 1–5
38. P.R. Rohit, P.R. Rahul, M. Keka, Simulation Studies of Composite Insulators used in High Voltage Transmission. Int. J. Eng. Res. Electr. Electron. Eng. **5**, 11 (2018)
39. M.S.S. Nia, M. Altimania, P. Shamsi, M. Ferdowsi, Comprehensive analysis for electric field and potential for polymeric and ceramic insulators. Am. J. Electr. Electron. Eng. **8**(1), 26–34 (2020)
40. P. Fan, H.M. Shen, C. Zhao, Z. Wei, J.G. Yao, Z.Q. Zhou, R. Fu, Q. Hu, Defect identification detection research for insulator of transmission lines based on deep learning. J. Phys.: Conf. Ser. **1828**, (2019)
41. H. Choi, J.B. Koo, J.A. Son, J.S. Yi, Y.G. Yoon, O. TaeKeun, Development of equipment and application of machine learning techniques using frequency response data for cap damage detection of porcelain insulators. Appl. Sci. **10**(8), 2820 (2020)

Security and Privacy Issues of Blockchain Technology in Health Care—A Review



Nida Fatima, Parul Agarwal, and Shahab Saquib Sohail

Abstract Recorded healthcare data by using electronic health record (EHR) can be shared with numerous medical management units, hospitals, health centers, laboratory for identification of disease. Regardless of sharing data, it is vulnerable because it could be tempered or harmed as security and privacy have not been promised. In current time, it is shown that medical data is using cloud for storage, but there is also security, privacy and trust which has not been guaranteed. Therefore, researchers have come up with the solution known as blockchain technology to preserve data. By integrating cloud with this technology, data becomes invulnerable. As matter of fact, blockchain-based cloud technology can resolve lot of issues concerning healthcare industry. In this paper, systematic review of previous literature has been discussed. Also, state of the art on blockchain-based medical healthcare system has been presented by analyzing a few works. Also, the blockchain-based healthcare sector is gripped with some challenges. Significant among them being adoption of blockchain-based technique as it is quite different from the traditional approach, its adaptability and need for more research in the applications of blockchain for ensuring security and privacy of data. These issues have been mentioned in this paper. Some future directions can be of significant value for researchers and healthcare practitioners.

Keywords Healthcare systems · Blockchain · Electronic health record · Blockchain-based healthcare · Healthcare data · Cryptography · Threats

1 Introduction

As it is known that in medical industry, ample amount of data is generated meaning thereby healthcare system is data-intensive systems where data is circulated and accessed by different hospital, health centers, laboratory, medical management units.

N. Fatima (✉) · P. Agarwal · S. S. Sohail
Department of Computer Science and Engineering, Jamia Hamdard University, New Delhi, India

P. Agarwal
e-mail: pagarwal@jamiahamdard.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_18

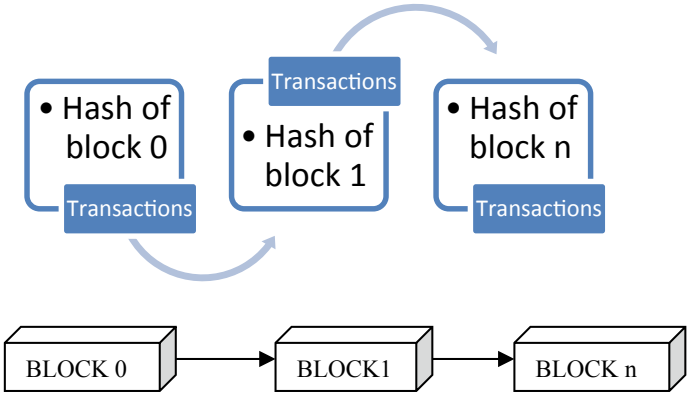


Fig. 1 Blockchain architecture

Now, digitization in healthcare industry is taking place resulting in development of healthcare information systems. Health care is an essential part of one's life so its data too as it helps in diagnosis of disease supporting proceedings for future reference. In old times, data was written and recorded which can be tempered and damaged effortlessly [1, 2]. There is a need to protect data arise. Thus, emerging technology came into view that is blockchain technology which promises to secure data from vulnerabilities and protect data leakage. If use with cloud computing, issue regarding to storage can be solved as it is most reliable method for management of data. Nevertheless, numerous security issues can be addressed while using blockchain-based cloud computing [3]. Basic architecture of blockchain is illustrated in Fig. 1.

Nakamoto [4], a report by Nakamoto concept of blockchain technology is introduced that amend challenges cryptocurrencies are facing. Author introduced technology for secure transaction. As blockchain technology insures genuineness, accountability, validity, anonymity and uprightness, it is preferred for securely sharing and hoarding information. Author proposed which promises confidentiality, answerability and validation for sharing of data. Proposed system considers public health authorities, researchers and blockchain miners. For preserving autonomy of information, cloud environment with blockchain is incorporated. Only verified users can access the system. All activities of users are monitored for purpose of answerability. For sharing of information, cryptographic techniques are used.

Li et al. [5], authors convey healthcare data is very essential for every individual and it storage too. The cause of concern is data vulnerability to theft, which can result in wrong diagnosis and mishap of revenue. Author proposes blockchain-based framework that authenticates storing of data effectively by using cryptographic techniques. Ethereum is a platform on which system is proposed as it sets out high accuracy of results. Proposed system assures security and privacy of data, and many users want their data to get stored in this architecture. As new patient arises, a novel fragment is created and every block has timestamp that gets authenticated by cryptographic mechanism and has hash data of prior fragment. Data is closely monitor so that

there is no unauthorized access. Proposed system has minimum risk to healthcare information as method used for recording of data is tamper proof.

Blockchain technology is distributed ledger technology with decentralized database management for multiple users and transaction. They are recorded with cryptographic signature know as hash. Thus, this technology can tolerate failure efficaciously [6]. Rest of the paper is organized as follows: Discussion is made on blockchain in health care in Sect. 2 with emphasis on its features in health care. Section 3 presents review of previously done work along with a review of some state-of-the-art blockchain-based healthcare systems. Section 4 discusses challenges faced by blockchain in health care, and lastly, work is summarized in Sect. 5.

2 Blockchain in Health Care

Presently, information of patients is being recorded electronically making use of electronic health record (HER), to diagnose a disease for further investigation. These healthcare records are being exchanged among various hospitals and health centers, but sometimes hospitals do not want to share data which results in data or information blockage, another threat in breach of privacy as it can be accessed. Thereupon, an approach came up as preserver known as blockchain to address issues like security and privacy of information which guarantees anonymity, confidentiality and accountability of records. Figure 2 shows features that would help in achieving security and privacy of blockchain in health care.

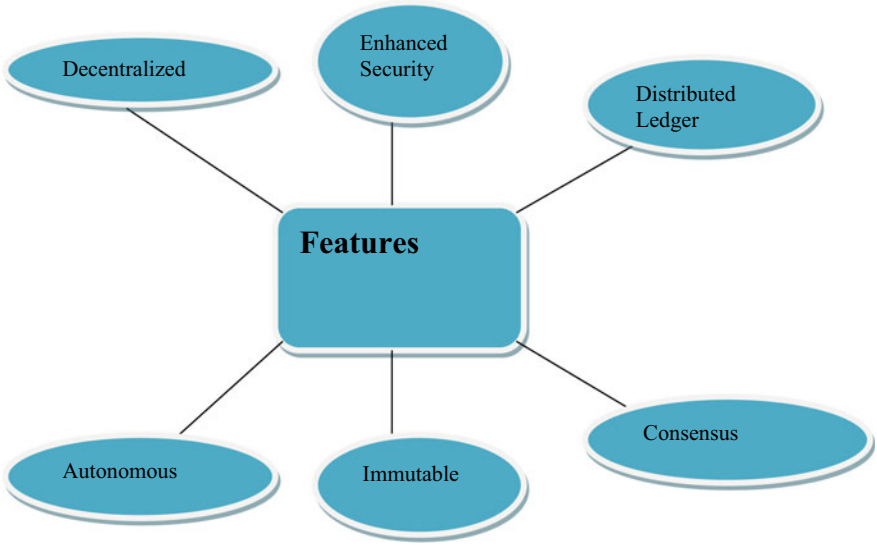


Fig. 2 Features of blockchain

Thus, features of blockchain can be summarized as follows [1, 7, 8]:

1. **Decentralized**—It is maintained by group of nodes where there is no governing authority. One can directly access data by using private key.
2. **Enhanced Security**—With the help of encryption technique, security of data is promised and information is hashed by hiding true content
3. **Distributed Ledger—**It uses nodes for storage of data so there exists ownership of data.
4. **Autonomous**—In blockchain, data is transferred and updated securely.
5. **Immutable**—Records in blockchain are immutable as they cannot be altered.
6. **Consensus**—Blockchain goes well with consensus algorithms; it helps network to make decision for the nodes that are registered on the platform.

3 Related Work

Health care is a complicated sector where ample amount of information is being generated, stored and shared on daily basis. Healthcare industry is having excessive resonance in terms of profit and information creation. As healthcare industry is expanding, there is an urge to secure data. With enormous amount of electronic health records (HER), invulnerability of information is the necessity of time. In today's time, data of patients is gradually shifting toward cloud repository. For making private data more certain, blockchain technology is impulse. In this section, discussion is being made upon blockchain-based health care with emphasizing on security and privacy of data [1]. Authors in Azaria et al. [9] put forward that in today's digital world, security and privacy of patient's data in healthcare industry are of at most important and the same needs to be stored in a digitized form. This can be done by employing blockchain technology to oversee healthcare data. This will help in achieving ultimate target of genuineness, answerability and assurance for data sharing which is required. Best suitable and flexible architecture is proposed to integrate information with regional and existing data storage. Proposed system guarantees secure access to medical records of patients with assuring them if any changes are done they are aware of it. Proper validation of credentials is done to check upon which blockchain minor has access to which data. Decentralization of medical records are put forward in secure way. Framework used is smart contact mechanism, and POW-based consensus algorithm is used to authenticate novel block in system. Recommended safety aspect of blockchain in health care is shown in Figure 3.

The works presented in Xia et al. [10] propound that privacy of healthcare data is utmost priority as it jeopardizes to violate patients' state. If infringement occurs, it will give negative impact on all the patients, stakeholders and miners. To overcome this situation, authors proposed blockchain-based technology framework to protect the liberty of data using cloud computing. Only verified users can have right to approach system. Cryptographic techniques are used for sharing of patient's details. So, it acts as a mediator between end user and radical medical data. Substantial blockchain has been suggested for swift transaction and actual competence. Three

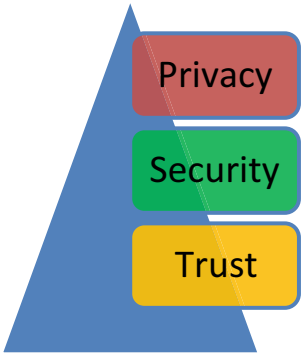


Fig. 3 Blockchain aspect of safety in health care

layers have been suggested by authors; they are user layer, system management layer and storage layer. The user layer comprises of data miners who want to entreat data. In system management layer, all connections are fixed for firm deal. Rearmost layer, i.e., storage layer, contains complete details which will set aside on cloud for further various applications. Dubovitskaya et al. [11], authors feel that healthcare data is immensely delicate and seldom the information required to conjunct with shareholders for exceptional motive. For this, blockchain-based health management system is proposed that guarantees accountability, confidentiality and lucidity of data. This architecture delineates for cancer-affected patients. The model ensures invulnerability of data, and time required for sharing of data is minimal. For storage of data, membership service databases is preferred that verifies blockchain face workers to ingress blockchain system. Uninterrupted data is stored on two databases that is local database and cloud server. The confined database holds cancer data, and cloud server holds unqualified information. All of execution appraisal by researchers is based on secrecy, certainty and extensibility. Work presented in Esposito et al. [12] shows that healthcare data is shifting to cloud services and is vulnerable to threats. For security and privacy of healthcare data, blockchain technology is proposed. In given system, it is identified who is the patient and how data is kept in blockchain technology. When a new patient is added, new block is attached to the structure. Blocks consist of distributed and decentralized network. Each block in existence blockchain has timestamp that gets verified with cryptographic techniques with hash details of prior block. Patients can directly access their data, and if any unlawful interference occurs, they get recognized effortlessly. Al Omar et al. [13], authors are of the opinion that cyber aggressor has interest in healthcare data as enormous revenue is involved. Author believes decentralized data can be secured effectively. For this purpose, healthcare data management system is integrated using blockchain technology as integrity and accountability are guaranteed. Privacy is ensured by using different cryptographic mechanism. It also checks information given by patient is lawful or not. The data receiver layer first authenticates system only after that data is received from end user. All the testimonials are stored by registration unit in which novel end user access data from system. Information like password, specifications, private information of users

are generated. After providing information one time, the user gets access through secured channel for transaction. The parties interact and exchange of information takes place by private accessible unit where secured transaction took place. In this, an arbitrator serves as a bridge between user and tactful information put down in subsist blockchain. In this blockchain technology, revert an identifier which assists user to approach the information. Kaur et al. [14], authors specify there is intense need to store healthcare data securely as the same is utmost importance being data heterogeneous in nature. So, they came up with idea of integrating blockchain with cloud computing as this platform is able to manage vast medical data very swiftly, thus guarantees security of information. In today's time, data is stored on centralized servers, but authors put forward decentralization thus incrementing interoperability. Files are stored in the form of fragments, so if any transaction occurs, it gets stored over different node and identification of user is done through cryptographic mechanism. Once verification process is completed, a new fragment is added about the deal and user gets permission to information access. Xia et al. [15], authors proposed structure, namely MeDShare that promises genuineness, answerability and efficacy of medical data using cloud storage as malicious activities which can cause damage to revenues that are generated by healthcare data, since current privacy policies are not that secure. In proposed system, data is secured in fiddle around manner by this healthcare data at minimum risk. Proposed method has four layers; they are user layer, data query layer, data provenance and structuring layer, lastly existing database infrastructure layer. First layer comprises blockchain miner as they want to access data to make transaction. Second layer processes and carry out queries generated by miners. Third layer consists of components likely authenticator, processing and consensus, contact, smart contracts permissioned database and blockchain network. The hindmost layer consists of all previous data. Uddin et al. [16], authors put forward blockchain-based framework for remote patients in healthcare environment in which they suggest that every single patient should have wearable devices so that their health data is monitored and information get stow in blockchain after computing. Fragments are built with the help of miner mechanics, and it diverges from existing bitcoin-based miner concept. In the proposed system, hash value of current block is generated by single minor which was not possible in bitcoin-based miner concept. Selection of miner is based on some feature extraction together with patient centric model for enduring patient information, but there is lack of proficiency as to how validation is done for block and authentication method is not completely probed**.** Table 1 summarizes some state of the art blockchain-based EHR work.

4 Challenges Faced by Blockchain Healthcare

Recent researches are concerned on employing blockchain technology in medical field i.e. healthcare to resolve issues related to trust, security and privacy of medical records but certain research opportunities and challenges need to be addressed for

Table 1 State-of-the-art blockchain-based EHR systems

Author	Technologies put forward	Repository	Security method	Privacy method	Blockchain forum
Griggs et al. [17]	Permissioned blockchain	Blockchain	Practical byzantine fault tolerance (PBFT)	Smart contracts	Ethereum
Shahnaz et al. [18]	Blockchain	Interplanetary File System (IPFS)	Data security is provided by role-based access control	Smart contracts	Ethereum
Zhang and Lin [19]	Consortium Blockchain	Blockchain	Consensus algorithms	Cryptographic mechanism	Consensus
Yang and Yang [20]	Blockchain	Local database and cloud server	Symmetric key encryption along with authorizing digital signature	Miner and smart contracts	Not discussed
Wang et al. [21]	Blockchain	Cloud	Searchable encryption with re-encryption conditional proxy method	Searchable encryption with re-encryption conditional proxy method	Ethereum
Zhou et al. [22]	Blockchain	Blockchain and Cloud	Cryptographic techniques used for security of patients	Cryptographic techniques for preserving privacy of patients	Ethereum
Liang et al. [23]	Permissioned Blockchain	Blockchain	Patient centric system which promises data integrity and ownership	Patient centric system which promises data integrity and ownership	Hyperledger Fabric
Tanwar et al. [24]	Blockchain	Blockchain	Provide data security by access control protocol	Provide data privacy by access control protocol	Hyperledger Fabric and Hyperledger Composer

gradually shifting from old method of recording data to blockchain-based electronic health record (EHR) system [25].

1. **It would take a major cultural shift—**Still, many doctors prefer to save record of patient on paper, asking them to shift on electronic mode that is electronic healthcare record (EHR) is a fact to ponder upon. Changing behavior of how people work in any industry is a big task.

2. **Health care is distributed so it is hard to implement—**It is tough for single user to access all the attributes altogether to adopt blockchain environment. If not adopted, practicality of system decreases.
3. **Some players are not willing to share**—Data which can lead to generation of revenue is kept private in organization, and if they are forced to share data with insurance companies, they get different quotations for different patients. Thus, it is very difficult to share data when it is for profit.
4. **There is nothing proven yet—**As there is no proven use-case healthcare professionals are not willing to adopt this technology and are not ready to work on the solution so that patient's data can be stored securely and in efficacious way.

5 Conclusion

Blockchain keeps track of all the data and the information shared over Internet. It promised invulnerability as one has to pass through different layer of security. If any unauthorized access is recognized by the system, it will block the network to safeguard the data. Sharing of information is secure as it is transparent and decentralized in nature. Blockchain rigorously protects information of patients. This paper put forwards review of previously done work using blockchain based technology for health care along with security and privacy issues in blockchain. Several state of the arts on blockchain-gleaned electronic health record (EHRS) system have been addressed with the motive to secure data from intruders. The need of the hour is to identify some effective methods of maintaining security and privacy of data which shall be identified and proposed in future work.

References

1. A. Saha, R. Amin, S. Kunal, S. Vollala, S.K. Dwivedi, Review on "Blockchain technology based medical healthcare system with privacy issues." Secur. Privacy **2**(5), e83 (2019). https://doi.org/10.1002/spy2.83
2. L. Ismail, M. Huned, Z. Sherali, in *Lightweight Blockchain for Healthcare* (IEEE, 2019), pp. 149935–149951. https://doi.org/10.1109/access.2019.2947613
3. F. Tian, *An Agri-Food Supply Chain Traceability System for China Based on RFID and Blockchain Technology* (IEEE, Kunming, China, 2016)
4. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008). http://www.bitcoin.org. Accessed 11 Feb 2019
5. H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, S. Liu, Blockchain-based data preservation system for medical data. J Med Syst. **42**(8), 141 (2018)
6. https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain. Date of access 31 March 2021
7. https://www.google.com/amp/s/101blockchains.com/introduction-to-blockchain-features/amp/. Date of access 2 April 2021
8. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in *2017 IEEE international congress on big data (BigData congress)* (IEEE, 2017), pp. 557–564

9. A. Azaria, A. Ekblaw, T, Vieira, A, Lippman, in *Medrec: Using Blockchain for Medical Data Access and Permission Management* (IEEE, Vienna, Austria, 2016)
10. Q. Xia, E. Sifah, A. Smahi, S. Amofa, X. Zhang, BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information **8**(2), 44 (2017)
11. A Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, F. Wang, Secure and trustable electronic medical records sharing using blockchain, in *AMIA Annual Symposium Proceedings* (Maryland, 2017)
12. C. Esposito, A. De Santis, G. Tortora, H. Chang, K.K.R. Choo, Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. **5**(1), 31–37 (2018)
13. A. Al Omar, M.S. Rahman, A. Basu, S. Kiyomoto, *Medibchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data*, vol. 10658 (Springer, Guangzhou, China, 2017)
14. H. Kaur, M.A. Alam, R. Jameel, A.K. Mourya, V. Chang, A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. J Med Syst. **42**(8), 156 (2018)
15. Q. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, M. Guizani, MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access. **5**, 14757–14767 (2017)
16. M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, A patient agent to manage Blockchains for remote patient monitoring. Stud Health Technol Inform. **254**, 105–115 (2018)
17. K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst. **42**(7), 130 (2018)
18. A. Shahnaz, U. Qamar, A. Khalid, Using Blockchain for Electronic Health Records. IEEE Access **7**, 147782–147795 (2019). https://doi.org/10.1109/access.2019.2946373
19. A. Zhang, X. Lin, Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. J Med Syst. **42**(8), 140 (2018)
20. H. Yang, B. Yang,. A Blockchain-Based Approach to the Secure Sharing of Healthcare Data (Norwegian Research Council, Oslo, Norway, 2017)
21. Y. Wang, A. Zhang, P. Zhang, H. Wang, Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. IEEE Access **7**, 136704–136719 (2019)
22. L. Zhou, L. Wang, Y. Sun, Mistore: a blockchain-based medical insurance storage system. J Med Syst. **42**(8), 149 (2018)
23. X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li, Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications. Montreal, QC (IEEE, 2017)
24. S. Tanwar, K. Parekh, R. Evans, Blockchain-Based Electronic Healthcare Record System for Healthcare 4.0 Applications. J. Inf. Secur. Appl. **50**, 102407 (2020). https://doi.org/10.1016/j.jisa.2019.102407
25. https://news.childrensmercy.org/6-challenges-to-healthcare-blockchain-adoption/. Date of access 1 April 2021

Hardware Trojan Detection Using Deep Learning-Generative Adversarial Network and Stacked Auto Encoder Neural Networks



Fredin Jose, M. Priyatharishini, and M. Nirmala Devi

Abstract The exponential growth in technological development boosted the IC industry in production of IC chips in a span of 12–18 months. It has paved way for increased outsourcing which leads to malicious modification by inserting hardware trojans. It becomes necessary to detect these defects before IC fabrication in pre-silicon production stage to save the production cost. In this paper, we propose a method for HT detection using gate level netlist. Extracted features from the netlist of circuits are used for dataset creation. From the extracted features, designed deep learning neural network model figures out salient trojan features required for HT classification of nets into trojan-free and trojan infected nets. In addition to this, data imbalance problem occurs in dataset is taken care by preprocessing data using generative adversarial network. Deep learning-based hardware trojan classifier is evaluated with performance metrics like confusion matrix, F-measure, accuracy for ISCAS'85,'89 benchmark circuits and Trust-Hub circuits.

Keywords Hardware trojan (HT) detection · Gate level netlist (GLN) · Trojan features · Deep learning (DL) · Neural network · Imbalanced data · Generative adversarial network (GAN) · Stacked auto encoder (SAE)

1 Introduction

Decades before the technological advancement, complexity as well as rate of production of chips per year was very less. Rapid developments in semiconductor field increased these chip production rate and majority of ASIC IC design were outsourced to 3rd party vendors. The first HT has discovered from a military-grade FPGA and since then every outsourced IC is suspicious to use by the companies because these

F. Jose (✉) · M. Priyatharishini · M. N. Devi
Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India

M. N. Devi
e-mail: m_nirmala@cb.amrita.edu

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_19

hidden HT which will get triggered under very rare conditions may steal confidential information from a device or may deteriorate the device performance or even affect the complete functionality of device. Conventional detection methods like reverse engineering may fail to detect these trojans and its drawback can be solved to an extend by HT detection using global power leakage-based methods [1] like side-channel analysis in post-silicon stage [2].

Later HT detection further improved by incorporating machine learning(ML) techniques like naive Bayes (NB), k-nearest neighbors (KNN), K-means, support vector machines (SVM) [3], neural network (NN). Among NN, there are various algorithms like Autoencoder (AE) [4], Denoising Autoencoder (DAE), Sparse Autoencoder, Deep Convolutional Network (DCN) are proven to perform better.

In this study, HT detection based on deep learning (DL) approach using GAN coupled with SAE deep neural network structure is employed. GAN model is used for preprocessing of dataset and autoencoder for classification of nets. Dataset for training and testing the model is developed using the features extracted from GLN.

The rest of this paper is organized as follows: Sect. 2 presents the literature survey of related experiments. Section 3 discusses about methodology of this experiment in various phases and novelty of this work by using preprocessing dataset and a gist of classification model. Section 4 demonstrates experimental results using DL and comparison of results with existing methods. Section 5 concludes this paper.

2 Overview

Liakos et al. [5] briefed effects due to this hazardous HT modification and also provided a ML applications for detection of HT. Huang et al. [6] classified all possible trojan attacks and discussed recent works with respect to different perspectives. Hasegawa et al. [7] proposed a method to detect HT, by extracting 11 features of trojan net from GLN. This method focused on training a multi-layer neural network ML model, in IC design step itself and obtained 100% TPR. In [8], it paved way for new feature extraction from netlist, which describes trojan nets of netlist. Sorting best set of 11 features out of 51 features helped for classification of all nets in netlist with improved performance metrics. In [9], they discussed a method for detecting trigger nets at gate level in which extraction of trigger feature values for each net from known netlist's used to train two different types of detection models. This method is able to obtain 88% TPR, 90% TNR, and 90% accuracy.

Reshma et al. [10] detected trojan nodes from genuine ones using transition probability and controllability as features. This work used those features for DL using k-means clustering and was able to validate without any golden model as reference. A novel design framework proposed called TSA-NoC which adopts artificial NN and deep reinforcement learning-based design for HT in run time is presented [11]. Alom et al. [12] surveyed different categories of learning such as supervised, unsupervised, and semi-supervised methods.

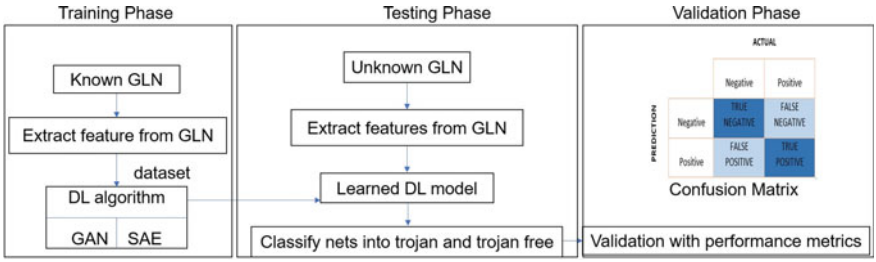


Fig. 1 Flow diagram of proposed scheme

A study on imbalanced fault diagnosis using GAN to create synthetic samples of faulty minority class is presented in [13]. This method solves data imbalance between normal class and fault class samples, which in turn is applied to stacked autoencoder for diagnosis of fault [14]. Tan et al. [15] try to overcome unstable samples of power system by introducing DL-based TSA framework, which used DAE classifier fed with synthesized data samplings to avoid data inequality of classes. Different benchmark circuits in Trust-Hub and different TRIT Generated Trojans inserted in various combinational and sequential circuits are also used in the work [16, 17].

3 Proposed Methodology

3.1 Feature Extraction

The proposed scheme for HT detection is implemented in three different phases as shown in Fig. 1. First phase has prior works like preparing GLN by synthesize Verilog code of different ISCAS'85,'89 circuits. Then, required number of trojan features are extracted from netlist using algorithms in Python. Using these extracted features, sufficient number of datasets of trojan-free circuit is created. Designing and inserting trojan modules in pure circuits and extracting trojan features of trojan infected circuit is followed. Integrating all these datasets to give full dataset, which is applied as input to created DL model for training is attempted.

3.2 Data Preprocessing

When the amount of the faulty data collected is less than that of genuine samples, even if fault samples are classified as normal, prediction accuracy will be high which results in model biasing. This issue can be handled by resampling techniques like oversampling of minority class or under-sampling of majority class or by generating

synthetic samples by using Synthetic Minority Oversampling Technique (SMOTE), Generative Adversarial Network (GAN).

GAN is implemented using Keras that runs on the top of TensorFlow. GAN consists of generator (G) with five fully connected layers of neural network, to create fake samples identical to real samples and, discriminator (D) with seven fully connected layers of NN, to identify difference between fake and real samples. By initializing G and fixing this value, D is trained with maximizing loss function for able to identify difference between real and fake samples. Then, noise sample $G(z)$ from G and real sample X is given to D, which results feedback error signal $D(x)$ to G. With that G is upgraded with minimizing loss function to make fake sample nearly identical to the real samples [13].

When $D(x)$ is not equal to equilibrium condition, G and D train again alternatively, and when equilibrium condition is satisfied, synthetic samples obtained in which generated fake samples will be identical to real samples. Preprocessed data is given to train classification deep learning model, which will reduce HT net classification error in this study.

3.3 Classification Model

Classification model is implemented using Keras. SAE with multiple hidden layers intake combined dataset of original data and synthetic data, for representing features in a reduced dimension by retaining salient features required for trojan classification. Hidden layer with minimum number of neurons finally decides what all are necessary features and output layer reconstructs these features. Model is trained by further tuning its parameter to increase accuracy which is then used for classification of any unknown nets into trojan infected or not. Performance of DL algorithms is evaluated using performance metrics for the classification problems like confusion matrix, accuracy, precision, recall, F1-score [8].

4 Results and Discussion

In this section, we demonstrate various extracted features, results of generative adversarial network used for preprocessing of data discussed in section III, and classification results of various test circuits. We have used Synopsys 90 nm technology for netlist preparation and algorithms are implemented in Python 3.8 using Atom editor and Google Colab.

Table 1 Extracted features from netlist

Trojan feature	Description ($1 \leq x \leq 5$)
Connectivity	Maximum number of inputs that output of single logic gate can feed
Primary input/ output	Minimum logic level, from any primary input/output to the net n
Fan_in_*x*	Number of logic-gate fan-in, up to x- level away from the net n
In/Out_Flipflop_*x*	Number of flip-flops, up to x-level away from the input/output side of the net n
In/Out _multiplexer_x	Number of muxes, up to x-level away from the input/output side of the net n

4.1 Feature Extraction

Different benchmark circuits are chosen for experimenting and their RTL design code is synthesized in 90 nm technology by Synopsys design compiler tool to create gate level netlist with logic cells. Sufficient number of trojan features are extracted with algorithms in Python as shown in Table 1.

Table 1 comprehends each trojan feature's relevance. Connectivity and fan in implicate number of transitive fans in of trojan net. Primary input and output implicate nearness of trojan net with input or output, which results in a chance to activate HT or to leak internal signal from chip. In and out flipflop explicitly says necessity of flipflops to memorize internal states of circuit. In and out mux also explicitly indicates multiplexer receives trigger signals to switch different output signals.

4.2 Synthetic Data Generation

A combined model of stacked generator and discriminator is used, which takes noise and generated data as input, respectively. It generates synthetic data when conditions are met. GAN can be evaluated using four methods as shown in Fig. 2 to check whether the generated data is similar to the actual data.

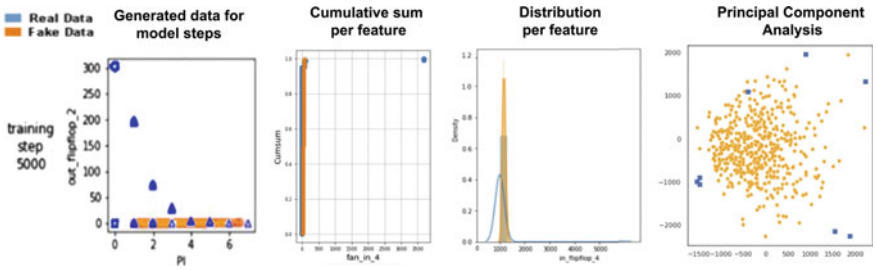


Fig. 2 GAN evaluation methods

Generated data for the model steps is the visualization of new synthetic data generation of various features with respect to iteration. It shows the generated data changes as the network learns the embedding more accurately. Cumulative sums per feature are used to display the total sum of data as it grows over iteration. It shows feature by feature comparison between the generated data and actual data. Distribution per feature shows how the newly generated data is distributed over the iteration on the horizontal axis and density on the vertical axis. If the generated fake data is similar to the real data, both plots will be overlapped each other and the variation between them shows inequality of real and fake data. Principal component analysis visualizes the dimensionality reduction method by minimizing loss of features information in newly generated data and indicates dependency among new data and real data.

4.3 Hardware Trojan Classification

Classification model used for binary classification, whether net is trojan infected or not. Binary cross-entropy is used as loss function and giving promising results. After training is done, any unknown test circuits can be tested to detect suspicious nets.

Trojan net is taken as positive and normal net is taken as negative for confusion matrix. Test results of the various test circuits are tabulated in Table 2. This binary classification results are obtained as confusion matrix, whose four values count the results, True Negative (TN), False Positive (FP), False Negative (FN), and True Positive (TP) [9]. TN means number of the genuine nets correctly classified to normal nets. TP means number of the trojan nets correctly classified to be trojan nets. FN means number of the trojan nets mistakenly classified to be genuine nets. FP means number of the genuine nets mistakenly classified to be trojan nets. Based on those

Table 2 Test results of various circuits

SI No	Test data	TN	FP	FN	TP	Acc.	Recall	Precision	F-score
1	C6288-T000	4528	0	1	7	99.97	87.5	100	93.3
2	C6288-T86	4528	0	2	4	99.95	66.66	100	80
3	C6288-T099	4527	1	0	7	99.97	100	87.5	93.33
4	C6288-T200	4526	2	1	12	99.93	92.31	85.71	88.88
5	C6288-T206	4526	2	0	11	99.95	100	84.61	91.66
6	C1908-T75	804	1	1	8	99.63	88.88	88.88	88.88
7	S13207-T601	8652	2	3	23	99.94	88.46	92.0	90.2
8	S13207-T214	8653	0	1	12	99.98	92.31	100	96
9	S820-T606	314	1	2	18	99.10	95	94.7	94.8
10	RS232-T1000	280	3	0	36	99.06	100	92.3	95.9
11	RS232-T1200	288	1	4	30	98.4	88.2	96.7	92.2

Table 3 Comparison with existing methods

Method	Accuracy	Precision	Recall	F-measure
Hasegawa [7, 8]	82	92.2	85	74.6
Wang [9]	96	NA	88	NA
Existing spare AE	99.3	91	76.9	83.4
Ours	99.6	92.94	90.5	90.9

values from matrix, there are four more indices for the evaluation of classification results: Accuracy, Recall, Precision, and F-score. Accuracy is the ratio of number of the correct classified nets to the number of the total nets. Recall is same as TPR, which is the ratio of number of the correctly classified trojan nets to the number of the total actual trojan nets. Precision is the ratio of number of the correctly classified trojan nets to the number of the total predicted trojan nets. F-score is harmonic mean of two fractions.

Comparison of the experiment results with existing methods is tabulated in Table 3. It is observed that an average 99% accuracy is obtained for the test circuits. It also achieved 92% precision, which is comparable to reference papers. Most of benchmark circuits realize 90% of recall and F-measures, which inferred that most of trojan nets of test circuits are correctly classified to be trojan nets. Since F-score gives a way for combining the precision and recall into single measure that apprehends both properties, which is good metric for binary classification model evaluation, where imbalance class distribution exists.

When comparing our results with existing sparse autoencoder model without preprocessing data, accuracy and precision results are comparable. But model fails to get good results for recall and f-measure. So, even it tries to minimize the error in reproducing the input by restricting number of vector for reconstruction, the application GAN for preprocessing data on SAE model has considerable impact on getting improved results. Results promising improvements in HT detection using DL over ML techniques. Further, work has to be done to improve F-score and to get good specificity.

5 Conclusion

In this work, 28 features from GLN are used in DL model for the HT detection. A novel preprocessing of dataset with GAN had been used prior to training of classification model, which improved experimental results with an average accuracy of 99%, recall, and F-score of 90% than the existing state-of-the-art method. Our technique is generic so that it can be applied to various test circuits. From performance results, it has been observed that F-score and recall to be improved. So as a future scope, adopting new DL methods to be executed for improvement of individual test circuit's F-score and recall.

References

1. V. Maruthi, K. Balamurugan, N. Mohankumar, Hardware trojan detection using power signal foot prints in frequency domain. in *2020 International Conference on Communication and Signal Processing* (ICCSP) 2020 Jul 28. (IEEE, 2021), pp. 1212–1216
2. S. Bhasin, F. Regazzoni, A survey on hardware trojan detection techniques. in *2015 IEEE International Symposium on Circuits and Systems* (ISCAS) 2015 May 24. (IEEE, 2015), pp. 2021–2024
3. N. Kailash et al., An approach to detect and classify defects in cantilever beams using dynamic mode decomposition and machine learning. in *Intelligent Manufacturing and Energy Sustainability* (Springer, Singapore, 2020). pp. 731–738
4. R. Vishnupriya, M. Nirmala Devi, Hardware trojan detection using deep learning-deep stacked auto encoder. in *Proceedings of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications*. (Springer, Singapore, 2021)
5. K.G. Liakos et al., Machine learning for hardware trojan detection: a review. in *2019 Panhellenic Conference on Electronics Telecommunications* (PACET). (IEEE, 2019)
6. H. Zhao et al., A survey on machine learning against hardware trojan attacks: Recent advances and challenges. IEEE Access **8**, 10796–10826 (2020)
7. H. Kento, M. Yanagisawa, N. Togawa, Hardware Trojans classification for gate-level netlists using multi-layer neural networks. in *2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design* (IOLTS). (IEEE, 2017), pp. 227–232
8. H. Kento, M. Yanagisawa, N. Togawa, Trojan-feature extraction at gate-level netlists and its application to hardware-Trojan detection using random forest classifier. in *2017 IEEE International Symposium on Circuits and Systems* (ISCAS). (IEEE, 2017)
9. W. Yuze et al., Ensemble-learning-based hardware Trojans detection method by detecting the trigger nets. in *2019 IEEE International Symposium on Circuits and Systems* (ISCAS). (IEEE, 2019)
10. K. Reshma, M. Priyatharishini, M. Nirmala Devi, Hardware Trojan detection using deep learning technique. in *Soft Computing and Signal Processing*. (Springer, Singapore, 2019), pp. 671–680
11. K. Wang, H. Zheng, A. Louri, TSA-NoC: Learning-based threat detection and mitigation for secure network-on-chip architecture. IEEE Micro **40**(5), 56–63 (2020)
12. A. Md Zahangir et al., A state-of-the-art survey on deep learning theory andarchitectures. Electronics **8.3**, 292 (2019)
13. M. Wentao et al., Imbalanced fault diagnosis of rolling bearing based on generative adversarial network: a comparative study. IEEE Access **7**, 9515–9530 (2019)
14. L. Han et al., Unsupervised fault diagnosis of rolling bearings using a deep neural network based on generative adversarial networks. Neurocomputing **315**, 412–424 (2018)
15. T. Bendong et al., A deep imbalanced learning framework for transient stability assessment of power system. IEEE Access **7**, 81759–81769 (2019)
16. C. Jonathan et al., An automated configurable Trojan insertion framework for dynamic trust benchmarks. in *2018 Design, Automation Test in Europe Conference Exhibition* (DATE). (IEEE, 2018)
17. Trust-HUB Homepage. http://www.trust-hub.org

Automatic Credit Fraud Detection Using Ensemble Model



S. Srinidhi, K. Sowmya, and S. Karthika

Abstract As dependency on credit cards and online transactions is increasing, the scope for unauthorized payments or fraudulent transactions is on the rise. Huge financial losses are borne by banks every year due to fraudulent transactions. The process of identifying such transactions among millions of transaction records can be perfected using machine learning models, even more so by ensembling them. This study takes a real-time financial dataset and analyzes the efficiency of various machine learning models in predicting fraudulent transactions. Individual ML models are also analysed, ensembled and tested on the dataset. Upon extensive analysis and research, it is concluded that an ensembled model of LightGBM, decision tree classifier and XGBoost gave the highest AuC score of 87%. Further, a user-interactive tool is also created, which predicts fraudulent transactions from real-time transactions. The tool makes use of the model with highest prediction efficiency and presents it in an interactive manner. This study and practical demonstration show advancement in prediction of fraudulent transactions when compared to existing ML models and its user-friendly software incorporation.

Keywords Fraud detection · Ensemble · Accuracy · Fraudulent transaction · Banking · Machine learning model

1 Introduction

Credit card transactions have significantly contributed to simplifying our financial lifestyle. Apart from easy credit, credit cards also offer efficient tracking of expenditures, which can be used for personal monitoring, or professionally for reimbursement

S. Srinidhi (✉) · K. Sowmya · S. Karthika
Department of Information Technology, SSN College of Engineering, Chennai, Tamil Nadu, India
e-mail: srinidhis17112@it.ssn.edu.in

K. Sowmya
e-mail: sowmyak17108@it.ssn.edu.in

S. Karthika
e-mail: skarthika@ssn.edu.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_20

or taxation [21]. But, along with the undeniable advantages come the significant risks which must be closely monitored. Risk of fraudulent transactions is one where unauthorized transactions can be made using the credit card in the event that the card is lost or through other illegal means [21]. With the exponential rise of e-commerce during the course of the recent years, the cases of fraudulent transactions are also soaring. Significant financial losses have been recorded annually due to this problem [6]. Mitigation of such losses involves identifying the fraudulent transactions among millions of other transactions with utmost accuracy, something which is out of human scope.

Advancements in machine learning and artificial intelligence have opened up many opportunities in the finance sector. Significant strides have been made in the field of transaction security, risk management, algorithmic trading and improving customer services [7]. Machine learning models inherently have the ability to identify patterns in large amounts of data which can seem insignificant to the human eye. Thus, using machine learning to monitor the ever-rising stream of transactions can be one of the possible solutions to overcome the problem of financial fraud.

The need to mitigate fraud is turning into a global concern and thus, priority must be given to refining the fraud detection systems. These systems will support the monetary institutions in providing its customers with better financial experience.

2 Existing Works

Fraudulent transactions with credit cards take place in two ways, either card-present fraud or a card-not-present fraud. The high chance of detecting these types of frauds is to identify unusual transactions from the user [21]. Losses due to such fraudulent transactions have reached upto $28.65 billion dollars worldwide [16]. Due to the largeness of the transaction data, it isn't feasible to identify the transactions manually, so patterns must be found in the transaction data to enable automatic detection. Due to continuous technological advancements in both data and processing, machine learning can now be successfully applied to a wide range of important problems such as speech recognition, Natural Language Processing (NLP), bioinformatics, stock market analysis, financial decision making, the set of potential applications seem to be endless [18].

In [12], the author analysed the patterns involved in credit card frauds and reviewed the classical solutions to identify fraudulent transactions. In [2], the author developed a risk scoring system in order to identify fraudulent transactions using random forest classification, logistic regression and support vector machines, out of which random forest classification gave the best prediction. The authors of [1] have created a Hidden Markov Model to identify Credit Card fraud and have used the card holder's profile to do so. An accuracy of 80% was achieved. In [11], a fraud detection model using Bayesian networks has been created yielding an ROC score of 68%. In [5], Clustering has been used to create to identify credit card fraud. This algorithm clusters the customer behaviour and accordingly separates fraudulent and non-fraudulent

transactions. The authors of [22] integrated K Means clustering along with AdaBoost and SVM to create a fraud detection model.

Recent studies have shown in-depth analysis on the machine learning models used, especially by combining them into an ensemble. In [24], Fraud detection Classifier is built using a bagging classifier based on Decision Tree, which resulted in MCC value of around 75%. The authors of [4] have conducted a comparative study between a hybrid ensemble and a Deep Learning approach on real-time transactional data. Their study concluded the better performance of the Deep Learning Model.

3 Proposed System Design

In this section, the overall design of the system is discussed. The workflow is introduced and is briefly explained. The workflow consists of Data collection and preprocessing, Data Analysis and Development of User Interface phases (Fig. 1).

The dataset required for the creating a model is one of financial transactions made through a credit card along with details of the transaction such as the age and gender of the owner, the amount transferred, etc. This dataset is split into a train set and a test set to train different models and test their performance on the test set. In the Data Analysis phase, each machine learning model is trained with the train set and its AuC score and other metrics are observed when tested with the test set. A User Interface (UI) is developed to allow user-friendly interaction to the most promising

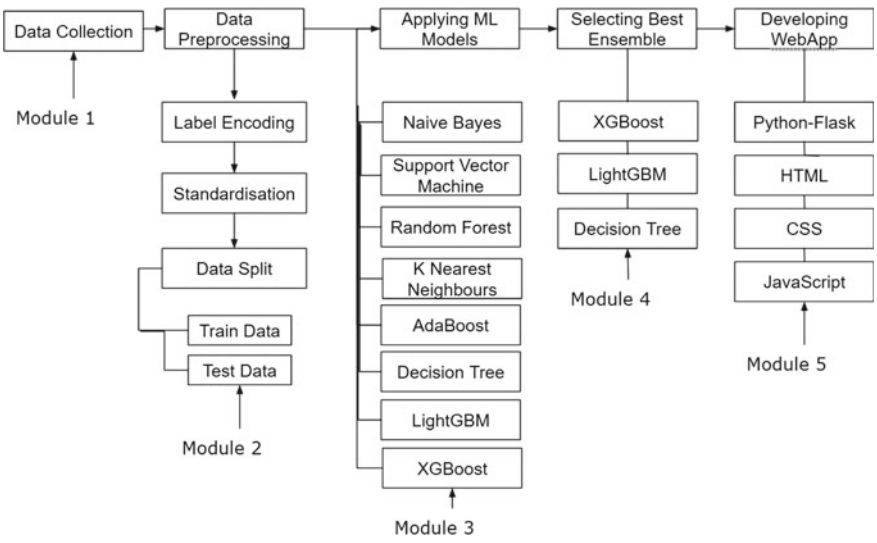


Fig. 1 System workflow design

ensemble using the tool Flask. The data statistics are also shown to the user and convey pictorial information regarding the transaction file uploaded.

4 Data Preprocessing

The dataset required to identify fraudulent transactions is expected to be a large number of transaction details made by credit cards. Each transaction is expected to have identifying features such as transaction number, credit card details and descriptive features of the card owner such as age, gender, state, etc. Such a dataset is hard to obtain due to privacy and ethical policies of financial institutions. In this study, a dataset is collected from Kaggle published by a user named karthik2112. It has legitimate and fraud transactions from the duration 1st Jan 2019–31st Dec 2020. The legitimacy and authenticity of the data are guaranteed by the forum and were found suitable for the nature of this study.

The dataset contains a total of 23 features whose details are index—Unique Identifier for each transaction in the dataset, trans_date_trans_time—Transaction DateTime, cc_num—Credit Card Number through which transaction is done, merchant—Merchant Name, category—Category of Merchant, amt—Amount Transacted through the credit card, first—First Name of Credit Card Holder, last—Last Name of Credit Card Holder, gender—Gender of Credit Card Holder, street—Street Address of Credit Card Holder, city—City of Credit Card Holder, state—State of Credit Card Holder, zip—Zip of Credit Card Holder, lat—Latitude Location of Credit Card Holder, long—Longitude Location of Credit Card Holder,city_pop—Credit Card Holder's City Population, job—Job of Credit Card Holder, dob—Date of Birth of Credit Card Holder, trans_num—Transaction Number, unix_time—UNIX Time of transaction, merch_lat—Latitude Location of Merchant, merch_long—Longitude Location of Merchant and is_fraud—Fraud Flag which is the target class.

There are a total of 18, 52, 365 records in the dataset out of which 12, 96, 675 records are considered as the train set and 5, 55, 689 records as the test set. Each of the features is examined and is transformed into a format required by the study. The preprocessing and analysis are explained in the subsequent sections [9]. Correlation is used to find the linear relationship between the variables. The merchant longitude and longitude of the credit card user in the data are negatively correlated to the zip. Since the features category, state, job and gender are labelled data, they are label encoded [8]. Features like amount, latitude, longitude, city_pop, time, merchant latitude, merchant longitude, transaction date and age are standardized [10] to minimize the effect of a variable on the predictions of the models [17].

5 Data Analysis

Ensembling is basically combining multiple learners. These learners can be from the same machine learning model or different. Sometimes, it is not a good idea to rely on the performance of a single model. Combining results of different models gives better results [3]. Since, the priority to classify a record as fraudulent is more, if any model participating in the ensemble predicts a particular record as fraudulent, it is considered as fraudulent.

Random forest classifier is one of the bagging models. For this model, the max_depth variable is set to 2 to avoid high bias condition[15]. Adaboost classification works in iterations. In each subsequent iteration, the model tries to learn incorrectly classified records better. n_estimators of 10 have perfect fitting to this model [19]. Naive Bayes Classifier uses Bayes' theorem which considers independence among the predictors. Sometimes it outperforms many sophisticated models even though its working is simple [9]. SVM is a simple classification algorithm. It strives to find the best hyperplane which helps to separate classes in space. 'Sigmoid' type of kernel is used in the presented model [14]. KNN classifier chooses the number of neighbours k, whose default value is 5. It takes the k nearest data points of the new datapoint, according to the Euclid distance, counts the number of points in each category and assigns the new data point to the category whose count is more [23]. Decision tree classifier algorithm works by selecting the most appropriate attribute to split the data and expands the leaf nodes of the tree until the stopping criterion is satisfied. The entropy criterion is used to split nodes in the tree formation and a max_depth of 10 is also applied to the model [20].

XGBoost is designed to work with large and complicated datasets. For the XGBoost model, the value of learning_rate is set to 0.01 and the total number of trees was 100. The alpha value was set to 0 since the dimensions used here were not more. Further, min_child_weight was 1 to avoid model learning from highly specific relations as higher values of this parameter tend to increase this case. Similarly, the max_depth parameter of the XGBoost model was set to 5 to hinder overfitting of the model by learning more with higher depths, which in turn performs less effectively on the unseen data. The model used the gain importance metric to decide node splits for the tree estimator, and the objective was set to binary logistic regression. The binary logistic regression returns the predicted probability and records whose probability is greater than 0.5 are considered as fraudulent records. Similarly, records with predicted probability less than 0.5 were predicted as non-fraudulent records. XGBoost model helps to decrease the chances of overfitting of the model.

LightGBM framework uses a leaf-wise tree growth algorithm, not the level-wise tree algorithm, and the tree is not balanced. To avoid overfitting, we can increase the path_smooth value for larger training sets, regularization of min_gain_to_split, and by avoiding growing of a very deep tree. LightGBM works well on categorical features that are not one-hot encoded [13]. Logloss objective function is used for binary classification. 'n_estimator' defines the number of boosted trees to fit which defaults to 200,000. LightGBM boosting type is set to goss. Goss is the newer

and lighter version of gradient boosting which avoids overfitting. In this model, the max_depth parameter is set to 10. To avoid overfitting, values higher than 10 are not selected. The objective of this model is set to binary since the model needs to classify between two categories. The goss boosting type is used in the model, as it is a better version of the gradient boosting algorithm.

6 User Interface

The three main phases in the User Interface are as follows: input collection and validation, classification and output presentation and Statistics.

Input and Validation: The input from the user is taken in the form of a Comma Separated Values (CSV) File. The user is expected to give the data with certain column names such as transaction number, date of transaction, location of customer and merchant, amount, etc. The columns in the input file are validated with the expected columns and an error message is given if required.

Classification and Output: The validated data file is transferred into a dataframe and is sent to the special prediction function made with the earlier discussed ensemble model. The dataframe is first label encoded and standardized before the prediction. After the prediction, a new dataframe of fraudulent records is created and is displayed on a web page through HTML tables.

Statistics: The statistics page of the UI is a pictorial representation of the relationships between the number of instances of fraudulent records predicted and the major features the ensemble model is learning from. The ensemble model makes the maximum predictions using the features age, gender, occupation, amount and category. These relations are shown in the form of pie plots, line plots and bar graphs and are displayed on the front end as images. These plots give the user a clear idea as to which and in what magnitude the features are affecting the predictions. The user will also be able to identify trends in the data for taking appropriate decisions.

7 Results and Discussion

Upon training the dataset using different machine learning models, each model was evaluated using certain quantitative metrics, so that the best performing models could be combined to form an ensemble. This ensemble model was included in a user interface so that qualitative inferences could be made through the statistical analysis of the data tested.

7.1 Comparative Analysis

The dataset is trained and tested using different machine learning techniques and was quantitatively evaluated using different metrics (Table 1).

In the Naïve Bayes classifier, the AuC score of 0.69366 is obtained that is because, out of 2115 fraudulent records only 827 records are correctly classified. Since this model considers each feature as an independent feature, results from the combined features are not learned. Both the support vector machine and random forest classifier models are not able to learn the presence of fraudulent records. That might be because of the presence of very few fraudulent records and the models were not able to learn significant differences out of them. The K-Nearest Neighbour model gave an accuracy score of 0.99477 and an AuC of 0.50399. With the neighbour count as 5, the model is only able to classify 20 records as fraudulent records and failed to classify 2095 records as fraudulent. Here also data imbalance would be the cause of failure. The Adaboost model is a boosting algorithm and it gives more importance to the weaker class. That is why this model is able to classify 248 records as fraudulent records. The misclassification of the non-fraudulent records is also less.

As the name suggests, XGBoost is an extreme gradient boosting algorithm which gives more importance to the weaker class than the Adaboost model. It outperforms the Adaboost model with an AuC score of 0.73573 and an accuracy of 0.99760. The LightGBM model is a lighter version of XGBoost model where the learning is leaf-based rather than level based, which allows faster learning with less computational power. Having said that, there is an increase in the correct classification of fraudulent records from 998 to 1158 when compared to the previous model. This also led to the rise in the AuC score from 0.73573 to 0.77194. Decision tree classifier with entropy criterion and a depth of 10 is one of the best models. The model was able to classify two-thirds of the fraudulent records correctly with an AuC score of 0.84668, which is the highest AuC score of individual models. But the problem with this model is that it has more misclassifications in non-fraudulent records, which is not good.

Table 1 Comparative analysis of ML models

Model name	Accuracy	AUC Score
Naive bayes classifier	0.99401	0.69366
Support vector machine	0.99619	0.5
Random forest classifier	0.99619	0.5
K-Nearest neighbour	0.99477	0.50399
Adaboost classifier	0.9956	0.5581
XGBoost classifier	0.99760	0.73573
LightGBM	0.99466	0.77194
Decision tree classifier	0.99764	0.84668
XGBoost + Dcision Tree + LightGBM	0.99574	0.87657

The above observations have led to the formulation of an ensembled model of XGBoost, decision tree classifier, LightGBM to add the advantage of all these models, creating a model with fewer faults and resulted in an improvement of 3% of AuC score when compared to decision tree whose AuC is 84%. In the ensembled model, even if a single model predicts a given record as fraudulent, the record is classified as a fraudulent record.

7.2 Ensemble Learning Analysis

The ensemble with the best prediction is created using XGBoost, LightGBM and decision tree classifier. Each of these models is further analysed individually to find the most prominent features responsible for classification.

The plot in Fig. 2 represents the role of different features in the learning of the XGBoost model. As observed, the features representing amount, category of transaction, gender of the card owner, age of the card owner and date of transaction are the top 5 features that influence the classification of a transaction when trained with the XGBoost model.

The plot in Fig. 3 represents the role of different features in the learning of the decision tree classifier model. As observed, the features representing amount, category of transaction and age of the cardholder influence the classification the most, when trained with decision tree classifier. Unlike the XGBoost model, the gender of the cardholder doesn't play as important a role in the Decision Tree Classification model. The decision tree classifier makes prominent use of only a few features while other features have negligible influence on the classification. This is dissimilar to

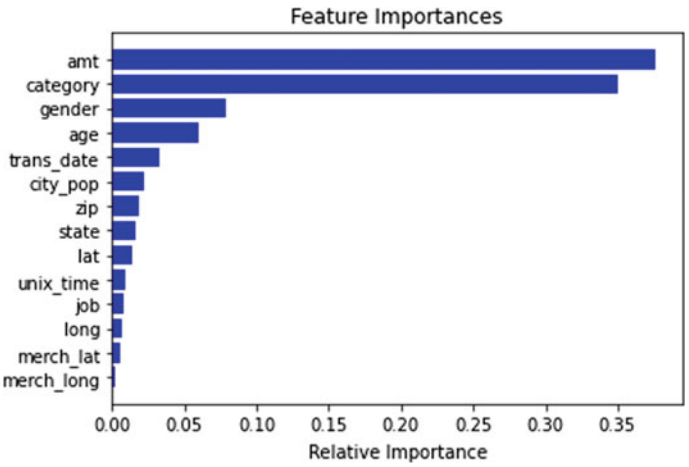


Fig. 2 XGBoost feature importance plot

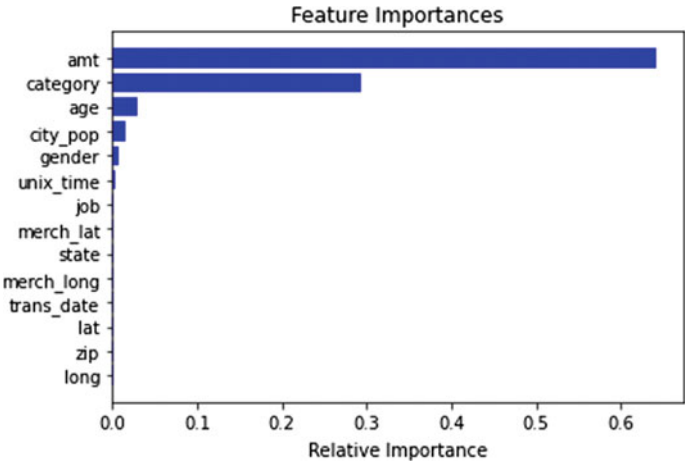


Fig. 3 Decision tree classifier feature importance plot

other models selected for the ensemble as the minor features also have considerable influence on the classification of the transaction.

The plot in Fig. 4 represents the role of different features in the learning of the LightGBM model. As observed, the features representing amount, category of transaction and age of the cardholder influence the classification the most, when trained with LightGBM algorithm. Unlike other models in the ensemble, classifications in LightGBM model are also influenced by features representing city population and unix time.

From the above feature importance plots, it is seen that the XGBoost model learns prominently from the features amount, category, gender, age and transaction date, Decision Tree model from amount, category, age and city_population and LightGBM learns from amount, category, city population and time. Ensemble of these 3 models results in overlap of similar features and addition of the unique learnable features. So, the ensemble of all these models leads to better learning from features transaction date, city_population, time and amount, which leads to better classification.

7.3 Prediction Analysis

For a given dataset, once the potential fraudulent transactions are predicted, statistical evaluations are performed and appropriate qualitative inferences are drawn from the data.

From the pie chart in Fig. 5, it is clear that the age groups 20–30 and 40–59 are more vulnerable to fraud. Inferences regarding causes of fraud in this age group can be derived upon further analysis. An example of an inference can be that people in

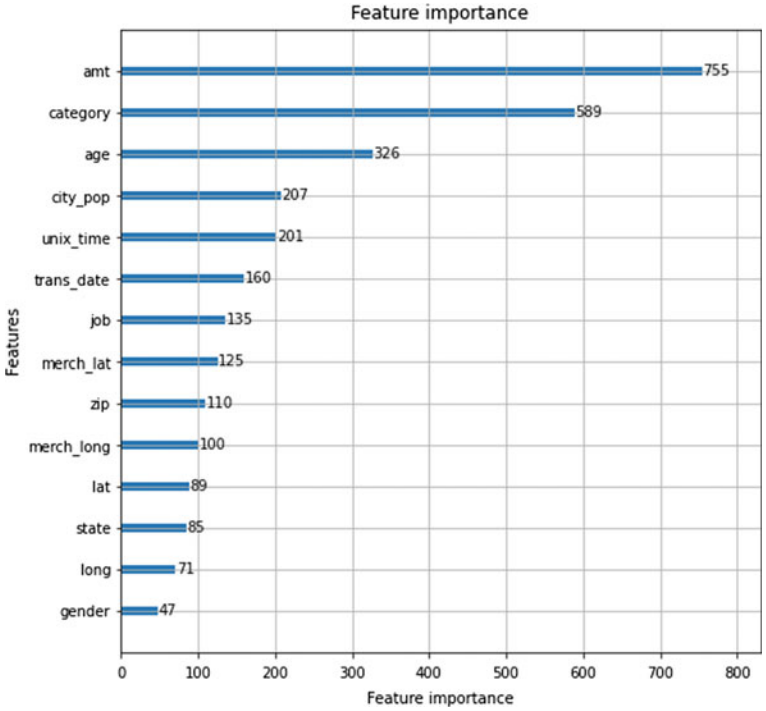


Fig. 4 LightGBM feature importance plot

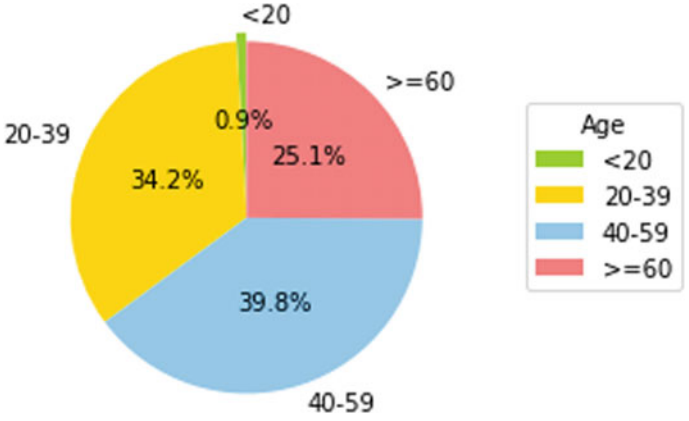


Fig. 5 Age pie chart

these age groups have maximum card usage and that people in their early twenties or late fifties might not be vigilant to the idea of fraud.

The pie plot in Fig. 6 is a representation of the gender of the victims of credit card fraud. It is observed that, in the examined dataset. more than half of the credit fraud victims are women. Inferences can be drawn that women are more susceptible to fraud due to lack of vigilance, or lack of awareness of methods to deal with such situations immediately.

The plot in Fig. 7 shows the comparative analysis of different merchants in the predicted fraudulent records. It is observed that grocery outlets and entertainment zones are major places where fraud takes place. Causal inferences can be drawn, such

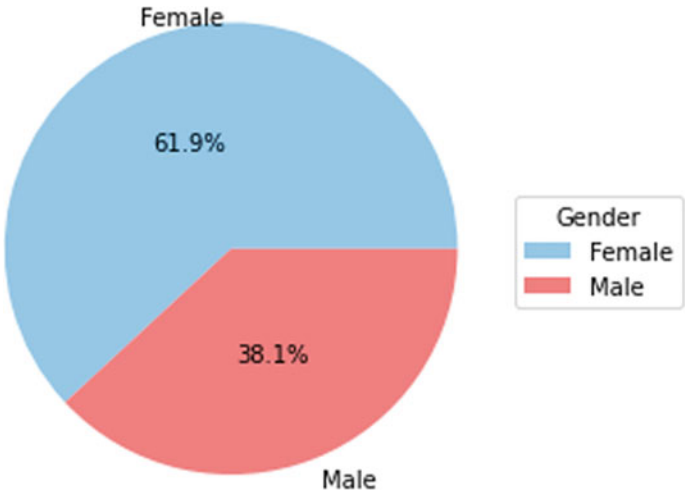


Fig. 6 Gender pie chart

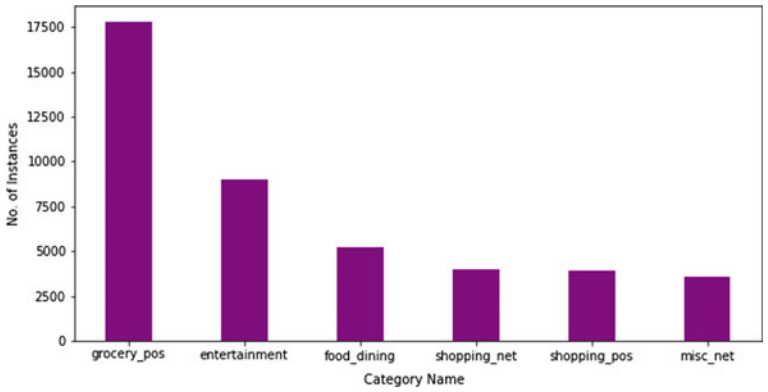


Fig. 7 Merchant versus no of instances bar chart

as people making transactions at grocery stores wouldn't really notice the details of the transaction as usually multiple items are bought at such places.

The line plot shown in Fig. 8 is a comparative analysis between the instances of fraud with respect to the amount lost in a transaction. It is observed that small amount fraud transactions are more than high amount transactions. Inferences of cause can be drawn such as, people tend to consider transactions with small amounts as trivial and overlook them, and multiple small amount fraud transactions help fraudsters launder more money.

The plot in Fig. 9 shows the top six professions of people who are highly vulnerable to fraud. From the dataset tested with the ensemble model, it can be observed that scientists are most vulnerable to credit card fraud followed by environmental consultants. These observations can be used to draw meaningful inferences regarding

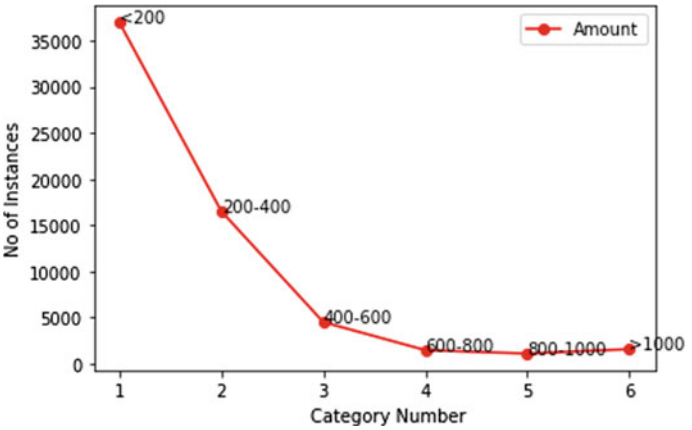


Fig. 8 Amount versus number of instances plot

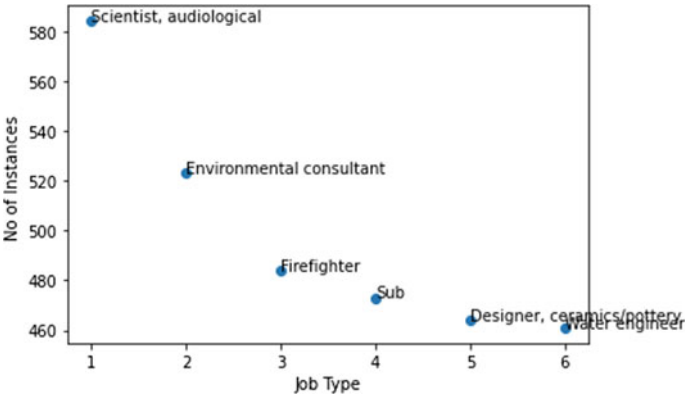


Fig. 9 Occupation versus number of instances scatter plot

the causes. An example of a psychological inference can be that scientists are more vulnerable to credit fraud as they are known to be well immersed in their field of study, little bothered to monitor their financial flow.

8 Conclusion and Future Scope

The exponential increase in losses due to fraudulent transactions is a major cause of concern. Combating these losses through machine learning models is the way to go. Further, identification of fraudulent transactions can be enhanced with the use of ensembling machine learning models. This study takes up a financial transaction dataset of approximately 15 lakh records and analyses the performance of individual ML models, ensembled ML models. After extensive analysis, it was observed that an ensemble of LightGBM, decision tree classifier and XGBoost models gave the highest prediction efficiency of 87%. This ensemble was then incorporated into an interactive tool that predicts potential fraudulent transactions from large size transaction data. The tool also gives pictorial representations of the analyses made from the data and the deciding features that lead to classification of a record.

This study thus makes a substantial contribution in enhancing the quality of credit card fraud detection systems. This tool can be further enhanced by implementing security measures for the financial data and can be scaled up by allocating larger resources for processing and testing. Inclusion in real-time banking applications can also be made feasible with appropriate measures. In culmination, it can be said that even a small step towards improving fraudulent transaction detection can contribute to saving lots of financial losses of the banks and customers.

References

1. A. Srivastava, A. Kundu, S. Sural, A. Majumdar, Credit card fraud detection using hidden markov model. IEEE Trans. Dependable Secur. Comput. **5**(1), 37–48 (2008). https://doi.org/10.1109/TDSC.2007.70228
2. C. Nuno, F. Gonçalo, C. Miguel, A data mining based system for credit-card fraud detection in e-tail. Decision Support Syst **95**, 91–101 (2017). https://doi.org/10.1016/j.dss.2017.01.002
3. T.G. Dietterich, Ensemble learning. In: The Handbook of Brain Theory and Neural Networks. vol. 2 (2002), pp. 110–125
4. E. Kim, J. Lee, H. Shin, H. Yang, S. Cho, S.-K. Nam, Y. Song, J.-a Yoon, J.-i Kim, Champion-challenger analysis for credit card fraud detection: hybrid ensemble and deep learning. Expert Syst. Appl. (2019). https://doi.org/10.1016/j.eswa.2019.03.042
5. H. Mohamed, A. Madian, M. Ragaie, Enhanced fraud miner: credit card fraud detection using clustering data mining techniques. Egypt. Comput. Sci. J. **40**(03) (2016) (ISSN: 1110–2586)
6. https://www.paymentscardsandmobile.com/card-fraud-losses-hit-21-84-billion-2015-20-/
7. https://marutitech.com/ai-and-ml-in-finance/#:~:text=Secure%20Transactions,precision%20of%20real%2Dtime%20approvals
8. https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.LabelEncoder.html
9. https://www.analyticsvidhya.com/blog/2017/09/naive-bayes-explained

10. https://towardsdatascience.com/normalization-vs-standardization-quantitative-analysis-a91e8a79cebf
11. J.J. Hopfield, Artificial neural networks. IEEE Circuits Devices Mag. **4**(5), 3–10 (1988)
12. S. Jha, J.C. Westland, A descriptive study of credit card fraud pattern. Glob. Bus. Rev. **14**(3), 373–384 (2013). https://doi.org/10.1177/0972150913494713
13. G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, T.-Y. Liu, Lightgbm: a highly efficient gradient boosting decision tree. Adv. Neural. Inf. Process. Syst. **30**, 3146–3154 (2017)
14. S.S. Keerthi, S.K. Shevade, C. Bhattacharyya, K.R.K. Murthy, A fast iterative nearest point algorithm for support vector machine classifier design. IEEE Trans. Neural Netw. **11**(1), 124–136 (2000)
15. A. Liaw, M. Wiener, Classification and regression by randomForest. R news **2**(3), 18–22 (2002)
16. NathanielLee. https://www.cnbc.com/2021/01/27/credit-card-fraud-is-on-the-rise-due-to-covid-pandemic.html#:~:text=Payment%20card%20fraud%20losses%20reached,prone%20country%20in%20the%20world
17. P. Andy, S. Mostaghim, A. Nazemi, Heatmap visualization of population based multi objective algorithms. in *International Conference on Evolutionary Multi-Criterion Optimization.* (Springer, Berlin, Heidelberg, 2007), pp. 361–375
18. S. Mark, in *Introduction to Machine Learning with Applications in Information Security*. (CRC Press, 2017)
19. R.E. Schapire, Explaining adaboost. in *Empirical Inference* (Springer, Berlin, Heidelberg, 2013), pp. 37–52
20. B. Thangaparvathi, D. Anandhavalli, S. Mercy Shalinie, A high speed decision tree classifier algorithm for huge dataset. in *2011 International Conference on Recent Trends in Information Technology* (ICRTIT) (IEEE, 2011), pp. 695–700
21. Wikipedia contributors, Credit card fraud,. Wikipedia, The Free Encyclopedia (2021). https://en.wikipedia.org/w/index.php?title=Credit_card_fraud&oldid=1011991333 Accessed April 1 2021
22. W. Chunhua, H. Dong, Credit card fraud forecasting model based on clustering analysis and integrated support vector machine. Cluster Computing (2018). https://doi.org/10.1007/s10586-018-2118-y
23. Y. Halil, A weighting approach for KNN classifier. in *2013 International Conference on Electronics, Computer and Computation* (ICECCO), (IEEE, 2013), pp. 228–231
24. M. Zareapoor, P. Shamsolmoali, Application of credit card fraud detection: based on bagging ensemble classifier. Proc. Comput. Sci. **48**(2015), 679–685 (2015)

Blockchain in Education Sector – Boon or Curse



Pratyush Jha, Yug Chandak, and Aman Gupta

Abstract Analysts and professionals keep on drawing fluctuated interests in blockchain (BC) technology. The idea has- some key highlights, for example, decentralization, dependability, security, and information veracity. In any case, even with the developing interest, much more has to be done concerning the current state of knowledge and practice in relation to the use of BC technology in education. Accordingly, this study presents a review of the current investigations on BC-based learning applications in the education sector. This paper has focused on three major themes: learning applications that have been made using BC technology, the contribution and merits of blockchain technology to the education sector, and the problems experienced while integrating BC technology in the education sector. A concentrated conversation is introduced as well as a complete outcome examination of each topic. This paper also highlights the key areas of the education sector which tend to benefit from the application of Blockchain technology.

Keywords Blockchain technology · Development · Education sector

1 Introduction

The deployment of blockchain technology in the education sector is as yet in the underlying stages. Right now, educational institutions utilizing this technology are very less in number. Most of the institution uses blockchain as a safe stage for approving and sharing individual students' information and academic certificates. Ongoing examinations propose online identity confirmation systems that utilize the blockchain to execute cloud education cooperation. As of now, blockchain technology is being used to give verification of information/content validness accordingly keeping up the system's reliability. For the growth of the BC-based applications in education, a few case studies have been directed at Chou College in Japan. Besides, BC ledgers and cloud computing are additionally being utilized to upgrade software engineering education. A decentralized P2P cloud model is recommended utilizing

P. Jha (✉) · Y. Chandak · A. Gupta
Marwadi University, Rajkot-Morbi Road, Gauridad, Rajkot, Gujarat 360003, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_21

Bitcoin and Torrent models to support proof of concept platforms to help education providers.

2 Background

In the year 2008, Blockchain was first introduced as an emerging technology by Satoshi Nakamoto. The main work of Blockchain was the enrolment of transactions of the bitcoin cryptocurrency as a peer-to-peer ledger. The tool would help encourage direct transactions along hence eliminating third-party intermediaries. For the objective to be understood, the design of blockchain was with the end goal that it included a decentralized network of peer nodes. A duplicate of the transaction's ledger is stored in every node of the network. Every node is additionally entrusted with the capacity of writing an entry to its ledger, after approval from other network nodes, communicating any transactions made by its user to other network nodes, and ensuring that the ledger it holds is the equivalent as the ones across the network consistently.

As the popularity of Bitcoin keeps on expanding, experts and specialists keep on revealing the capability of this technology. Blockchain's extraordinary capacities like trustworthiness, immutability, and precision have been important in cryptocurrencies as well as likewise, in a wide range of fields like education. Researchers accept that technology has a lot to offer in the education sector that might change the world.

3 Discussion

3.1 Educational Applications Developed with Blockchain Technology

Even though few blockchain-based applications are accessible for use in the education sector, very few of these are accessible to the public. As [1] describes, a portion of the applications related to certificates management. These sorts of applications handle all types of scholastic academic credentials, students, transcripts, students' certificates, and any other form of achievement certificate. Most applications depend on blockchain technology for the issuance of digital certificates. Moreover, some of the applications that issue these credentials have depended on the increased trust level and the privacy assurance of BC technology.

Utilizing the blockchain, we will avail a means through which employers or education providers will give official certificates with significant data security. This could empower students to share their official documents straightforwardly with anybody upon demand.

Some blockchain applications can be developed to upgrade students' learning objectives and help them to achieve new heights in education. This

would bring advancement in the education sector and improve the learning process. Few applications can be made to assess and measure students' performance utilizing quantitative and subjective elements. For instance, the authors in [2] built up a system to track students' performance for their multi-learning activities.

The utilization of blockchain avails a decentralized organization. The idea makes it feasible for multiple users like students, department members, and authorities to get to it with high security and veracity. They introduced the Ubiquitous learning (U-learning) system which utilizes BC technology to give students an improved learning atmosphere highlighted with an increased security level.

Regarding fees and credit transfer, some blockchain applications with unique qualities for credential records or fee transfer in educational institutions have been created. Ordinarily, educational institutions rely upon intermediaries to deal with and approve credit or fees transfer. Fortunately, because of its high security and trust level, blockchain technology can be utilized as an efficient method of transfer and eliminate the requirement for an intermediary.

3.2 Blockchain Technology Benefits to Education

BC technology has an incredible potential to carry various benefits to education. Some benefits are low cost, increased safety, student enhancement, enhanced data access management, boosting trust, supporting learners, identity authentication, improving students' records efficiency and career decisions. As [3] authors contend, utilizing blockchain ensures safety, data confidentiality, and transaction exchange among the parties involved. Utilizing cryptographic hashes and signatures likewise guarantees transactions' reliability. The best thing about blockchain technology is that it depends on itself for protecting the data and confirming its authentication.

Authors in [4] outline how BC technology assists with bringing down storage costs, transaction associated costs, and the cost of maintaining and managing education records. The costs related to storing data on the cloud can be decreased altogether by utilizing private/public networks accessible from any location. Usually, extra expenses are brought about in processing and verifying academic certificates which could be reduced fundamentally by utilizing blockchain technology which additionally assists with upgrading the student's assessment process. Each block stores information like scores, learning results, students' names, and the course.

Arenas and Fernandez [5] underline the blockchain advantage of controlling and restricting stored records access. The blockchain system utilized in such a manner restricted access to academic credentials by restricting access to specific groups. Hence, only certified institutions could access and change the data stored. Blockchain improves accountability and transparency in the education sector since all educational and school records are stored in one spot where they are effectively accessible.

The legitimacy of digital certificates is very much guaranteed while utilizing blockchain technology since it helps to keep the identity of users confidential. As per [6], a digital syllabus was kept in a BC. After making the book, a private key will

be utilized by authorized parties to sign in. Thus, there is a need to guarantee that the content developed can't be messed with. For this situation, the course syllabus is secured using the cryptographic hash. In this way, the hash and the key availed to every institution are basic parts that confirm that the data is genuine.

3.3 Results

The reviewed journals detailed several benefits that comes with the adoption of blockchain technology in education.

- A majority of applications have been developed with a prior goal of the management of certificates. The sources introduced applications for handling, storing, issuing, and sharing students' scholastic certificates. One detailed application that can be used by organizations to review students' proficient abilities and capacity dependent on their educational performance.
- Security as a significant advantage through improved information enhanced data privacy, protection, and integrity.
- Utilizing blockchain in education to encourage controlled access to students' data.
- Integration of blockchain technology would help acknowledge tremendous cost reduction. The idea of the blockchain can assist with reducing pointless expenses connected to data storage and transactions.
- BC technology can advance the assessment of the student's exhibitions and their learning results.

3.4 Challenges of Integrating Blockchain Technology in Education

Although BC has shown that it has a high potential for patching up the education sector, numerous issues should be considered before arrangement and dynamic use in the field. As indicated by Bandara et al. [7], the technology is exceptionally secure however not immune to malicious attacks. It is difficult to avail a system that is both secure and guarantees users of privacy. The issue is graver when it risks careers by approving academic testimonials and certificates online. To improve confidentiality, various BC systems utilize private and public keys. In any case, the privacy of transactions can't be guaranteed since the information for every one of the public keys is visible to people in general. Therefore, one can link transactions made to a specific user and reveal their information.

Besides, [8] portrays how the immutability feature in blockchain technology is a challenge. This component makes it difficult to make data changes except if all parties offer to agree to change the ledger content. Besides, the immutability characteristic of systems with defined policies makes it difficult for governments to impact changes.

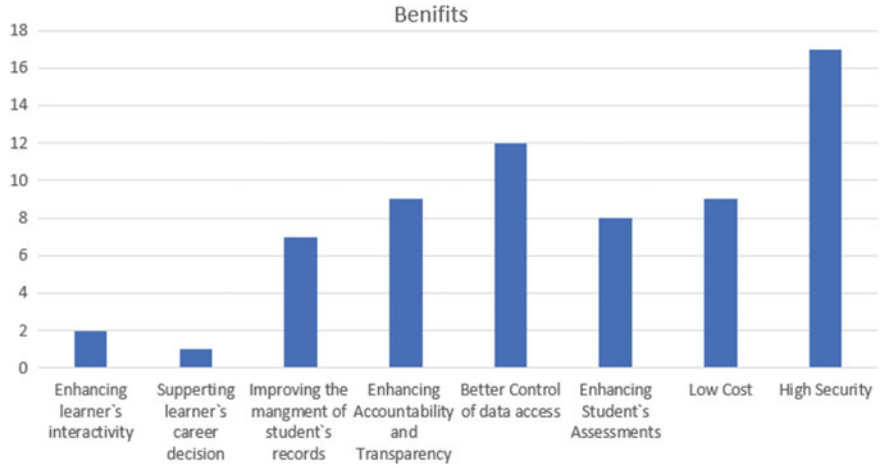


Fig. 1 Benefits of blockchain technology in the education sector

The notion might prompt significantly more serious issues in circumstances where an ex-external examiner or an ex-employee makes an unapproved erase. This is a direct result of the irreversible and immutable nature of such data that limits alterations.

Blockchain technology is decentralized while education systems are centralized. Consequently, adopting the technology would disrupt the system to a large extent. Like in blockchain, having a ledger that aggregates everything can impact the traditional school accreditation's worth. As one of the astounding developments in present-day times, blockchain technology is required to set aside an extensive time of effort for large-scale adoption. This is because of the current difficulties related to technology adoption in the education sector.

3.5 Graphs of Benefits vs Challenges

See Figs. 1 and 2.

4 Conclusion

The integration of BC technology into the education sector is in its developmental stages. The selection criteria for the journals utilized in this paper were applicability, benefits, and challenges. First of all, the review showed that blockchain technology is generally used for issues and verification of academic certificates, assessment of students' professional capacities, and sharing students' skills and academic accomplishments. In any case, various blockchain applications continue to arise every day.

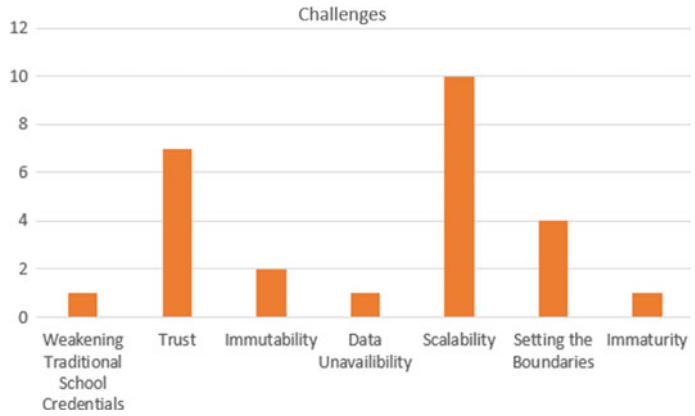


Fig. 2 Challenges faced by blockchain technology in education sector

Secondly, it shows that blockchain has a few advantages that could be acknowledged by fusing blockchain technology in the education sector. These include a secure platform for sharing students' data, improved transparency and reliability, and tremendous expense decreases. Thirdly, the study additionally featured the difficulties like lack of Trust, Immutability, weakening of traditional school accreditation's worth amd a few more that can be faced by educational institutions for the adoption of BC technology in this sector. An educational institution is advised to consider challenges (Fig. 1) associated with many benefits (Fig. 2) like cost, confidentiality, security, scalability, and availability before deciding to adopt the BC technology in the education sector or not. Nonetheless, blockchain technology has much more to bring to the table and there is no uncertainty that it can offer a lot more benefits than it has drawbacks, to all educational sectors worldwide. As BC technology is enhancing day by day there's no doubt it will improvise and will provide much more benefits in the future by overcoming every challenge faced as of now. Hence, we can accept that Blockchain in Education is a Boon to the sector**.**

References

1. J. Nespor, Cyber schooling and the accumulation of school time. Pedagog. Cult. Soc. **27**(3), 325–341 (2018)
2. J.C. Farah, A. Vozniuk, M.J. Rodriguez-Triana, D. Gillet, A blueprint for a blockchain-based architecture to power a distributed network of tamper-evident learning trace repositories. in *2018 IEEE 18th International Conference on Advanced Learning Technologies* (ICALT) (2018)
3. R. Bdiwi, C.D. Runz, S. Faiz, A.A. Cherif, A blockchain-based decentralized platform for ubiquitous learning environment. in *2018 IEEE 18th International Conference on Advanced Learning Technologies* (ICALT) (2018)
4. M. Holbl, A. Kamisalic, M. Turkanovic, M. Kompara, B. Podgorelec, M. Hericko, EduCTX: an ecosystem for managing digital micro-credentials. in *2018 28th EAEEIE Annual Conference (EAEEIE)* (2018)

5. R. Arenas, P. Fernandez, Credence ledger: a permissioned blockchain for verifiable academic credentials. in *2018 IEEE International Conference on Engineering, Technology, and Innovation* (ICE/ITMC) (2018)
6. N. Bore, S. Karumba, J. Mutahi, S.S. Darnell, C. Wayua, K. Weldemariam, Towards blockchain-enabled school information hub. in *Proceedings of the Ninth International Conference on Information and Communication Technologies and Development- ICTD 17* (2017)
7. I. Bandara, F. Ioras, M.P. Arraiza, The emerging trend of blockchain for validating degree apprenticeship certification in cybersecurity education. in *INTED2018 Proceedings* (2018)
8. D. Lizcano, J.A. Lara, B. White, S. Aljawarne, Blockchain- based approach to create a model of trust in open and ubiquitous higher education. J. Comput. Higher Educ. (2019)

Image Feature Generation Using Binary Patterns—LBP, SLBP and GBP



S. Divya, L. Padma Suresh, and Ansamma John

Abstract Image features play pivotal role in digital image processing and computer vision problems. To retrieve image features accurately and effectively, various texture descriptors are needed. This paper presents a comprehensive evaluation of various descriptors such as local binary pattern (LBP), significant local binary pattern (SLBP), gradient binary pattern (GBP) and its effectiveness in plethora of applications such as medical image analysis, object detection and classification. Moreover, the descriptors are validated using brain tumorous magnetic resonance image (MRI).

Keywords Texture · Local binary pattern · Significant local binary pattern · Gradient binary pattern · MRI

1 Introduction

Image processing is a pivotal research domain based on rigorous mathematical foundations which demand solutions that are drew on machine learning practices and problems of content-based image retrieval systems. Most of the methods to texture analysis evaluate texture measures by single values such as mean and variance. These measures are used as elements of feature vectors in further classification model. In this manner, some of the vital information contained in the distributions of the feature values in the input data might be lost. Another popular method, called gray level co-occurrence matrix (GLCM), is an enumeration of how frequent various combinations of intensity levels concur in an image, creating a GLCM and then excerpt statistical measures from this matrix. During the past decade, local binary patterns (LBPs) [1] and gradient binary patterns (GBPs) [2] have knocked up keen interest in medical image processing and computer vision.

S. Divya (✉)
TKM College of Engineering, APJ Abdul Kalam Technological University, Kollam, India

L. P. Suresh
Baselios Mathew II College of Engineering, Sasthamkotta, India

A. John
TKM College of Engineering, Kollam, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_22

The LBP feature is extensively used in object detection, classification and shadowing owing to its low dimension, fast computational capability, rotation and gray level invariance, monotonic illumination variation and its computational simplicity and insensitivity. LBP is a non-parametric texture operator which flags the image pixels as a binary number (LBP binary code) by thresholding the neighborhood of individual pixel. The histogram of these various flags can then be taken as a texture descriptor for further applications.

Because of the inadequacy of LBP feature in object detection, researchers [3] are instigated with an ameliorate LBP feature, entitled significant local binary pattern (SLBP). The SLBP feature can bring down the impact of various artifacts such as noise and inflate the description of noteworthy characteristics of object that has evident dominance in comparison with LBP feature.

Gradient binary pattern (GBP) descriptor [2] describes individual pixel by the relevant gradient values on horizontal, vertical and diagonal directions of the pixel. GBP seizures feature by counting the happenings of gradient orientation. It dissects the image into different cells and determines histogram of gradient orientations over it.

The remainder section of this paper is categorized as follows. Sections 2, 3 and 4 briefly provide an assessment about divergence in binary patterns such as LBP, SLBP and GBP, respectively, to bring out the texture features. Section 5 details the application of these descriptors in medical image domains with standard datasets. Section 6 illustrates visualization of these descriptors over MR input image, and Sect. 7 concludes the paper with the future enhancement.

2 Local Binary Pattern (LBP)

Ojala et al. [1] proposed the initial LBP method to extract local binary patterns in a texture. In the initial two-level version, there are only 258 (2^8) texture units expound in a 3X3 neighborhood of eight pixels threshold by a gray value of center pixel. The LBP code computation process [4] is illustrated in Fig. 1. The intensity value of neighborhood pixel is represented by $a_{i,}$ where i is the number of neighborhood pixels and it varies from 0 to 7. The intensity value of center pixel is depicted as a_c, where c indicates the count of neighborhood pixels, which is 8. The two-level LBP is interpreted as:

$$\mathbf{LBP} = \sum_{i=0}^{i-1} s(a_i - a_c).2^i \tag{1}$$

$$\mathbf{s}(x) = \begin{cases} 0, x < T \\ 1, x \geq T \end{cases} \tag{2}$$

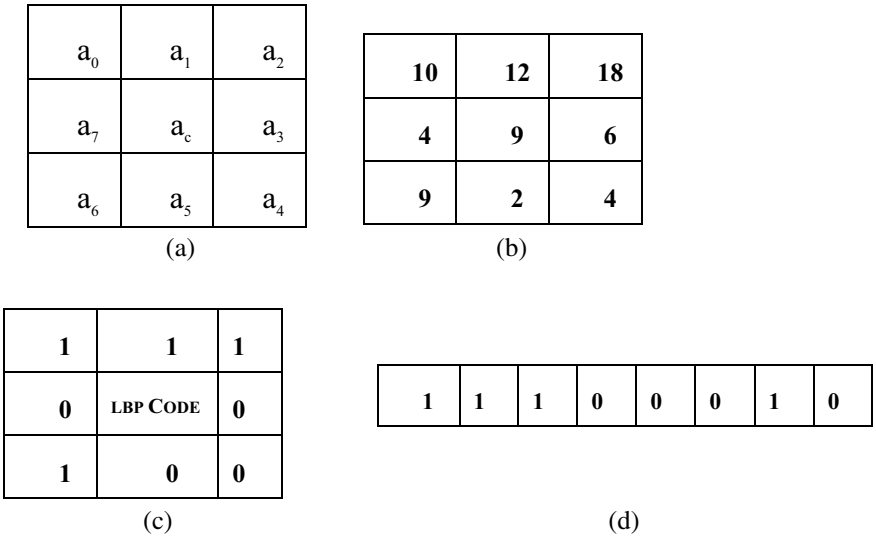


Fig. 1 LBP computation process

where $s(x)$ is a comparison function and T denotes the threshold and its value is set to one.

The main constraint to LBP operator is its small 3×3 neighborhood, which cannot record pre-dominant features in case of large scale and irregular shapes. In addition, LBP feature uses sign feature which illustrates the difference between the center and neighborhood pixels so that it does not account off the difference information between them. Due to this, LBP feature shortfalls the interpretation of significance of the object. In addition, the size of the features increases exponentially with the number of neighborhood values, which leads to an increase in computational intricacy in terms of time and space.

3 Significant Local Binary Pattern (SLBP)

To describe the significance information, an improved LBP descriptor called SLBP descriptor is proposed [3]. SLBP shows the significant characteristics of object locally. According to Weber's law, it is stated that local significant is not analogized with absolute value of the difference threshold, whereas portrayed by its initial value [5].

SLBP is formulated by fusing significant characteristic factor as weight to LBP feature. The significant characteristic factor of the center pixel (a_c) is represented as

$$\mathrm{S}(a_c) = \arctan \sum_{i=0}^{i-1} \frac{a_i - a_c}{a_c} + \frac{\pi}{2} \tag{3}$$

Thus, in order to describe the significance information of an object, SLBP feature is defined as,

$$\chi(a_c) = S(a_c) \sum_{i=0}^{i-1} s(a_i - a_c).2^i \tag{4}$$

4 Gradient Binary Pattern (GBP)

The gradient binary pattern [2] was initially put forward as a texture descriptor and has demonstrated to be a triumphant in many computer vision applications. GBP descriptor describes individual pixel by the relevant gradient on various directions of pixel, whereas LBP descriptor describes individual pixel by the relative pixel intensity values of its neighborhood members.

For GBP computation, it is required to compute the gradients on four different directions such as horizontal, vertical and two diagonal directions of a pixel. Let us consider two 2-D masks as [001; 000; −100] and [−100; 000; 001], and their gradients on diagonal directions are given as T_1 and T_3; and, two simple 1-D masks as [−101] and [−101], and their gradients are specified as T_2 and T_4. Hence, the GBP feature of the pixel at (i, j)th position is computed as,

$$\begin{aligned} \delta(i, j) = h(\|T_1(i, j)\| - \|T_4(i, j)\|) + h(\|T_3(i, j)\| - \|T_4(i, j)\|)2^1 \\ + h(\|T_1(i, j)\| - \|T_2(i, j)\|)2^2 + \sum_{r=1}^{4} h(T_r(i, j))2^{7-r} \end{aligned} \tag{5}$$

$$h(\sigma) = \begin{cases} 1; \ \sigma \geq 0 \\ 0; \ \text{otherwise} \end{cases} \tag{6}$$

However, the pixel intensities of input image are normalized to the range of [0, 1], before computing the gradients. According to the above Eq. (5), GBP code (h) can be any integer, which lies in the range 0 to $2^7 - 1$. The histogram of the GBP values assessed over a sub-image potion retains the structure and texture description very well. So, we can create the final GBP image by restoring each pixel intensity value in the original image with its GBP value.

5 Applications

During the last decade, binary pattern descriptor has engrossed the leading domains such as image processing and computer vision and has proven its triumph in plethora of applications, in particular of medical image analysis, object detection and classification.

To cite object analysis, Alhindi et al. [6] extracted texture features using LBP for the categorization of histopathological images with SVM as classifier and obtained an accuracy of 90.52%. They conducted experiments on KIMIA Path960 dataset using LPB, HOG and deep network's features, and the results showed that LPB extractor has surpassed other methods, mainly used along with SVM algorithm classifier.

To cite object detection application, Feigang et al [3] extracted texture features for pedestrian detection by fusing features of human visual pedestrian system, i.e., significant characteristic factor, as a weight to the LBP eigen code. They conducted investigations on the INRIA dataset along with AdaBoost classifier and achieved an accuracy of 92.37% with an improved recognition rate for pedestrian detection.

To cite object classification, Zhou et al [2] extracted texture features using a new sight descriptor entitled gradient binary pattern and weighted histogram of gradient orientation. For more spatial information, the image is divided in to sub-regions and depicts each sub-region with the above-mentioned descriptor directly. Furthermore, the multiple category scenes are classified with SVM classifier.

To cite object detection application, Jiang et al [7] used gradient local binary pattern (GLBP) for feature extraction, by fusing gradient and texture information for human detection. They claimed that computational intricacy and time utilization of linear detector are least in case of SVM-based detector. Also, GLBP feature calculation is done as parallel, which eased hardware acceleration.

6 Elucidation of LBP, SLBP and GBP

The representation of various descriptors over a brain tumorous MR image is shown in Fig. 2. The samples used in the experimental analysis are collected from KAGGLE. SLBP can extract significant information of the MR input image as compared to LBP and GBP. Furthermore, these descriptors can be combined for the extraction of features of input image in order to get accurate detection, classification and prediction outcomes.

7 Conclusion and Future Enhancement

LBP feature extraction method is elementary and simple and has less computational intricacy. It is gray scale invariant and rotation invariant and has even more benefits.

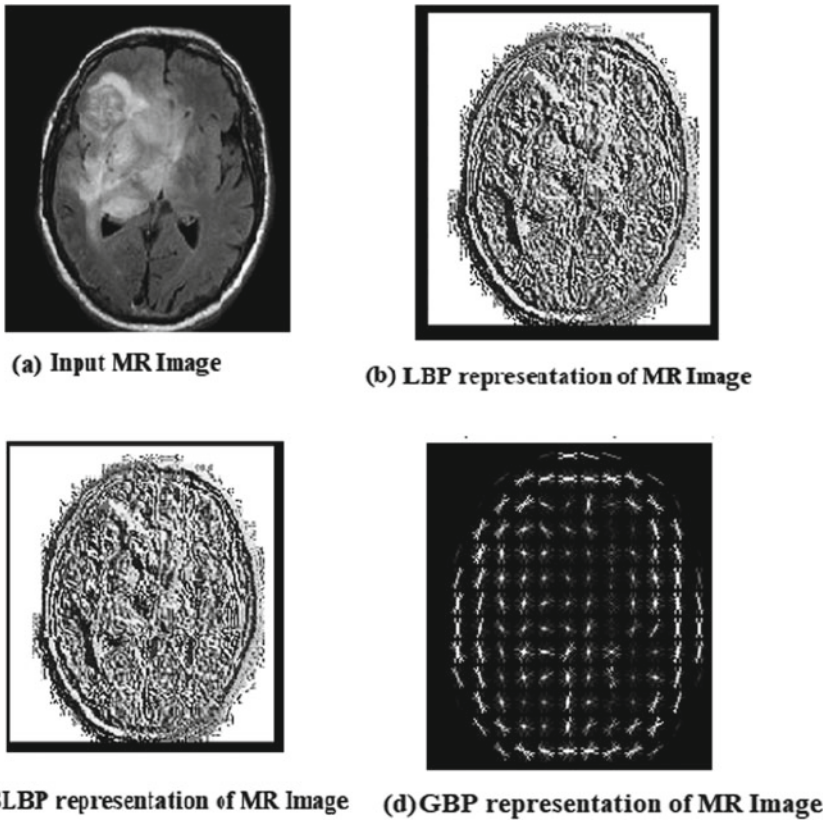


Fig. 2 Representation of LBP, SLBP and GBP descriptors

Its triumphant journey can be visualizable in many applications such as texture analysis and classification, human facial analysis and medical image analysis. The main drawback of LBP descriptor is it lacks structural information because of the ignorance of magnitude information. To capture the significance information, an improved LBP descriptor called SLBP descriptor is used by fusing significant characteristic factor as weight to the LBP feature. It can bring down the influence of various artifacts such as noise and inflate the description of noteworthy characteristics of object. GBP descriptor describes individual pixel by the relevant gradient on horizontal, vertical and diagonal directions of pixel. These descriptors can be combined and used as feature extractors in many computer vison and image processing problems such as object detection, classification and prediction for the better accuracy of outputs.

References

1. T. Ojala, M. Pietikainen, T. Maenpaa, Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Trans. Pattern Anal. Mach. Intell. **24**(7), 971–987 (2002)
2. L. Zhou, Z. Zhou, D. Hu, Scene classification using multi-resolution low-level feature combination. Neurocomputing **122**, 284–297 (2013)
3. T. Feigang, SLBP: an improved texture feature for pedestrian detection. in *IEEE International Conference on Smart City and Systems Engineering (ICSCSE)*. pp. 202–204, November 2017
4. Local Binary Patterns: New Variants and Applications, vol. 506. (2014). ISBN : 978–3–642–39288–7
5. J. Chen, S. Shan, C. He et al., WLD: a robust local image descriptor. IEEE Trans. Pattern Anal. Mach. Intell. **32**(9), 1705–1720 (2010)
6. T.J. Alhindi, S. Kalra, K.H. Ng, A. Afrin, H.R. Tizhoosh, Comparing LBP, HOG and deep features for classification of histopathology images. in *2018 International Joint Conference on Neural Networks (IJCNN)*, Rio de Janeiro, Brazil, 2018, pp. 1–7. https://doi.org/10.1109/IJCNN.2018.8489329
7. N. Jiang, J. Xu, W. Yu, S. Goto, Gradient local binary patterns for human detection. in *2013 IEEE International Symposium on Circuits and Systems (ISCAS)*, Beijing, China, pp. 978–981.https://doi.org/10.1109/ISCAS.2013.6572012

Location Dependent Safety Application for Women



M. B. Shanthi, Prakhyath Jain, and M. Prateek

Abstract Women's safety is one of the major concerns that have been the most important topic till date. As per National Crime Record Bureau (NCRB) reports, many women of various ages have been subjected to violence, domestic abuse and rape. When ladies normally need to drive late at night, it's necessary to be alert and safe. While the government takes the measures appropriate for their protection, there are also free apps for women's safety that can help them remain safe. These days, many women carry their cell phone with them, so it is critical to have at least one activated personal security app. In one way or the opposite, such a women security app will definitely make it easier. The current applications either web applications or the android apps had given a focus on the alert generation and informing the close ones or the police people for the emergency help when the victim is in need of help when a person is in danger. Main goal of this research review is to propose a women safety solution to generate a swift alert to change the route when the user reaches an area which is found to be risky for travel because of the identified reasons. We propose a system to develop the android application which maintains the currently available feature in the app by adding the new feature which helps by guiding them on the basis of "Prevention is better than cure".

Keywords Women's safety · Security · NCRB report · Android application

1 Introduction

In India, women have been granted the same rights as men. They contribute to our country's growth and development. Women are now in positions of respect in the

M. B. Shanthi (✉) · P. Jain · M. Prateek
Department of CSE, CMR Institute of Technology, Bengaluru, India
e-mail: Shanthi.mb@cmrit.ac.in

P. Jain
e-mail: prak17cs@cmrit.ac.in

M. Prateek
e-mail: prat17cs@cmrit.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_23

world, but if we look behind the scenes, we can see that they are still oppressed. Every day, we read in the news about heinous crimes against women in our country. For decades now, the safety of women in India has been an issue. We are aware that women's safety is critical, but we need to understand that they should be given with a safe environment around them. Identifying and calling on services to help them to get out of dangerous conditions is the perfect way to minimize the risk of becoming a victim of crime. In the light of the recent uproar in Delhi that rocked the country and awakened us to our daughters' safety concerns, the public is planning to strike back in numerous ways. Many applications have been designed to provide women with security mechanisms on their phones. Here, we are launching an android app that ensures women's safety. By knowing the location of the person that is in danger, it decreases the risk and assists us in need.

The growing trend towards cell phones with embedded GPS strongly indicates that the main applications for future mobile devices will be navigation and location-based services (LBS). New hardware features such as digital compasses and tilt sensors that are now making their way into state-of-the-art phones promise to accelerate the use of mobile geospatial services and transform the way people explore and interact with their physical environment. This paper presents a detailed review on the current research in developing the safety solutions for women and identifying all the required features to build an effective and complete solution for women's safety.

2 Literature Study

Crimes against women have risen tremendously in the country's urban and rural areas. In 2018, Thomson Reuters Foundation reports rated India, as the most dangerous country for women in terms of their protection. In the past, numerous studies and surveys suggested the same thing, when experts were consulted, and it was discovered that not much was done to curb their distress. The National Crime Record Bureau (NCRB) has published its "Crime in India" report for 2019 and has published some disturbing facts and statistics on women's insecurity in India. Women are gradually becoming unsafe in India. The rising incidence of crimes against women in recent years is illustrated in Fig. 1.

A total of 405,861 cases of crime against women were registered during 2019, showing an increase of 7.3% over 2018 (378,236 cases). The above report has revealed that the crimes against woman are found to be increasing from year to year though there is swift technological growth in every other field of human life. There is an immediate requirement for the invention of an effective solution to save the gender-specific crimes. Figure 1b shows the average crime cases per day reported against woman. This report shows that the average cases per day are on the decreasing side of the curve. Increased awareness and smart solutions for woman safety will surely help in decreasing this rate by making the awareness programmes and smart solutions. Based on NCRB report data about the Rape cases in last 10 years has been

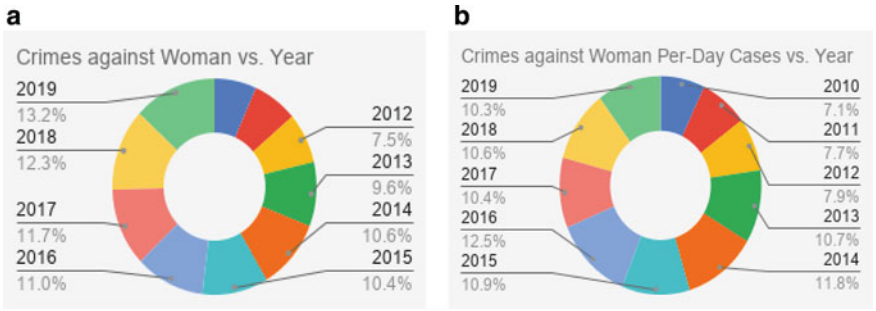


Fig. 1 **a** Crime against women in India, **b** Average crimes reported per day (*Source* National Crime Record Bureau (NCRB))

collected. The graph given in Fig. 2 shows that in the year 2014 and 2017 the highest number of rape cases get reported.

Based on NCRB reports, the data about rape cases in last 10 years was collected. The graph given in Fig. 2a. shows that in the year 2014 and 2017 the highest number of cases get reported. Average rape cases reported per day in the recent years have been shown in Fig. 2b. The Govt. initiatives and efforts from the research community in development of the smart solutions could find decrease in the reported cases. This stands true with the average cases reported per day as well. Still, there is an ample space for improving the currently available solutions and provide a safe place for all to live without gender-specific crimes. Abhijit Paradka et al., in their research work [1], discussed different problems faced by women. The primary emphasis was on the implementation of protective policies for women in public spaces and while travelling to the workplace alone. The safety of female passengers and drivers is assured by smart navigation by apps such as Uber and Ola, which work closely with the police. These apps have improved user-friendly functionality and response teams with a zero-tolerance approach with respect to discrimination and inequality

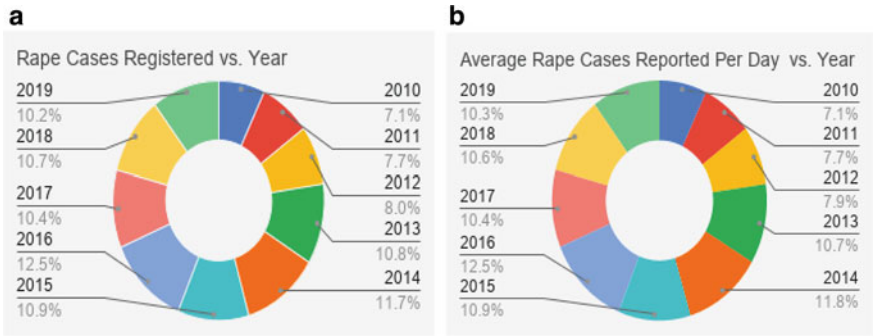


Fig. 2 **a** Rape cases reported per year, **b** Average rape cases per day (*Source* National Crime Record Bureau (NCRB))

against women. Hand in hand with the initiatives taken by the government, many researchers have proposed different technological solutions to develop Woman safety applications. The solutions are mainly based on 3 major approaches.

2.1 Android Applications

Research works have been carried out in the development of mobile applications which could be accessed through android phones. Many features in such applications were found to be common, added with new features as enhancement in each of them. Few among them have been discussed below.

Sankalp Mehta et al. in the work [2] have developed an android application for women. This app includes GPS tracking and sending the URL of the target location to nearby mobile which is having the same app. The Yarabothu et al. [3] developed an app having the function of calling the first contact stored in the emergency contact list and sending the victim's location URL to all contact numbers. The creative role included here is to give the victim's location URL to all contact numbers once every five minutes to all contacts, helping to keep track of the contact numbers. Inventions [4–7] introduce woman safety application with real-time database and data stream network for location tracking using GPS SoS. They have added little more crucial functionality to the app, like adding the spy camera functionality to silently record the video of the incident and surrounding and sending it to the emergency contacts automatically. Authors have added access to the toll-free numbers for emergency help and provision of the first-aid information for getting emergency assistance.

Research work in [8] offers a smartphone service named Women's Protection App (WoSApp) that provides a secure means for women to make an emergency call to the police. WoSApp uses a special function to enable alert through a panic button. The victim can press the panic button to initiate the alert and to send message to the close ones. The user should shake her phone and an emergency message with her GPS coordinates would be sent to her emergency contacts. Star India Pvt. Ltd. has developed an application "VithU" [9] for emergency requirements and double click of the power button of the android mobile would facilitate sending a present alert message to the saved contacts once every two minutes. "Nirbhaya" is a mobile application [10] developed by Kenil Doshi as an open-source project. When a button on the app screen is pressed, it sends a message to an emergency contact list with the user's GPS coordinates. A message updating the location will be sent every 300 m shift in position. The application Glympse [11] allows users to share their location with friends and family in real-time using GPS tracking. This app does not include any registration or contact information from the user. This is a GPS location sharing app that lets the user share the location with selected contacts.

Mahindra et al. [12] have implemented an application for android mobiles which sends message alert either through SMS or through a mail. In order to identify the user and enable app features even though the mobile keyboard is closed, the application [13] recommends a voice keyword recognition app. The GPS module

records a user's position and transmits the pre-stored emergency alert to the recorded contact numbers, including the location. The application [10] suggests an emergency management scenario that recognizes an app named IPROB to provide women with protection even in circumstances such as terrorist threats or natural disasters by automatically triggering the device by only shaking the mobile over the predefined threshold value. Once a warning has been transmitted to the registered contacts, it continues to catch the surrounding speech. A spy camera identification and women attack rescue system (SCIWARS) app is proposed in this application [14]. It serves as an intelligent warning device that senses the infrared rays from hidden cameras installed in changing quarters, hotel rooms, etc., and also warns the user via message about the unsafe location. Application [11] proposes a Save Our Souls (SOS) app to provide protection for women travelling alone or at night with a single click of the SOS button. Simply pressing the power button causes the application to run in the background and send an emergency message to the registered contacts, including the venue. The summary of the features added in different android apps has been listed in Table.1.

2.2 IoT-Based Approach

Research work involved in the paper [15] suggests an automatic, and reliable safety device composed of ATMEGA8 microcontrollers with ARDUINO software and GSM that hold users under surveillance at all times. To monitor for unpleasant conditions, it measures the heartbeat rate, temperature and pressure in the body by sensors. In such a scenario, the GPS module will be enabled to monitor the location and the wireless camera to capture images as evidence of incident for later investigation. It also amplifies the voice above the threshold limit to make it audible to the receiver with more clarity in tone.

Monisha et al. [16] have discussed a woman safety device designed using both ARM controller and the android application by synchronizing both through Bluetooth. Both could be triggered independently. The device was enabled to work even in the places where there is no internet access. In [12], researchers have proposed a wearable device enabled with voice recognition and cloud computing technology. This device enables the victim to handle risky situations effectively by reaching the close ones using the voice command. This also enables the capture the footages of the incident and uploads it to the cloud storage. In the research work [17], a smart band for woman that was connected to the phone to access the internet and to get required services on emergency. Mobile Phone attached to a smart band through Bluetooth via a specially built framework that serves as an interface between the device and the phone, the device interacts with mobile phones. An IoT-based smart ring has been developed in [18]. Just a click of a small button on the ring would initiate recording the surrounding of the incident location, and the information along with the location details would be sent to the emergency contact list. Invention in [19] and [20] also

Table 1 Summary of android applications

APP	Features included	Innovation
Android app for women safety	GPS location tracking, attaching the location URL of the location to the message to the emergency contacts	Update of location of victim during the incident
ABHAYA	GPS location tracking and live location update to all the contact numbers in the victim's list	Adding of live location update by sharing the URL every 5 min to all the contacts
We'RSafe	Added real-time database streaming to share the GPS locations of the victim	Video of the hidden camera functionality has been captured silently by the application
WoSApp	Just the vibration of the mobile beyond the threshold places an emergency call to the present contact number	Trigger the calling function by shaking the phone,
VithU	Safety app for making the guardian/parents to keep track of child's movement through GPS	Double click of the power button in the emergency begins sending the emergency message to the selected contacts
Nirbhaya	Sending alert message with press of a PANIC button. Updates location of the victim once after finds a distance of 300 m	Live location tracking of the victim and location update once after every 300 m distance
CLYMPSE	GPS location sharing app that lets you share your location with select contacts	Continuous location update to family members by sharing the live location
Fightback	App sends a message to your friend or contacts that "User is in trouble" using Email, GPS, SMS and GPRS	Sends SMS of location and Map
Android application for women safety based on voice recognition	Recognizes the voice keyword to recognize App when keyboard is locked. Sends alerts to emergency contacts	GPS location tracking and forwarding to emergency contacts Audio recording to record conversation at the incident place
PROB-emergency application for women	Allows for the management of the situation in the event of a natural disaster or any unexpected attacks	Captures the surrounding video for later investigation

(continued)

Table 1 (continued)

APP	Features included	Innovation
SCIWARS	Detects hidden cameras in shopping centres, dressing rooms, hotel rooms, and other public places	Spy camera identification and women attack rescue system
Mobile phone embedded with medical and security applications"	Provides a security warning for women who need emergency medical assistance with a single click of the SOS button	Creating and sending emergency medical assistance
I safe apps	Sends a message to the guardian number with the location and/or an audio–video call	Tools like first-aid help, fake call help and video call

is based on IoT module for tracking the location of the victim and update of the information to the selected list of contacts.

The work carried out in the research work [21] is for responding aptly in critical condition automatically. The proposed system consists of a voice recognition module, GPS module along with other sensors like heartbeat sensor and accelerometer to correctly monitor the situation of the victim and raspberry pi is used for the processing of the obtained data, and preventive or protection action is taken as per the severity of the threat. The protection system consists of call for rescue action in which the GPS located position of the victim is to send to the concerned authority the system also comprises of a shock generation jackets for on-time protection (Table 2).

2.3 ML Approach

The research discussed in [22] focuses on the role of social media in promoting women's safety in Indian cities, with a particular emphasis on the role of social media websites and apps such as Facebook and Instagram on Twitter. This paper also reflects on how the common Indian people should build a sense of duty on the part of Indian community so that we can concentrate on the welfare of women around them. Twitter tweets that usually include photos and text as well as written messages and quotations focusing on safety of women in Indian cities can be used to read a message and to take strict action and punish those who harass the women. The research work proposed in [23, 24] proposes the "Suraksha" women's safety system, which is an easy-to-operate device. You can trigger this system with a voice command by pressing the switch key. Emergency message would be sent to the selected contacts.

An automated approach to predict the danger based on female emotions such as anxiety, rage, etc. is proposed in paper [25]. In order to obtain body movements and

Table 2 Summary of the applications based on IoT

Device	Features included	Innovation
Advanced security system for women	GSM and ATMEGA-8 microcontroller with ARDUINO for all time observation of the user. GPS module to track the location. Wireless camera to capture the images as proof	Amplification of the voice of the woman to scream out above the threshold value
FEMME	Instant location tracking and update to identify the victim's location	ARM controller and the android application by synchronizing both through Bluetooth
IoT-based wearable device for women safety	Enables the victim to handle risky situations effectively by reaching the close ones using the voice command	Enables the capture the footages of the incident and uploads it to the cloud storage. The feature of voice recognition for activation brings novelty to this solution
Smart security technology for women based on IoT	Developed a smart band connected through the Bluetooth to the android mobile	Smartphone connected to a smart band through Bluetooth Low Energy (BLE)
SMARISA: a raspberry pi-based smart ring for women safety using IoT	A safety button was included in the design of a smart ring. The operation of producing and sending the warning was triggered by a single click of the mouse	To activate the services, use a Raspberry Pi, a camera, a buzzer, and a button
Women safety system based on IoT technology	A portable computer with a button that sends a message warning to the emergency contact list when pressed	Microcontroller, GSM module, GPS module, IoT module, Neuro Stimulator, Buzzer, and Vibrating Sensor are some of the components

provide monitoring, a camera was mounted at a higher altitude. Situation is analysed based on the emotions recorded in the successive images (Table3).

3 Conclusion

Women's safety is one of the major subjects which have attained the extensive attention to develop complete solution for avoiding the gender-specific crimes. We have put our effort in bringing together all the features implemented through different approaches like android apps, IoT-based solutions and applications added with artificial intelligence. The main goal of this intensive study is to design and develop an

Table 3 Summary of applications based on ML approach

Title	Features	Innovation and technology
Analysis of women safety in Indian cities using machine learning on tweets	Works based on the quotes, messages and images shared through social media networks	Use of Twitter platform Facebook and Instagram
Women security safety system using artificial intelligence	Travel safety by alerting red alert zones	Use of crime history related data and Artificial intelligence
Suraksha"—a women safety device	To handle emergency situations with live update of the location	Activation of the device through voice command
An intelligent security system for violence against women in public places	An advanced automatic technique to predict the unsafe situation based on the female emotion as fear, anger, etc	Use of sentiment analysis

effective and complete solution for women's safety by aggregating all the available security features from different applications added with location-specific alert to the user based on the crime analysis history of the location during journey. We propose a women's safety application adding all the discussed features in the current research and enhance the application to generate an alert about how safe the travelling location is and to provide details about the alternative path to reach the destination safely.

References

1. R.S. Yarabothu, B. Thota, Abhaya, An android app for the safety of women. IEEE, December (2015). 978–1–4673–6540–6/15/$31.00©2015
2. S. Mehta, S. Janawade,V. Kittur, S. Munnole, S. Basannavar, An android based application for women security. IJESC **7**(6), (2017)
3. R.S. Yarabothu, B. Thota, Abhaya, An android app for the safety of women. IEEE, December (2015). 978–1–4673–6540–6/15/$31.00©2015. https://doi.org/10.1109/INDICON.2015.7443652
4. R. Simon, P. Fröhlich, T. Grechenig, GeoPointing: evaluating the performance of orientation-aware location-based interaction under real-world conditions. J. Location Based Serv. (Taylor and Francis Group, 2008). ISSN: 1748–9725 (Print) 1748–9733
5. D.S. Prashanth, G. Patel, B. Bharathi, Research and development of a mobile based women safety application with real-time database and data-stream network, ICCPCT (2017)
6. M. Vijayakumar, D. Devi Kala Rathinam, M. SwethaVadera, N. Karpagam, S. Leelavathi, Women safety location tracker. Int. J. Scientif. Eng. Res. **8**(7) (2017). ISSN 2229–5518
7. R.R. Khandoker, S. Khondaker, Fatiha-Tus-Sazia, F.N. Nur, S. Sultana, LIFECRAFT: an android based application system for women safety. in *International Conference on Sustainable Technologies for Industry 4.0* (STI), 24–25 December, Dhaka (2019)
8. D. Chand, S. Nayak, K.S. Bhat, S. Parikh, Y. Singh, A. Kamath, A mobile application for Women's safety: WoSApp. in*TENCON 2015–2015 IEEE Region 10 Conference* (2015). https://doi.org/10.1109/tencon.2015.7373171
9. World Health Organization, Global and regional estimates of violence against women: prevalence and health effects of intimate partner violence and non-partner sexual violence, (Geneva, WHO, 2013)

10. S. Magesh Kumar, M. Raj Kumar, IPROB—emergency application for women. Int. J. Scientif. Res. Publicat. **4**(3), (2014.) Online at the link www.ijsrp.org
11. B.K. Baishya, Mobile phone embedded with medical and security applications. IOSR J. Comput. Engg. (IOSR-JCE) **16**(3) (Version IX), 30–3 (2014). Department of Computer Science North Eastern Regional Institute of Science and Technology Nirjuli Arunachal Pradesh India, e-ISSN: 2278–0661 p-ISSN: 2278–8727
12. A. Singhal, S. Jain, K. Agarwal, Rakshak—An IoT based wearable device for women safety. Int. J. Eng. Adv. Technol. (IJEAT) **9**(4), (2020) ISSN: 2249–8958
13. D. Uma, V. Vishakha, R. Ravina, An android application for women safety based on voice recognition. Int. J. Comput. Sci. Mobile Comput. (IJCSMC) **4**(3), 216–220 (2015) . Department of Computer Sciences BSIOTR wagholi, Savitribai Phule Pune University, India. ISSN 2320–088X Online at www.ijcsmc.com
14. V. Pawar, N.R.Wankhade, D. Nikam, K. Jadhav, N. Pathak, SCIWARS android application for women safety. Int. J. Eng. Res. Appl. **4**(3)(Version 1), 823–826 (2014). Online at the link www.ijera.com,. Department of Computer Engineering, Late G.N.S.COE Nasik India, ISSN: 2248–9622
15. V. Thooyavan, Advanced security system for women. Department of IEEE 2014 Project List under real time target surveillance system, slides share on www.slideshare.net, Jun 24, 2014
16. D.G. Monisha1, M. Monisha, G. Pavithra, R. Subhashini, Women safety device and application-FEMME. Indian J. Sci. Technol. **9**(10), (2016). https://doi.org/10.17485/ijst/2016/v9i10/88898
17. J.K.Thavil, V.P. Durdhawale, P.S. Elake, Study on smart security technology for women based on IOT. Int. Res. J. Eng. Technol (IRJET) **04**(02), (2017). e-ISSN: 2395-0056 www.irjet.net p-ISSN: 2395–0072
18. D. Mani Megalai, U. Leena Agaliya, K. Aarthi, Smart security solution for women using IOT IOSR. J. Eng. (IOSRJEN) 49–53 (2020). www.iosrjen.org ISSN (e):2250–3021, ISSN (p): 2278–8719
19. B. Sathyasri, U. Jaishree Vidhya, G.V.K. Jothi Sree, T. Pratheeba, K. Ragapriya, Design and implementation of women safety system based on IOT technology. Int. J. Recent Technol. Eng. (IJRTE) **7**(6S3) (2019). ISSN: 2277–3878
20. M.R. Tejonidhi, Aishwarya, K.S. Chaithra, IOT Based smart security gadget for women's safety. in *2019 1st International Conference on Advances in Information Technology* (IEEE, 2019). 978–1–7281–3241–9/19/$31.00 © 2019
21. C.K. Sruthi, K. Mridul, K. Zayan, V. Ashin, K. Sreehari, AI based women security system. Int. J. Scient. Res. Rev. (2020). ISSN NO: 2279–543X
22. D. Kumar, S. Aggarwal, Analysis of women safety in indian cities using machine learning on tweets. (IEEE, 2019). 978–1–5386–9346–9/19/$31.00 ©2019
23. H.R. Rashmi Rani Agnihotri, K.S. Malipatil, A brief study on women problems in India. Int. J. Develop. Res. **8.8**, 22583–22587 (2018). (Can be refered for Introduction)
24. N. Bhardwaj, N. Aggarwal, Design and development of "Suraksha"-a women safety device. Int. J. Info. Computat. Technol. **4**, 787–792 (2014). Department of Electronics and Communication ITM UNIVERSITY Huda Sector 23-A Gurgaon Delhi, India. ISSN 0974–2239. Online Available at http://www.irphouse.com
25. R. George, V. Anjaly Cherian, A. Antony, H. Sebestian, M. Antony, T. Rosemary Babu, An intelligent security system for violence against women in public places. Int. J. Eng. Adv. Technol. (IJEAT) **3**(4), (2014) ISSN: 2249–8958

A Review of Adaptive and Intelligent Online Learning Systems



Deshna Sachan and Kriti Saroha

Abstract Education is a vital part of everyone's life. With the advancement of the internet, online learning has gained a wide scope. With the availability of a wide variety of courses and course content available online, learners usually struggle while choosing the course that will be most beneficial to them. It's mainly because of the learners having different learning styles, different level of understanding, and different knowledge domains. Along with this, the learners also suffer from improper monitoring and evaluation. The adaptive learning system adapts itself as per the learning style of the learner and an intelligent tutoring system helps in the monitoring and evaluation of the learner's performance. An intelligent tutoring system also provides an immediate and customized response to the learner. With the combination of Adaptive learning system and intelligent learning system, the online learning system can be developed with advanced capabilities and can be more beneficial to the learners than traditional online learning system. There are various learning styles in which learners can be categorized. Various learning style models are Felder Silverman model, VAK model, David Kolb learning style model etc. The paper presents a discussion on the research work done in the area, showing the work done on adaptive learning systems and intelligent tutoring systems.

Keywords Adaptive learning system · Intelligent tutoring system · Learning style · Learning style model · Online learning · Personalized learning

1 Introduction

In a world, where the internet has become one of the important part of our day-to-day life, merging the internet with education leads to massive success. Online courses were becoming quite popular in the past few years. Educational institutes use the Learning Management System (LMS) to offer online courses, thereby eliminating

D. Sachan (✉) · K. Saroha
C-DAC, Noida, India

K. Saroha
e-mail: kritisaroha@cdac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_24

problems like time preferences and physical barriers. Even considering the scenario of the covid-19 pandemic, education institutions all over the world were shut down, and everyone struggled with learning at home deciding on what, where, or how to begin the learning process. Whenever a learner seeks a course online, he/she starts perusing the first course they find without examining if it suits their learning style, knowledge level, content preferences, etc. This might not cause a problem in beginning but as they move forward with the course, the learners might lose interest in the course and/or are not able to understand the course content. This is mainly because every learner has a different learning style. There are various learning style models to identify learning styles of students. Using learners learning style, the adaptive learning system provides personalization with the course content to the learner using the recommender system.

David Kolb [10] learning styles model (1984) indicates 4 learning styles that includes: **Reflective-Observation** which implies to Review/reflect on the experience, **Concrete-Experience** that suggests having/performing experience, **Active-Experimentation** suggesting to try/plan out what is learned and **Abstract-Conceptualisation** that implies to conclude/learn from the experience.

According to **VARK** model of Neil D. Fleming, based on their preference of learning material, the learners are divided into **V**isual, **A**uditory, **R**eading/writing, and **K**inesthetic categories [8].

As per Kolb's experimentation, Honey and Mumford developed four learning style preferences: Activist, Theorist, Pragmatist, and Reflector in their learning style model [9].

The most considerable and prominent learning style models, Felder Silverman Learning Style Model **(FSLSM)** [3], classifies learners based on four dimensions i.e., Active/ Reflexive, Sensing/Intuitive, Visual/Verbal, Global/Sequential.

The Mayer-Briggs Type Indicator **(MBTI)** [11] is a pensive and self-examining questionnaire that includes four classes: **I**ntroversion or **E**xtraversion, **S**ensing or **I**ntuition, **T**hinking or **F**eeling, **J**udging, or **P**erceiving. These categories are divided into 16 different combinations. MBTI indicates different people having different psychological preferences and the way they perceive information and make decisions.

Felder and Solomon developed an Index of Learning Style **(ILS)** Questionnaire [6] which contains forty-four questions divided into eleven questions for each of the dimensions of Felder Silverman Learning Style Model and its results indicate the individual's learning preference in every dimension.

The Adaptive Learning system adapts itself as per the learning style of the learner and the intelligent tutoring system is used to provide an immediate, customized, and personalized response to the learner. It also monitors and evaluates the student based on their performance. The paper is organized as follows: Sect. 2 of the paper presents a review of the previous works done in the area and gives a comparative analysis. In Sect. 3, an approach is presented and proposed to be used in implementing the proposed adaptive and intelligent online learning system and Sect. 4 gives the conclusion followed by references.

2 Related Work

Brusilovsky and Peylo et al. [14], explained that Intelligent systems and adaptive systems are not really synonyms. The adaptive systems are the one that are different for every student or group of students by taking the individual's or group's accumulated information into account. On the other hand, Intelligent system systems use techniques to provide deeper and better support to the learners of the system.

Ibrahim et al. [7] proposed a new adaptive learning framework to identify a student's learning style using Felder-Silverman Learning Style Model (FSLSM) to develop learner's profile and therefore recommend study content in a new internet-based Learning Management System (LMS). The instructors are allowed to not only set up various courses and their contents but also monitor learner's learning styles and performance. In this way, the framework of Adaptive learning solves the drawbacks and of the traditional Learning Management System and therefore improving the process of learning and also the learner's performance. The framework also uses both static and automatic student modeling approaches. Static modeling is defined using the Index of Learning Style (ILS) questionnaire feedback. In the automatic student modeling approach, the record of the learner's activities is maintained by the Learning Management System keeps by recording the number of clicks and amount of time spent by learner on each of the learning content.

An adaptive learning system for higher learning [12] was introduced by Kasinathan et al. They discussed an adaptive learning system that was well suited for both instructors and students and was designed to enhance or improve learning based on various different learning paces across the classes. It's a user-friendly system that can analyze a student's level of understanding as per their cognitive behaviour. The system permitted the use the online application by the learners as per their requirements, so that they can access the module beyond the traditional class-hours. The system also has a reporting module that enables instructors to monitor and alter the method of teaching as per the learner's requirements. The adaptive system implementation was tested on a course of Java programming in the trial run. To check if the system is working properly and fault-tolerant, it undergoes Ad-hoc testing during execution along with unit testing. The GUI testing and usability testing were performed in parallel with UAT. Besides, the paper also discusses adaptive e-learning platforms like **Smart sparrow adaptive learning system, Fishtree,** and **Knewton Adaptive Learning System.** These platforms provide learners with an interactive interface, has adaptive quizzes and simulations. These platforms accept every learner as unique and hence create the most novel personalization with standard-aligned resources, social media-based tools and world-class analytics to assist the instructors that also saves time while improving the learning experience. Besides this, these systems provide helpful features that includes mobility, security, ease of use, and fun with learning.

In [5], Adaptive Online Learning Design Using LMS Moodle is proposed to eliminate the complexity of technical works. The Adaptive Learning System undergoes two evaluations- Formative evaluation and Summative evaluation. The formative

evaluation is performed at the developing process of the course and summative evaluation is performed at the end of the course. Both the evaluations aim to improve the course and check its effectiveness and are applied using two testing models, i.e., Alpha testing and Beta testing. The alpha testing is performed by teachers and experts while beta testing is accomplished by users or learners. The Moodle suitability table for adaption illustrated in Table 1, is used to check the content preference type for different category of learner.

This LMS Moodle has been applied in Udayana University since 2008 with the major features as a resource, forum activity, assignment, and survey. The two evaluations and two testings are performed to improve the adaptive capability of the system to accommodate various types of learner's style.

Thankachan et al. [3] proposed a design of an Intelligent & Adaptive Tutoring System which is a modified form of teaching from the traditional form of teaching for web-based courses. The designed system not only offers pedagogical support but also utilizes information in the **MOOC** (Mass open online courses) database with logs of learner-system interaction to create a system that supports the learning system to adapt as per the learner's needs. The course administrator has the authority of manual intervention for at-risk learners. Techniques like educational data mining, visual data analytics and learning analytics are used to determine the best teaching methods and provide pedagogical support to every learner of the system. The designed system personalizes the learning for each individual and helps the instructor in administrating the course to the large number of learners. The author also suggests the gaze-tracking system for detecting if students are engaged in cheating activities. Therefore, a minimalist view of an Intelligent Tutoring System (ITS) is suggested that includes an adaption engine and unique data collection methods and its analysis to provide unique perception into the field of personalized learning.

Jing and Quan et al. [1] proposed a new adaptive-personalized approach for teaching that makes use of grid agent architecture and artificial psychology techniques. From the architectural point of view, the personalized grid agent model has 4 components i.e., Learner's Agent (Sends request for learning), Manager's Agent (passes learner's information to get most suitable learning resources), Teacher's Agent (Returns the matched service information using grid discovery agent) and Knowledge base. The grid agent learning model includes features like registry, directory, and discovery. Using these features, the manager's agent finds suitable learning services. By implementing the adaptivity of the grid agent model and artificial psychology, the student's agent emphasizes if the learning material matches the personality type of the learner. The experimental data was used to support the theory that the learners accomplish better at learning if they use the defined adaptive model.

In [2] Yixuan and Yang explained the composition of intelligent teaching system (ITS) and the realization process of the system as system core. The system adopts data mining association rules and decision tree mining algorithms to enhance its personalization and intelligence. It uses association rules to find interest points of the learner whereas the decision tree algorithm is used to excavate learners' understanding of knowledge points. Classification of cluster analysis is used to teach students as per their ability and knowledge level. The proposed system has 4 main

Table 1 Moodle suitability table for adaption [5]

	Active	Reflexive	Visual	Verbal	Sequential	Global	Sensitive	lnituitive
Forum	Concrete problems	Topics for thinking	No	Yes	Yes	Global topics	Facts, examples	Abstract topics
Chat	Yes	No	No	Yes	Frequent	No	Yes	No
Glossary	Many terms	Concepts	No	Yes	Yes	No	Yes	No
Works flop	Experiment	Unexplored topics	Yes	Yes	Yes	Yes	Practical examples	Unexplored topics
Survev	No	Yes	Yes	Yes	No	Yes	Yes	Yes
Choice	Yes	Yes	Yes	Yes	Yes	Rarely	Yes	No
Lesson	Problems examples	Provided topics	lllustration	Written multimedia	Yes	Rarely	Facts, algorithm	Rarely
Comm	Face-to-Face	Email	Combined	Combined	Combined	Combined	Combined	Combined

modules as **Teacher module** (Information acquisition system and student information base), **Student module** (Teaching strategy library and inference engine), **Knowledge library** (Domain knowledge base resource library), and **Information mining module** (Describes association, classification, and cluster analysis). The system not only provides personalization but also solves the problem of traditional ITS by providing the malpractice of the system.

In [4], Educational data mining is used in developing the methods to analyze the learner's performance in order to enhance the learning quality. The authors used the academic, behavioural, and non-behavioural features to analyze the performance of the learner. By finding the relationship between the mentioned three features, a massive improvement in student's academic performance and reduction in dropout rate was analyzed. The system has 2 main modules as Data mining module and the personalized tutor module. The data mining module acquires student's information and forms student clusters depending upon similar characteristics to apply corrective measures to enhance the academic performance whereas the personalized tutor module identifies learner's behavior using clusters and hence provides classified learning content and customized instructions to the learner.

In [13], an intelligent tutoring system named "Poly-X" is presented which is integrated with different modules including the Intelligent Quiz Module (Generates tests, quiz and hints, checks results and suggests checkpoints for further explanations), Learning Control (Provides contents as theory notes, short videos, animations or graphics, real case studies etc.), Statistical and Analysis Module (Users actions are recorded for future investigation), and the video conferencing module for group conference. The system used a quiz-based approach by replacing the text with images to prevent cheating.

A comparative analysis of the papers discussed in Sect. 2 is presented in Table 2.

The learning systems implemented earlier were either adaptive learning system or intelligent learning system. The hybrid approach i.e., adaptive and intelligent learning system were not found to be implemented in a way to enhance the existing online learning systems. Moreover, the earlier implemented approach of finding the learning style of learner was dependent on models like Felder-Silverman model, VAK, MBTI etc. The proposed system, in addition to using such models also, uses learner's information including the learner's behaviour to find their learning style.

3 Proposed Approach

This section describes the proposed approach for designing an Adaptive and Intelligent Online Learning System and is illustrated in Fig. 1. The courses would be divided manually into the level of difficulty and then the learner's information (including basic details like name, DOB, Address, Phone number, etc., along with the learner's knowledge level of the course and his/her learning style) would be collected. Various learning style model and learner's behaviour would be used to identify the learner's

Table 2 Comparative analysis

Paper	Techniques/ model used	Work done	Conclusion
Ibrahim et al. [7]	Felder-silverman learning style model (FSLSM)	The system detects learning style using FSLSM and hence recommends learning content on web-based learning management system	The system framework supports both static student modeling and automatic student modelling approach Adaptive system is implemented using FSLSM
Chen and Yang [2]	Data mining association rules, decision tree mining and cluster analysis	The paper uses data mining and decision tree algorithm to enhance the intelligence and personalization of intelligent tutoring system. Student evaluation module and data analysis modules are designed while student's performance and evaluation library, students and teacher's basic information module are used as data mining objects	Association rules are used to find students' interest points, decision tree algorithm to improve learner's learning abilities and classification of cluster analysis to teach students according to their level of understanding and knowledge level
Kasinathan et al. [12]	Smart Sparrow, Fishtree and Knewton	The system analyses the learners on the basis of their cognitive level and hence provide the suitable learning content that is accessible beyond the class hours. The reporting module allows the lecturer to monitor and make changes in the method of study. The learner can gauge and monitor their level of understanding. The system also generates a status report of the student's performance which can help in finding where the learner lags behind and what is the highest failure rate. Hence, more focus can be given on such topics	The system allows lecturer to provide personalized study material and content including an appropriate level of questions for the students, who have the access to practice the questions. ALS evaluates the student's progress and knowledge level of the student and suitable tests are provided accordingly

(continued)

Table 2 (continued)

Paper	Techniques/ model used	Work done	Conclusion
Jing and Quan [1]	Grid-agent model	Proposed here is an advanced personalized approach using grid agent using artificial psychology techniques to implement adaptivity. A grid agent is independent unit that has specific behavior rules. In proposed model, grid agent environment is composed of a system general control or learner's agent, a manager's agent and knowledge service or the teacher's agent. Along with AP mathematics theories, the system architecture is integrated	The adaptive e-learning model evaluates learner's personality and thus provides learning content that is better suitable than traditional learning material
Liu et al. [13]	Zone of proximal development (ZPD)	The proposed intelligent e-learning system is integrated with various modules like adaptive navigation learning control, quiz module for learning assessment and video conferencing module	"Poly-X" provides the e-learning model to support adaptive and flexible teaching–learning activities
Karun Thankachan [3]	Educational data mining, visual data analytics and learning analytics	The proposed intelligent system offers pedagogical support that utilizes the information in database with system-user interaction information that enables system to adapt according to user's needs. Course admin provides manual intervention to help at-risk students	The designed system provides personalized learning support & experience and helps teacher in administrating the course to a large number of students
Linawati et al. [5]	Felder-Silverman model, Web-based educational system with learning style adaptation (WELSA)	The use of Learning Management system or LMS MOODLE improved the system in term of effectiveness. The proposed approach has of two evaluations (formative and summative evaluation) and two testing (alpha and beta testing), to improve the adaptivity and to accommodate various type of learning style	The design of adaptive system using LMS Moodle is easy to implement and doesn't involves the complexity of technical works. Two evaluations and testings improved the system in terms of effectiveness

(continued)

Table 2 (continued)

Paper	Techniques/ model used	Work done	Conclusion
Jenila Livingston et al. [4]	Educational data mining, cluster formation, performance analysis	The academic, non-behavioural and behavioural features are used to analyze the performance of learners by clustering them on the basis of similar characteristics and then providing the customized instructions to improve their academic performance	There is a massive improvement in the learner's performance and reduction in student dropout rate by analysing behavioural, non-behavioural and academic achievement of the learner
Maher et al. [15]	Personalized adaptive gamified e-learning model (PAGE)	The personalized adaptive gamified e-learning model or PAGE model is used to enhance the existing MOOCs by providing extended levels of satisfaction in visualization and learning analytics in enriched online learning process which supports learner's intervention in resulting learning analytics	The learning analytics proposed has been developed with required adaption the courses and learning flow of the learner. The obtained results signify a positive potential in visualizing the learning process & adaption decisions of learner

learning style. Using learner's information, the recommender system would recommend the most suitable course content to the learner. An instructor or a teacher would monitor and evaluate the learner's performance. After each evaluation, the learner's information would be updated and the recommender system would suggest course content using the updated information. This process would stop when the learner's evaluation is satisfactory and he/she is ready for the next chapter/course.

The intelligent tutoring system will be used on the teacher/instructor end to provide an immediate and customized response to the learner. This will provide them with a proper guidance and evaluation during the course run.

3.1 Description of the Proposed Approach

- Before beginning the course, the learner will be given a test to confirm his/ her knowledge level.
- The hybrid approach will be used to determine the learners' Learning style.

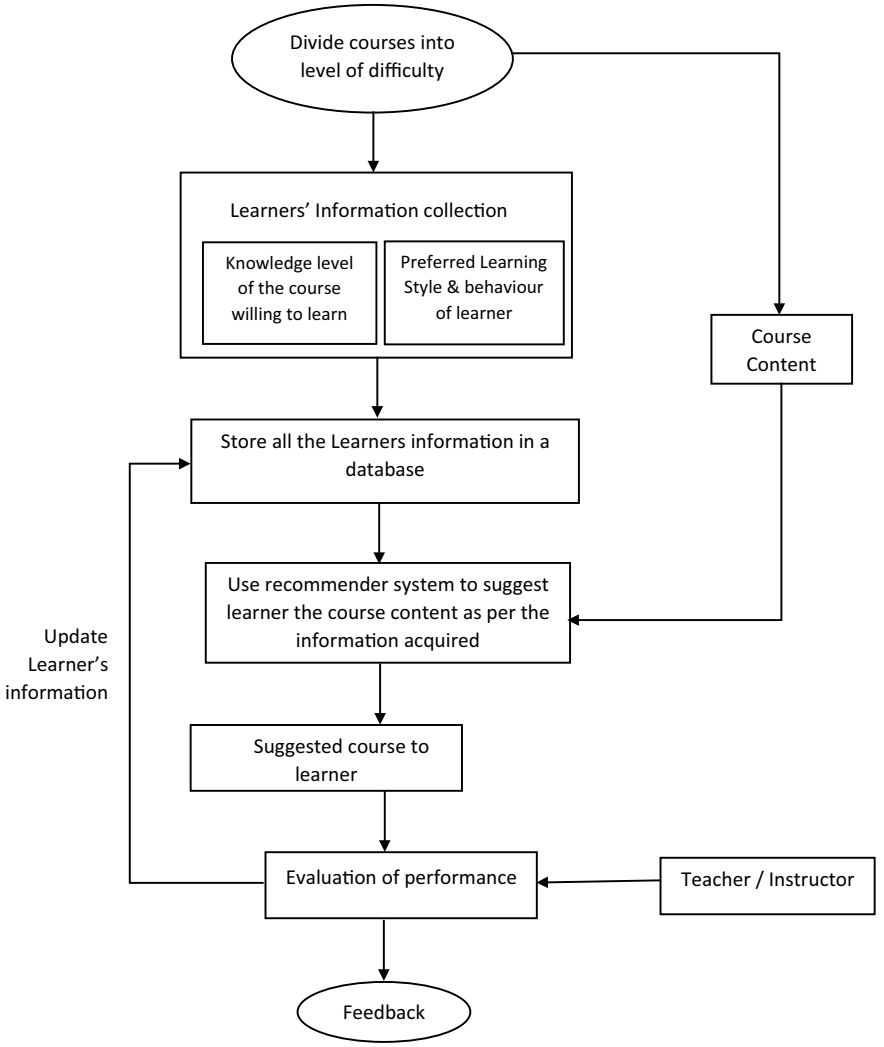


Fig. 1 Proposed model

- Combination of content-based filtering and collaborative filtering will be used as recommendation techniques.
- The learners' information will be updated after each evaluation and the recommendation process works again to suggest the course content.

4 Conclusion

This paper discusses various frameworks for detecting learner's learning style and using it to develop his/her profile. The information hence stored in Learner's profile is used to recommend Personalized Learning Content to the learner in the Learning Management System. The paper also discussed student modelling approach to automatically detect learning style of the student/learner in future. The adaptive and intelligent feature of the leaning system are used in enhancing the existing learning system to be more customized and/personalized for every learner. The future work deals with the implementation and performance evaluation of Adaptive and Intelligent Online Learning System.

5 Limitations and Future Work

Since the models that are used to identify the learning style of learner consists of various questionnaire and sometimes students may not answer them correctly, in such cases it will be difficult to identify the learning style of the learner. Moreover, the learner's learning style may change with time and therefore it would be required to develop a model that dynamically modifies its content as per the current learning style of learner. The analysis of the proposed model is our next steps of focus.

References

1. C. Jing, L. Quan, An adaptive personalized e-learning model. in *The Proceedings of International Symposium on IT in Medicine and Education* (IEEE, 2008)
2. C. Yixuan, Z. Yang, Research on intelligent tutoring system based on data mining algorithms. in *The Proceedings of International Conference on Intelligent Transportation, Big Data and Smart City* (ICITBS) (IEEE, 2019)
3. K. Thankachan, Intelligent tutoring system. in *The Proceedings of International Conference on Inventive Computing and Informatics* (ICICI) (IEEE, 2017)
4. L.M. Jenila Livingston, L.M. Merlin Livingston, L.G.X. Agnel Livingston, A. Annie Portia, Personalized tutoring system for elearning. in *The proceedings of International Conference on Recent Advances in Energy-efficient Computing and Communication* (ICRAECC) (IEEE, 2019)
5. Linawati, N.M.A.E. Dewi Wirastuti, G. Sukadarmika, I.M. Arsa Suyadnya, D.C. Krishne, Adaptive online learning design using moodle. in *The Proceedings of International Conference on Smart Green Technology and Information Systems* (ICSGTEIS) (IEEE, 2017)
6. M.B. Yel, S. Sfenrianto, E.T. Meistiawan, An adaptive e-leaming model based on myers-briggs type indicator (MBTI). in *The proceedings of 3rd International Conference on Informatics and Computing* (ICIC) (Palembang, Indonesia, 2018)
7. M.S. Ibrahim, M. Hamada, Adaptive learning framework. in *The Proceedings of 15th International Conference on Information Technology Based Higher Education and Training* (ITHET) (IEEE, 2016)
8. N.D. Fleming, in *Teaching and Learning Styles: VARK Strategies.* (IGI Global, 2001)

9. P. Honey, A. Mumford, in *The Learning Styles Helpers Guide*. (Peter Honey Publications Ltd., 1992)
10. R.F. Ammerman, P.K. Sen, R.A. Streveler, Work in progress—the kolb learning model applied to an advanced energy systems laboratory. in *The Proceedings of Frontiers in Education 35th Annual Conference*, (Indianopolis, 2005)
11. R.M. Felder, B.A. Soloman, Index of learning styles questionnaire (1997). Online available at http://www.engr.ncsu.edu/learningstyles/ilsweb.html
12. V. Kasinathan, A. Mustapha, I. Medi, Adaptive learning system for higher learning. in *The Proceedings of 8th International Conference on Information Technology* (IEEE, 2017)
13. J.N.K. Liu, S. Shiu, Y. Wang, Z. Li, L. Jia, Y. Rao, Poly-X: an online intelligent tutoring system for e-learning. in *In the Proceedings of 3rd International Conference on Data Mining and Intelligent Information Technology Applications*, (Macao, 2011)
14. P. Brusilovsky, C. Peylo, Adaptive and intelligent web-based educational systems. Int. J. Artif. Intell. Educ. (2003)
15. Y. Maher, S.M. Moussa, M.E. Khalifa, Learners on focus: visualizing analytics through an integrated model for learning analytics in adaptive gamified e-learning. IEEE Access (2020)

Background Manipulation with Computer Vision



A. Tamilarasi and Gourav Kumar

Abstract A Background gives an extra advantage to one's presentation. In today's world, we are digitalizing every section of the professional lives of humans, and often we need to be present digitally in an event. In those times, we look for a place which is has a decent background where we can present ourselves while maintaining our privacy. Privacy is important to everyone and we try to ensure our private details are not made public in any way. However, it is not possible for everyone to ensure a common background. If we can select our background digitally then it would solve this issue. Computer vision can help us in manipulation of background during video calls and ensure safety of our personal information. For this purpose, we are going to use Open CV to change the background to a video of our choice. We can select a video of our choice and upload it to the module and get the desired background by replacing it. The proposed technique is more efficient and execution time is lesser compared to existing techniques.

Keywords Computer vision · Open CV · Background image

1 Introduction

In the year 2020, we were hit with a global pandemic caused by the COVID-19 virus. The effect of the disease was extremely devastating and we were all advised to stay home. There was a complete lockdown across many countries in the world. During this time, we had no other option but to shift to a more digital approach. People were forced to work from home. Since we live in an era dominated by technology; working from home did not have much of a negative impact. Almost everything was available at our fingertips. During this time so many small firms got shut down but so many new opportunities were available as well. Many people utilized the opportunities well and started doing business online. All communications had to be done digitally. Presenting yourself digitally from your location can be challenging. It is not easy to

A. Tamilarasi (✉) · G. Kumar
Department of Computer Application, Kongu Engineering College, Erode, TamilNadu, India
e-mail: drtamil@kongu.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_25

find a quite place in our home as there is disturbance everywhere. Even if we find a quite place from where we can attend the meeting, the next challenge is to find a decent background that makes the presentation more attractive. It is not possible for everyone to have access to a presentable background.

Background plays a vital role in online presentations. Presentations can be made more simple and neat if we can find a suitable background no matter where we are located. This can be carried out using the Computer Vision libraries in Python. Engineering and Sciences have been a critical building block to mankind. Computer Vision is one of the major parts of that system, since it can help machines look at the things in more humanized way and give it human perspective. This system has slowly grown over the years and now has a variety of libraries the can helps to write algorithms in a more effective and optimized way producing the desired results. Nowadays, Computer Vision is used in most of the applications which we use on a regular basis that we are not aware off. In this proposed system we are going to use OpenCV library from Computer Vision to modify our background in videos during online video conferences.

1.1 Overview

The proposed paper set up an approach to modify the background of a real-time video meeting conducted through online using Computer Vision Technique. By altering the background video of members participating in a meeting or by exchanging the background video of an individual while he attends a meeting, the individuals can safeguard their privacy. The background-altering method in this proposed paper includes a Computer vision library that is OpenCV model for video semantic segmentation. We all want to protect our privacy at all cost. But there at times we need to present digitally for our meetings, and in such cases, we do not wish to compromise with our privacy. We need a tool with the help of which we can change the background as we wish. During this pandemic all the schools started teaching online and all the students need to present online with their video on. If somehow, we can have a video of our own choice; it would make our lives so much better. With the help of OpenCV we can manipulate the background as we wish. We do not have to be concerned for our privacy.

1.2 Computer Vision (CV)

Computer vision (CV) is that the sector of technology that creates a specialty of replicating components of the complexity of the human imaginative and prescient device and permitting computer systems to select out and manner gadgets in snapshots and motion pictures within the identical manner that citizenry do. So far, CV is best labored in constrained way because of advancement in Artificial Intelligence,

neural networks and deep learning, the world has been capable of take first rate leaps in current years and has been capable of exceed citizenry during a few obligations with respect to detecting and tagging gadgets. One of the elements at the rear of the success of CV is that the quantity of information we produced nowadays is often we want to educate and make computer vision better.

Along with an incredible amount of visual data (for example, per day nearly 3 billion images are pooled), the computing power is essential to evaluate the information. The area of CV is an up-growing research field with newly introduced algorithms, and the object identification accuracy rate is higher. Now the systems have extended up to 98.5% accuracy and nearly fifty percent more accurate than humans at speedily responding to visual inputs. In the year 1950 experimentation had been started using CV and came to use commercially. The technique was first used in the year 1970 to differentiate between typed and handwritten text. Today the scenario has changed as it has lot more applications and by the year 2022, it is expected that the CV and hardware market will succeed.

In some level both CV and pattern recognition is same. A method is introduced to train a system, to understand visual data, to input images which are labeled, then subject to those techniques and algorithms that enable the computer to search for the patterns related to those labels.

For example, we may provide 1,000,000 images of dogs as input algorithms which allow them to analyze the colors of the images, the shapes, and the image border and so on. When it's completed, the computer will be ready to use its knowledge, if any other unlabelled objects is given then it identifies as dog.

1.3 OpenCV

The expansion of OpenCV is Open-Source Computer Vision Library. It's a library of programming functions, which is written in C++ and used to supply a standard infrastructure for CV applications and to speed up the utilization of machine learning perception within the products. OpenCV is a BSD-licensed, which makes OpenCV easy to use for commercial purpose as the source code is customized.

The library has nearly 2500 well-developed algorithms that include a widespread set of CV and machine learning algorithms. For recognizing faces and matching we use these algorithms. Sometimes it is also used to categorize objects, analyze actions of humans in videos, track movements in camera and moving objects and so on. Also, using stereo cameras to produce 3D point clouds, sew up images jointly to provide a high-definition image of an entire scene, find similar objects from the database, eliminate blue/red eyes from the photo of a human taken with flash light on, capturing eye movement, make out views and create markers to superimpose it with augmented reality. With thousands of people using OpenCV and downloading it, the library is employed broadly in research groups, companies, and by governmental bodies.

Next to well-known companies like Google, IBM, Microsoft, Sony, Toyota, and Honda, there are many startups like VideoSurf, Zeitera, etc. are extensively using OpenCV. OpenCVs have many applications like: A street of a city view images of TamilNadu, intrusion detection in surveillance video camera, monitoring radar equipments, helping robots navigate and devour objects, detection of road accidents in USA, creating a virtual painting app, conducting online classes in the pandemic situations, checking runways of airports, inspecting labels on products in factories and so on.

C ++ , Python, Java and MATLAB works well with OpenCV and provide the useful operation regarding projects and works really well with Android, Windows, Linux, Mac OS. Even though OpenCV is quite challenging to work through, but if anyone is acquainted with it, he can create variety of new projects. CUDA and OpenCL are two different frameworks which allow the use of GPU to general purpose tasks. CUDA provides access directly to GPU instruction set and parallel computing elements, whereas OpenCL writes programs that execute across heterogeneous platforms which contains CPU, GPU, FPGAs and other processors/ hardware's. There are over 400 algorithms that are composed off or supported by around 10 times as many functions.

2 Literature Review

Bouwmans, Thierry [1] have given comprehensive survey of various Background Modeling Methods discussed in various papers and patents, like Basic, Statistical, Fuzzy, Clustering, Neural Network, Wavelet, and Estimation Background Modeling. The given modeling techniques make use of background subtraction that result in the following: modeling, initialization, maintenance, foreground detection, choice of the feature size (pixel), and choice of the feature type. All these decisions facilitate and develop a robust background subtraction method to deal with important situations met in the video sequence. Using this survey, the author recommends classification such as intrinsic and extrinsic enhancements. The method of totaling spatial and temporal information to each step or process leads to the robustness of the initial model to life conditions.

Seki et al. [2] described online convention equipment which might be beneficial and transportable forces humans' that may also earn a living from home or journey on enterprise trips. However, some people might be embarrassed to present themselves when they are in certain private areas or open space. In a web convention, attendee's hope to see others' identity however they do not need to expose their personal history due to privacy concerns. A video contains two major components: one is objects or people and background, pointed by Chen Barrie et al [3]. This paper assumes that picture versions are prompted most effective with the aid of using shifting items (i.e., the heritage scene is believed to be stationary), however, its applicability is limited. In this paper, the proposed concept became a heritage subtraction approach that robustly handles diverse adjustments within the heritage. The approach learns the sequential

adjustments within the noted scene's heritage in phrases of distributions of scenery. This allows the particular method to discover items with the right sensitivity.

Beck et al [4] discussed the use of video telephony, which permits remote events to see and listen to one another, is becoming popular. The term 'video telephony' used here refers to the visible conversation used in each video and audio transmitted over a conversation network. When engaging in a video convention or factor-to-factor Video call, a player may also prefer to control the video exhibited to alternative contributors for privacy or various other factors. For example, the player won't need his or her face to be clearly visible to at least one or more of the alternative contributors. Removing the favored or undesired picture data from the received picture data can be used to shape filtered picture data and eliminate favored and/or undesired picture data. Lee [5] combined the filtered picture data with substitute picture data to shape composite picture data. Adaptive Gaussian combinations have been employed for modeling no stationary temporal distributions of pixels in applications related to video surveillance. Significant enhancements are proven on each artificial and actual video information.

Li et al [6] incorporated a set of rules in a statistical framework for history subtraction that leads to an advanced segmentation and overall performance in comparison with the popular methods. This paper offers a gadget for mechanically detecting and reading heritage video sequence. The movement primarily depends on sports activities, motion pictures indexing and imparting kinematic measurements to instruct and help, and to measure overall performance improvement. The gadget works in worse-to-better fashion. The movies contain the favored movement as summaries for widespread consumer viewing purposes. Morde et al [7] presented a foreground /background segmentation technique using Chebyshev probability inequality. The technique employs shadow detection, feedback from object tracking and classification for further filtering to improve the segmentation accuracy. Jodoin et al [8] introduced a new approach to background subtraction by means of local shape of tiny image sections. An image section centered on a pixel is modeled using the local self-similarity descriptor. The technique first develops a background model and then the local self-similarities between the background model and the subsequent frames to differentiate between background and foreground object. Post-processing is done to filter the borders of moving objects. The author claims that the foregrounds acquired are complete, even though shadows were included. Xiang et al [9] described an error analysis for background modeling and pixel labeling by using the probability for false alarm and miss detection. The authors analyzed both static and dynamic background modeling using Gaussian models. Zhong et al [10] presented a new foreground–background segmentation technique that clearly applies for non-stationary scenes and imprecise appearance for dynamic texture. The authors designed a model using Autoregressive Moving Average Model, Kalman filter algorithm to segment dynamic texture.

3 Implementation

Virtual Backgrounds are of great interest among employees that work remotely at present. With most of the working class being isolated currently because of the pandemic, people are required to attend video calls in order to carry on with their work. Some software tools for video conferencing allow setting a virtual background so that users can build a friendlier atmosphere for attending these calls. The aim of this undertaking is to take a video and determine the heritage and the foreground of the video, remove the heritage component, and update it with a different picture of digital heritage. In this undertaking, we will make use of the concept that the foreground will, in general, have colors extremely varied from that of the heritage.

3.1 Proposed Algorithm

Step 1: Import dependencies

Import the OpenCV and numpy Python libraries for the operations that we need to implement, which will help in image manipulation and working with indexes.

Step 2: Load the video from the local environment and initialize data

Declare a video variable to store the captured variable and upload video in the variable background Video which we then replace with the original Background.

Step 3: Create a mask

Create a mask for subtracting the video frame by frame and add the subtracted value into a new value and compare that with the absolute value.

Step 4: Invert the mask

Mask will be inverted and the background will become foreground and foreground will become background.

Step 5: Use the masks to extract the relevant parts from FG and BG

Using the properties of Foreground image and background image using mask, this helps for image subtraction and addition.

Step 6: Combine both the BG and the FG images

We combine the desired background and foreground image.

Step 7: Manual Control

We can break the session using ‘q’ key, capture new video using ‘d’ key and new background using ‘r’ key. Finally, will combine the background and foreground image and implement then execute it.

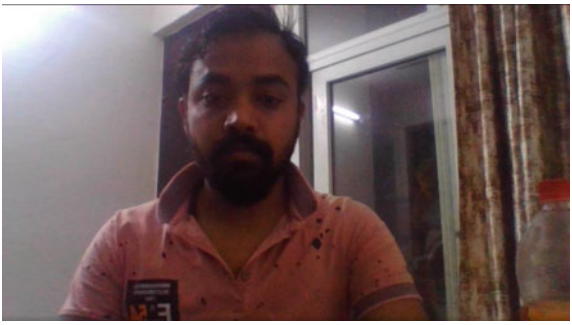


Fig. 1 Normal image



Fig. 2 Image after applying algorithm

4 Result and Discussion

The proposed algorithm is implemented by taking the image or video and modifying the background to produce the intended results. The foreground image is kept constant while the background image is replaced with the image of interest (Fig. 1).

In Fig. 2 as we can see from the output of the screen the person is sitting on a beach giving a presentation. Originally he is in his room. Using this proposed algorithm, a video of a beach is uploaded as an input, and the output we obtained is the person's background is a beach. In this way, we can upload a video of our choice.

5 Conclusion

In this paper, the background of a video can be changed without altering the foreground image of the video. Compared to the method introduced by Bouwmans Thierry [2], the proposed system works more efficiently and with the aid of Computer Vision, the method will produce better results with lesser execution time. We can

extend the scope of work by enabling censorship to ensure video quality and professionalism. Image processing can also be implemented to overcome problems in the background of the video by analyzing it and replacing required sections with the desired content.

References

1. B. Thierry, Recent advanced statistical background modeling for foreground detection-a systematic survey. Recent Patents Comput. Sci. **4**(3), 147–176 (2011). https://doi.org/10.2174/2212375911104030147
2. M. Seki, H. Fujiwara, K. Sumi, A robust background subtraction method for changing background. in *Proceedings Fifth IEEE Workshop on Applications of Computer Vision*, Palm Springs, USA (2000), pp. 207–213. https://doi.org/10.1109/WACV.2000.895424
3. C. Barrie, Q. Iris, C. Richard, Changing an online video meeting background in real-time using deep learning. Technical Disclosure Commons, (January 27, 2020)
4. A.J.G. Beck, C. Blair, A.W. Lang, P.T. McNamara, D.P. Thambiratnam, K.W. James, Customizable background for video communications, U.S. Patent No. US7227567B1 (2007)
5. L. Dar-Shyang, Effective Gaussian mixture learning for video background subtraction. IEEE Trans. Pattern Anal. Mach. Intell. **27**(5), 827–832 (2005). https://doi.org/10.1109/TPAMI.2005.102
6. L. Haojie, J. Tang, S. Wu, Y.D. Zhong, S. Lin, Automatic detection and analysis of player action in moving background sports video sequences. IEEE Trans. Circuits Syst. Video Technol. **20**(3), 351–364 (2009). https://doi.org/10.1109/TCSVT.2009.2035833
7. M. Ashutosh, X. Ma, S. Guler, Learning a background model for change detection. in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition* (2012) https://doi.org/10.1109/CVPRW.2012.6238921
8. J. Jean-Philippe, B. Guillaume-Alexandre, N. Saunier, Background subtraction based on local shape (2012). arXiv preprint arXiv:1204.6326. 10.1.1.749.3094
9. G. Xiang, T. Boult, R. Visvanathan, Error analysis of background adaption. in *Proceedings IEEE Conference on Computer Vision and Pattern Recognition.* CVPR 2000 (Cat. No. PR00662). vol. 1. (IEEE, 2000). https://doi.org/10.1109/CVPR.2000.855861
10. J. Zhong, S. Sclaroff, Segmenting foreground objects from a dynamic textured background via a robust kalman filter. in *Proceedings Ninth IEEE International Conference on Computer Vision* (IEEE, 2003)

Swear Words Replacement Suggestion System



S. Naveen, Mayank Singh, and S. Karthika

Abstract While giving the reviews the customers intentionally/unintentionally use the swear/bad words to express their disappointment to the service provider. Customer care representatives spend each day of their working lives dealing with a lot of angry customers and the casual use of curse words. Even when it is not any fault of their own, they have to be patient and help resolve issues with composure. This kind of interaction affects the mental health of the employees who have to work despite these unkind words, and it does not solve the problem rather it makes the world of the internet an unkind place. So, we want to make the internet savvy millennial aware that with a little effort, we could speak kindly to strangers, even in stressful scenarios. This paper proposes an application which helps users respect the person on the other side of a chat by offering an autocorrect option that replaces the swear word with the name of the related item for which user is complaining about.

Keywords Glove word embedding · Vectorization · Hyperparameters · LSTM · Random forest · Deep learning · Recurrent neural network · Swear words

1 Introduction

The anonymity provided by web, speech, and chat-based platforms can make us forget about the person on the other end of the line. According to the study, social media is a very common place for people to publicly share their views and communicate with others online [1]. Unfortunately, many people who engage online, whether on social media, forums, or blogs, run the risk of being harassed or abused by abusive language [2], which can have a negative impact on their online experience and the community

S. Naveen (✉) · M. Singh · S. Karthika
Department of Information Technology, SSN College of Engineering, Chennai, Tamil Nadu, India
e-mail: naveens17057@it.ssn.edu.in

M. Singh
e-mail: mayanksingh17047@it.ssn.edu.in

S. Karthika
e-mail: skarthika@ssn.edu.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_26

as a whole. The presence of social networking sites necessitates the detection of hateful messages created by users before they are released.

Unfortunately, reliably identifying offensive language is challenging since even the most basic solution (e.g., using keyword matching techniques) necessitates a list of swear words [3], which can be difficult to build and maintain [4]. Although swearword detection research is rapidly expanding, one of the current issues is that the majority of datasets are only available in English.

As a result, hate speech in other languages is not adequately detected, which could be harmful. This is also a challenge for organizations like Facebook, which can only detect hate speech in a limited number of languages (English, Spanish, and Mandarin). Although there are a few datasets available in other languages, they are all relatively limited in scale, as we've shown. As a result, our identification and substitution would be limited to a single language.

2 Literature Review

The detection of the toxicity in the conversational data, both traditional machine learning methods and advanced deep learning techniques, has been availed. The use of various classifiers, e.g. Decision Trees [1], Logistic Regression [5], Support Vector Machine models, or Ensemble Models are included in Traditional machine learning approaches.

The authors present a CNN model capable of detecting toxic tweets in their research paper [6]. Authors also use hashtags from tweets that are similar to toxic tweets to monitor the spread of toxicity over time. A number of previous studies looked at toxicity detection as a binary classification issue.

Despite the fact that Natural Language Processing (NLP) methods are used in the majority of solutions for automatic detection of offensive text [5]. According to the research work [6], there has been a recent trend towards using pure machine learning techniques like neural networks for that role. Furthermore, to achieve good classification model efficiency, the majority of current automated approaches rely on using pre-trained vectors (e.g., Glove, Word2Vec) as word embeddings [7]. As a result, our approach is limited to converting swear words into amusingly similar or rhyming words in the English language.

3 Proposed System

The system has the following major modules namely: Data collection, Machine and deep learning model, computing probability of offensiveness and GUI for user reviews (Fig. 1).

Data Collection

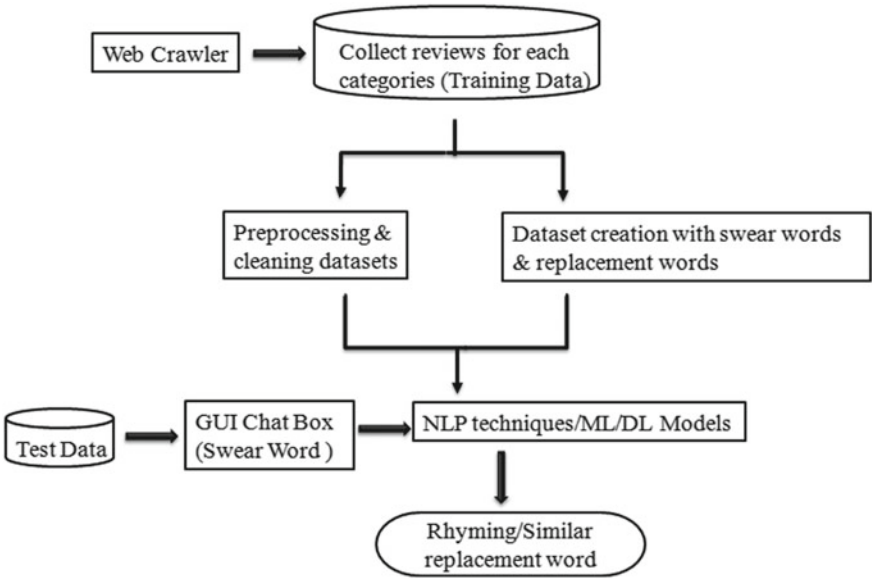


Fig. 1 Proposed system architecture

The data has been collected from scrapping the twitter, Wikipedia comments and YouTube comments. Then they have been combined together (Table 1).

If the text contains offensive language, then it is marked as 1 else marked as 0 in the column "Is_Offensive" in the dataset. Dataset containing the most commonly used swear words and similar/rhyming replacement words for each category (such as Food and Vegetables, Footwear and Clothes, Transport and Stationery) is created. The below table shows the few records of the dataset used for swear words replacement (Table 2).

Machine and Deep Learning Models

For detecting swear/bad words, two Machine Learning Models (Linear SVM and Random Forest) and one deep learning model (Recurrent Neural Network-LSTM) [8] are used for training the datasets. The Two major steps in Linear SVM are: (1)

Table 1 Final dataset

Dataset	Not offensive	Offensive	Total
Tweets	4,163 (16.8%)	20,620 (83.2%)	24,783 (100%)
Wikipedia	143,346 (89.8%)	16,225 (10.2%)	159,571 (100%)
Combined	147,509 (80%)	36,845 (20%)	184,354 (100%)

Table 2 Table containing the swear words and their replacement words

Swear words	Food and vegetables	Clothes and footwears
Fuck	Falooda	Frock
Fucking	Fruiting	Earring
Asshole	Aloo jhol	The sole
Shit	Shiitake	Shirt
Bloody	Biryani	jersey

vectorization and (2) training. Random Forest is also used to train the model so that we can compare the performance of various classification algorithms. Long Short-Term Memory (LSTM) [9] is also used here because LSTM is capable of learning long-term dependencies.

Computing Probability of Offensiveness

The trained model is used to detect the offensiveness in the customer reviews and the model will return the probability of offensiveness. If the value of probability is greater than 0.5, then it is considered as "offensive" else "not offensive".

GUI for User Reviews

The Graphical User Interface (GUI) for posting user review is created using HTML, CSS, JavaScript and Python. It is deployed using XAMMP server using CGI (Common Gateway Interface) which is used to exchange the information between the server and the client.

Data Pre-processing

The list of pre-processing rules shown in Table 3 is applied to the collected data [10].

Table 3 List of pre-processing rules

No	Rule	Description
1	Tokenization	Split a textual instance into smaller words
2	Lowercase conversion	Transform textual instances into lowercase letters
3	URL and hashtags removal	Removes the URL links and '#' symbol
4	Removal of punctuations and symbols	Remove punctuations and symbols including emojis and non-English characters
5	Lemmatization	Standard coreNLP is used to transform texts to its base form
6	Stopword removal	English stopword list provided by NLTK is used to remove stopwords like a, the, and, etc

Vectorization of Data

CV stands for Count Vector and this representation is often used in text mining. The vector is a measure of how frequently the word occurs in a document. CV converts the text documents to a matrix of vectors. The frequency of the word in a document is represented through the corresponding count occurrence for that vector.

Train-Test Split. The train-test split is helpful in estimating the performance of the model as we divide the dataset into two subparts and one subpart is used to train the model and the other subpart is employed to test the model. Here we have used two split ratios to evaluate the performance of the models and they are:

Train: 80%, Test: 20%

Train: 70%, Test: 30%

The deep learning model used here is Recurrent Neural Network (RNN) with glove Embedding. Global Vectors for Word Representation (GloVe) [11, 12] is predicated on matrix factorization techniques on the word-context matrix. Vector space representation yields a projection where words with alike contexts are grouped together. The advantage of using Recurrent Neural Network (RNN) is that it processes the elements as sequences and remembers the preceding elements.

The original dataset is split into training and testing data. The offensiveness of the reviews is determined by evaluating the prediction results of the testing data applied over the trained models.

4 Results and Discussions

The various observational results that were noted are presented in this section. The content and the contextual features have been applied on the pre-processed data and their results are shown. The machine learning and deep learning models that were discussed in the previous section were evaluated for different criteria and their results have also been discussed in the following sections.

Data Collection

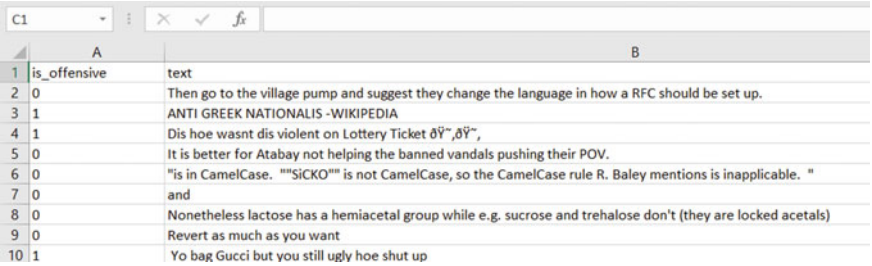
Data was gathered from the month of January and February in 2021 (Fig. 2).

Data Pre-processing

All the pre-processing rules described in the previous chapter are applied and the pre- processed text is displayed against the original text. The pre-processing rules are in the same order in which they are described in Fig. 3.

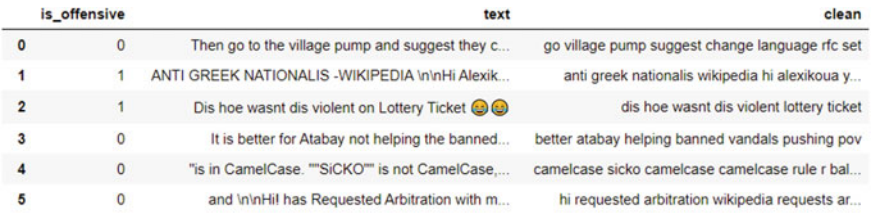
Evaluation of Metrics of Machine Learning Model

The evaluation metrics such as accuracy, precision and recall are used to evaluate the model. Here accuracy is considered to evaluate the model. The following shows the evaluation of metrics (Table 4):



	A	B
1	is_offensive	text
2	0	Then go to the village pump and suggest they change the language in how a RFC should be set up.
3	1	ANTI GREEK NATIONALIS -WIKIPEDIA
4	1	Dis hoe wasnt dis violent on Lottery Ticket ðŸ˜‚ðŸ˜‚
5	0	It is better for Atabay not helping the banned vandals pushing their POV.
6	0	"is in CamelCase. ""SiCKO"" is not CamelCase, so the CamelCase rule R. Baley mentions is inapplicable. "
7	0	and
8	0	Nonetheless lactose has a hemiacetal group while e.g. sucrose and trehalose don't (they are locked acetals)
9	0	Revert as much as you want
10	1	Yo bag Gucci but you still ugly hoe shut up

Fig. 2 File (.csv) containing the user review along with the class label



	is_offensive	text	clean
0	0	Then go to the village pump and suggest they c...	go village pump suggest change language rfc set
1	1	ANTI GREEK NATIONALIS -WIKIPEDIA \n\nHi Alexik...	anti greek nationalis wikipedia hi alexikoua y...
2	1	Dis hoe wasnt dis violent on Lottery Ticket 😂😂	dis hoe wasnt dis violent lottery ticket
3	0	It is better for Atabay not helping the banned...	better atabay helping banned vandals pushing pov
4	0	"is in CamelCase. ""SiCKO"" is not CamelCase,...	camelcase sicko camelcase camelcase rule r bal...
5	0	and \n\nHi! has Requested Arbitration with m...	hi requested arbitration wikipedia requests ar...

Fig. 3 File (.csv) containing cleaned text

Table 4 Table illustrates the evaluation metrics of the linear SVM model

Validation split	No. of records	Accuracy (%)
70:30 ratio	50,000	80.16
	100,000	80.28
	200,000	70.08
80:20 ratio	50,000	79.93
	100,000	79.93
	200,000	70.08

It has been observed that linear SVM [13] is found to perform better when the number of records used to train the model is less. When the number of records increases, the accuracy seems to be decreasing because with lesser number of records it can easily remember the offensive words used in the training records to predict the testing data and when the number of records increases it is unable to remember the offensive words and the prediction seems to be less accurate. Random Forest [14] is found to give better result than the Linear SVM as it is an ensemble method, and it creates multiple random decision forests to provide the accurate results. It achieves an accuracy of 93%. When Recurrent Neural Network (RNN) with glove embedding is used, it gives the maximum accuracy of 94.25%. The training observation details are listed in Table 5.

Inference from the table is that when the value of epoch is 7 we get the highest accuracy for the RNN model for 80:20 validation split and it remains the same till

Table 5 Table illustrates the evaluation metrics of the RNN

Validation split	Epoch	Accuracy (%)
70:30 ratio	3	93.37
	7	92.47
	20	92.24
80:20 ratio	3	93.57
	7	94.25
	20	93.55

Table 6 Table illustrates the evaluation metrics of various models

Validation split	SVM (%)	Random forest (%)	RNN (%)
70:30 ratio	70.08	93.4	93.37
80:20 ratio	70.08	93.45	94.25

the value of epoch is 15. After that when the value of epoch increases, the accuracy is found to be decreased (Table 6).

We infer that RNN model gives the highest accuracy of 94.25% for 80:20 validation split as it uses glove embedding to convert the text into vectors where closely related words are clustered together which makes easy for the model to detect the offensiveness in the text, thereby increasing the accuracy.

Swear Words Replacement

Now the user selects the category and enters the review. When the user clicks the post button, the model will detect the offensiveness in the review and then the offensive words are replaced by the corresponding category's similar/rhyming word, and it is displayed in the web page with offensive words marked in red colour. This is shown in the following figures (Figs. 4, 5, 6 and 7).

5 Conclusions and Future Work

Now a days we are getting most of the services like ordering food, clothes, electronic gadgets, cab, etc. through online. Sometimes order can take longer time to get delivered than it should have and technical issues can arise during payments. When this kind of issue arises, we are bent out of shape and we might post a review with hurtful language to show our disappointment and it hurts the customer care representatives who are trying to solve our issue. It isn't easy to assist change everybody and therefore the way they behave in a world filled with technology and the impersonal interface of chats. But, we can use technology as a tool to raise awareness about the need for a gentler speech on the internet. The major contribution is that by replacing the swear words in the customer reviews makes the people on the other side of the chat smile.

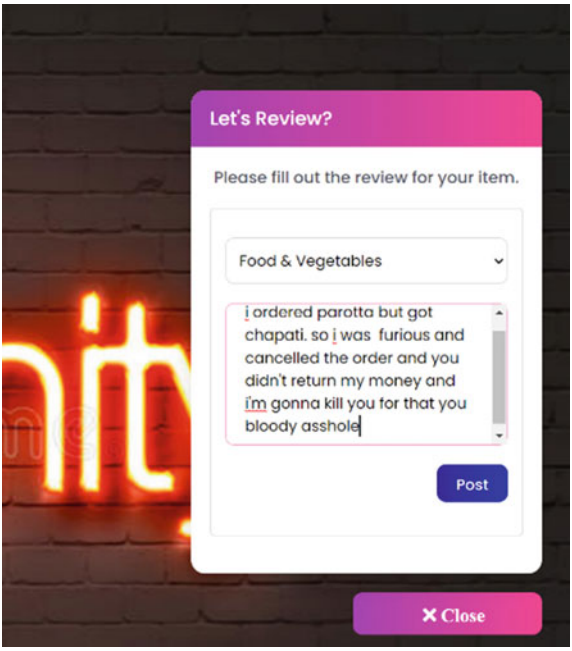


Fig. 4 Review form

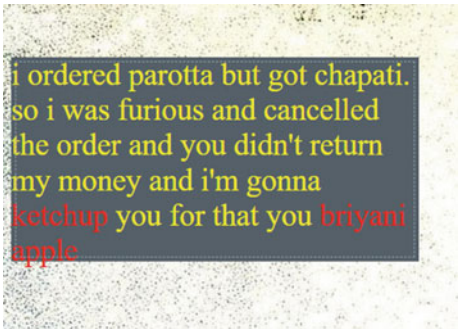


Fig. 5 Swear words replacement

The implementation of RNN model with glove embedding overcomes the weakness compared with individual models and achieves an accuracy of 94.25% as it uses glove embedding to convert the text into vectors where closely related words are clustered together which makes easy for the model to detect the offensiveness in the text thereby increasing the accuracy. It can be observed that Linear SVM and Random Forest reports the best performance with lesser number of records because with lesser number of records it can easily remember the offensive words used in the training records to predict the testing data. For future work, we plan to detect the swear words in regional languages like Hindi and Tamil. In addition to replacing the

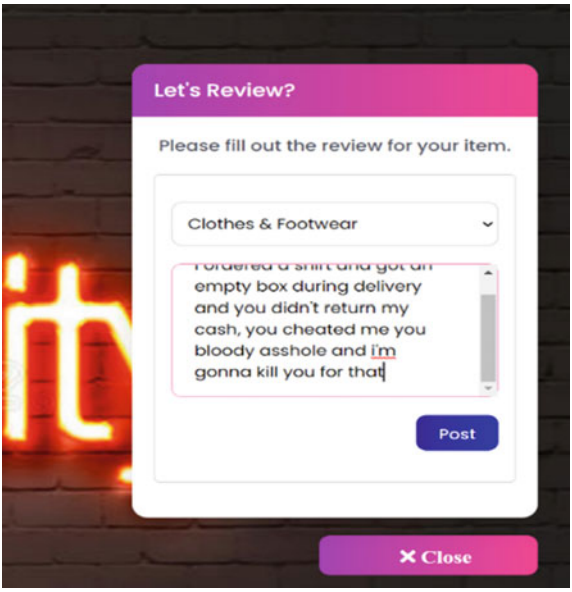


Fig. 6 Review form

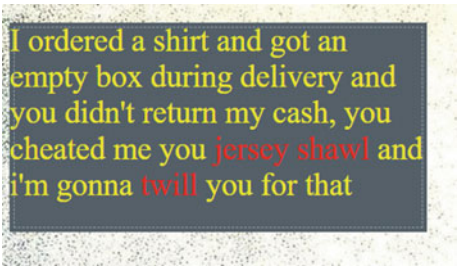


Fig. 7 Swear words replacement

swear words in the review, we also intend to calculate the score of offensiveness in the review.

References

1. P. Mykola, Detection of social network toxic comments with usage of syntactic dependencies in the sentences (2019)
2. G.K. Pitsilis, H. Ramampiaro, H. Langseth, Detecting offensive language in tweets using deep learning (2018). arXiv preprint arXiv:1801.04433
3. Profanity Detection, https://towardsdatascience.com/building-a-better-profanity-detection-library-with-scikit-learn-3638b2f2c4c2. Last Accessed 21 Feb 2021
4. M. Fahim, Is preprocessing of text really worth your time for online comment classification?. arXiv preprint arXiv:1806.02908 (2018)

5. M.A. Saif, A.N. Medvedev, M.A. Medvedev, T. Atanasova, Classification of online toxic comments using the logistic regression and neural networks models. in AIP conference proceedings, vol. 2048, no. 1 (AIP Publishing LLC, 2018), pp. 060011
6. S.V. Georgakopoulos, S.K. Tasoulis, A.G. Vrahatis, V.P. Plagianakos, Convolutional neural networks for toxic comment classification. in *Proceedings of the 10th Hellenic Conference on Artificial Intelligence* (2018), pp. 1–6
7. B. Snehal, T. Ghorpade, V. Mane, Comparative analysis of different word embedding models. in *2017 International Conference on Advances in Computing, Communication and Control* (ICAC3), (IEEE, 2017), pp. 1–4
8. S. Meredita, A.F. Rahman, M.D. Normansyah, A. Irawan, Offensive language detection using artificial neural network. in *2019 International Conference of Artificial Intelligence and Information Technology* (ICAIIT) (IEEE, 2019), pp. 350–353
9. LSTM Classification, https://machinelearningmastery.com/sequence-classification-lstm-recurrent-neural-networks-python-keras/. Last Accessed 12 Mar 2021
10. V. Maslej-Krešňáková, M. Sarnovský, P. Butka, K. Machová, Comparison of deep learning models and various text pre-processing techniques for the toxic comments classification. Appl. Sci. **10**(23), 8631 (2020)
11. P. Jeffrey, R. Socher, C.D. Manning, Glove: global vectors for word representation. in *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing* (EMNLP) (2014), pp. 1532–1543
12. Glove Embedding, https://nlp.stanford.edu/projects/glove/. Last Accessed 17 Mar 2021
13. LinearSVM Classification, https://aiiseasy.com/2019/06/09/text-classification-svm-naive-bayes-python/. Last Accessed 16 Feb 2021
14. Random Forest Algorithm, https://medium.com/@Synced/how-random-forest-algorithm-works-in-machine-learning-3c0fe15b6674. Last Accessed 19 Feb 2021

A Review of Deduplicate and Significance of Using Fuzzy Logic



V. Ranjith, M. K. Dhananjaya, P. Yamini Sahukar, M. Akshara, and Partho Sharothi Biswas

Abstract It is a common practice to integrate data from more than one resource in this age of cloud and big data. It has never been this easy in the past to get such huge chunks of memory in one place and allow processing at the present high speeds. In the process of integrating data from various sources, it is seen that there could be a number of repeated tuples in the big data. This hampers all analysis and also could lead to serious problems of false implications in analysis leading to absolute failure of purpose of data research. The paper presents a review of existing novel method commonly used in detecting duplicate tuples which are different but provide same meaning to the real world. The paper discusses the need and uses of fuzzy logic to detect such records with or without the intervention of the user for confirmation for deletion or removal of such records. The degree of similarity is the key review in this paper.

Keywords Amalgamation of cloud · Deduplication · Degree of similarity

1 Introduction

1.1 Fuzzy Set Theory

Fuzzy logic is based on fuzzy set theory. It is a methodology that recognizes the processes involved in human decision making with respect to indefinite situations where a gross generalization of the real world is not available and the circumstances do not lead or need to be educated by either by a zero or a one like Boolean logic. Since the inception of the concept, a number of systems have been in line of control by this logic as there are real-world problems without precise availability of data and without the need on precise output. Fuzzy logic controllers provide other means of approach for controlling real world processes which are not only complex but also cannot be judged in Boolean logic [1]. The fuzzy logic controllers provide

V. Ranjith · M. K. Dhananjaya · P. Y. Sahukar (✉) · M. Akshara · P. S. Biswas
Department of Computer Science and Engineering, Raja Reddy Institute of Technology, Bangalore, Karnataka, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_27

inference to the users of the system based on the 'condition-action' model where an 'IF–THEN' guideline is followed. These inferences are in the form of fuzzy outputs which are easy to understand and instruct the system. Fuzzy logic controllers are cost-effective, large range of operation are considered and are bespoke. Fuzzy would have to be configured through fuzzifier and also the reverse operation is performed by defuzzifier.

Data cleaning is a process of correcting, detecting inaccurate data before the data can be used for analysis, needs inaccurate data and redundant data to be replaced or removed from the database. This process is more tedious and time consuming in big data though it is easy to recognize/identify manually.

The main difference between the data cleaning data validation id that data validation is a process at entry time, where the data is cross checked with various predefined characteristics for entry data and cleaning is a process that is taken up either in backend or batch processed to identify and correct or eliminate data that adheres to qualifications of entry but not to consistency and convenience of required analysis [2]. The need for data quality arises from the fact that most of the analysis done on such data these days is used for machine learning which is mostly unsupervised. The trend is a welcome move in making the DSS self-sustainable and fast learning. However, it is also all that dangerous as it could be as one bad decision due to lack of quality data is hazardous. In all, this cleaning process faces a major problem of duplicate records which are a common problem these days due to the integration of records from different resources and different physical locations. Adding to the problem are the errors due to various data entry operators, confusing data types, lack of metadata, geographical and social integrations, etc. The duplicate records are different in computer's perspective but have a same meaning and are describing the same act of transactions. This poses challenges to elimination of duplicate tuples.

1.2 Fuzzy Logic

LA Zadeh first introduced the concept of Fuzzy sets in the year 1965, which can be conveniently termed as way of addressing uncertainty and inaccuracy using logic and provide representation mathematically [3]. It provides a representation for data and with indefinite boundaries mathematically leading to a better process of decision making [4]. The concept of fuzziness tries to represent the human style of decision making, which is far beyond the binary yes or no and a zero or one. The human brain has the capacity to consider the indefiniteness, data which has undefined boundaries, the ability to consider partial 'yes' and partial 'no', reasoning for incompleteness and ability to represent and make a decision based upon such data [5]. Fuzzy allows for real world terms like high, mid, low, very high, very low, little, lot, little dangerous, dangerous, very dangerous etc. this provides power to group the data with more accurate preciseness and deal efficiently with groups rather than individual badly qualified data.

In set theory, it is seen that an element is well defined and given an element it is possible to say if that element belongs to the set or not. This is definiteness which again leads to Boolean representation and a precise decision/inference. This mathematical function is so well defined that members are accurately identified. In fuzzy logic, this well-defined mathematical function is generalized to provide resulting 'fuzzy sets' [6]. In fuzzy sets, each element is defined by grade of membership, indicating the extent to which it belongs to the set. As in the real world, the grade of membership depends on the concept of universe of discourse set. Hence, grades of memberships are more subjective in nature and are more real world oriented or rather represent real world indecisive data which could be better scientifically represented and better handled.

Let $U = \{X1,X2,X3, \ldots Xn\}$ be the Universe of discourse set. Fuzzy set is defined from this set U as 'F' where $F = (F\ C\ U)$ is defined as the set of ordered pairs, where the degree of membership is defined by $\{(\text{xi}, \mu F(\text{xi}))\}$ where μA is a value between 0(non-member of the set) and 1(complete member of the set).

If different fuzzy sets are defined on the same universe of discourse, then form a partition on the universe of discourse set. The members of the set could be more conveniently described in a human language, which are called as the linguistic variables. The value of such linguistic variables would be words of the common language rather than numbers. The linguistic variables are defines as (X, T, U, G, M) where X is the name of the variable, T is the linguistic values, U is the Universe of discourse, G is the rule to give a name to the term T and M is the semantic rule which associates with each linguistic value X its meaning [7].

2 Review of Literature

Deduplicate can be defined as a procedure performed on the data to remove redundant data, thereby reducing the storage and increasing the efficiency and accuracy of data analysis [8]. This process can be an inline procedure whereby the input data before being entered into the database or the cloud could be checked for duplicity and then inducted into system as data or it could be a background process working on the storage medium after it is stored.

There are a number of deduplicate removal models, which act on the data either offline or inline to remove the duplicate records. There exist models which even act on encrypted data stored on cloud based on proxy re-encryption. In general, such models use access control and data integrity as their main tool for removing the duplicate records on the cloud [9]. There exist models using rule based to eliminate duplicate tuples in a database as well. These rules are built based on the context of the main wellbeing of the reason of creation of database most of the times. All these methods are significant in handling effectiveness of the data [10]. Generalizing all these methods helps us to integrate data in big data storage [11].

Deduplication is a necessary procedure before any analysis. It is seen in most of the cases big data stored on the cloud is a resultant of backup setup. Multiple

backups from different data sink and repeated full backups with unchanged data force the deduplication issues. Context-based rewriting is a method to minimize the redundancy. In this method, the latest fragments are shifted to older backups and are avoided for backup. The algorithm context-based rewriting [7] is based on this method. By selectively rewriting the duplicates it is demonstrated that a duplicate is reduced to 4–7% from 12–55%. The increase in writing time is nearly 1–5%. It is worth rewriting the duplicates, old copies, etc. The memory overhead is also small and temporary [12].

Optimization of cloud storage is also achieved by reducing the space. A secure fuzzy keyword search is used to search the fuzzy logic securely files from cloud storage based on approximation of key values [13]. Fuzzy keyword interface provides a user friendly environment on cloud. It also uses deduplication and private preserving fuzzy keyword search technique [14]. Fuzzy keywords are used in networks as well [15].

Deduplication based on text and multimedia data also exists. The data with corresponding taxonomies are used for analysis and understanding of data. Hence, these methods are useful for text, videos and images. The challenges that exist in such a decision support system development are also discussed in this paper providing suggestions for further work on removal of duplicate data [16].

Similar records detection is also carried out based on active learning-based technique [17]. The method uses active learners which actively select subsets of instances from data that is unlabeled. These records when labelled provide will deliver highest information gain. However, this technique needs good training sets and is not augmented to handle clouds. This problem of raining data can be handled by defining distance metric and an appropriate threshold for records that do not need training data [18]. Duplicate records form a cluster in this technique. On deduplication of either a single database or on a group of database will yield error-free data with minimal duplication.

Number of methods other methods are also proposed where in a cloud storage, to reduce integrity and storage, a predictable file is converted into an unpredictable file, and its security is subjected to an upgrade to provide better results [4].

3 Matching Techniques

The following are commonly encountered field matching techniques used for removal of duplicates in the real world. Some of them though are not commonly in use but are reviewed as they are the most effective techniques for the given set of data. It is worth noting some of the methods work best for specific data sets and sometimes need a combination of these along with other concepts to eliminate duplicates [19]. There are a number of concepts used along with these methods like the artificial intelligence, fuzzy logic, machine learning techniques, data analytics, etc. to deduplicate records. However, the following methods are an integral part in the models developed and hence the review.

Similarity metrics based on string comparison calculates the syntactic similarity of two strings labelled by the same name. String-based similarity matching can be broadly classified into three types: character-based similarity matching, token-based similarity matching and phonetic-based similarity matching. In character-based similarity matching, the similarity is measured based on the sequence and appearance of the characters. In token-based similarity matching, the strings are first the given two strings are tokenized and then their similarity is computed based on the two sets. In phonetic comparison, we obtain the quantitative analysis of pronunciation between the speech and spelling the word. Some of the other methods could be comparison between numbers where not much of emphasis id given as mathematical comparisons are strong enough to handle most of the situations, but in specific cases, a few algorithms exist. Anaphora resolutions are comparison of same entity where the words are different but the meaning is the same. Mirror detection is the process of finding the similar or identical webpages on the net. Active learning techniques use active learning rather than a static set of data. Active learners choose subsets of instances in the unlabelled data, which on labelling would deliver information to the distance-based learning supervised learning. Rule-based methods allow us to check for duplicates in database based on deduplication rules. These rules could use multiple fields, partial matches, phonetic matches or a combination of matching methods. Unsupervised learning avoids the burden of manual labelling. Clustering algorithms/techniques are used to group similar records and produce a comparison vector (Fig. 1).

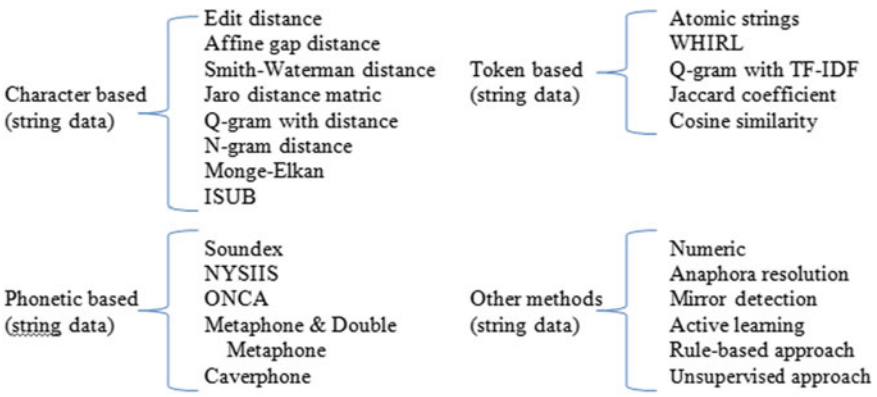


Fig. 1 Classifying matching techniques

4 Conclusion

It is seen that distance-based techniques need a good training set in which a correct threshold value is defined. It is possible in training sets to define the needed parameters, however, in real-world situations it is not appropriate to expect threshold value defined so easily, which would act as a major disadvantage. It is seen that in many research so far conducted are very specific and efficient to a particular set of data and the results begin to vary as we start changing data sets and generalizing the algorithms.

In this paper, we have presented a survey of the existing techniques popularly used in the real world for detecting duplicate entries in cloud and databases. From the survey, we draw objectives for our research. It is seen that a situation like a complete 'match' or 'no match' of 'yes' or 'no' or 0 or 1 is rare in the real world and hence a method which would address partial inclusions and partial exclusion is a necessity. The technique that adheres to such use cases is the fuzzy logic and hence the ways to use these deduplication methods along with Fuzzy and generalizing them based on the type of data defined in the database schema is needed. The main objective of further work would be to improve accuracy in cloud storage service, develop hybrid techniques using fuzzy logic and other methods of neural networks which provide better performance.

The paper provides an understanding of fuzzy logic duplicate elimination as the capability to specify rules in natural language enhancing faster development time, removing hard core processes, flexible rules and ease of use. Hence, further work to build and improve the efficiency, accuracy, flexibility, easy to use, easy to build constraints and generalized fuzzy model is the immediate need of research as the cloud technology flourishes.

References

1. S.D. Pochhi, P.V. Kasture, Encrypted data storage with de-duplication approach on twin cloud. Int. J. Innov. Res. Comput. Commun. Eng.
2. N.R. Venkat, R.N. Kushal, S. Sangam, Application of fuzzy logic in financial markets for decision making. Int. J. Adv. Res. Comput. Sci. **8**, 382–386 (2017)
3. B. lakshmi, N. Manikandan, M secured authorized de-duplication in distributed system. IJIRST Int. J. Innov. Res. Sci. Technol. **1**(9) (2015)
4. B. Choudhary, A. Dravid, A study on secure deduplication techniques in cloud computing. Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **3**(12) (2014)
5. A.P. Dempster, N.M. Laird, D.B. Rubin, Maximum likelihood from incomplete data via the EM algorithm. J. Royal Stat. Soc. Ser. B. **39**(1), 1–38 (1977)
6. N. Werro, *Fuzzy Classi Cation of Online Customers* (University of Fribourg, Fribourg, Switzerland, 2008)
7. Z. Yan, M.J. Wang, Protect pervasive social networking based on two dimensional trust levels. IEEE Syst. J. 1–12 (2014). https://doi.org/10.1109/JSYST.2014.2347259
8. M. Lillibridge, K. Eshghi, D. Bhagwat, Improving restore speed for backup systems that use inline chunk based deduplication. in *Proceedings 11th Usenix Conference File and Storage Technologies* (2013), pp. 183–198

9. Z. Yan, W. Ding, Y. Xixun, H. Zhu, R.H. Deng, Deduplication on encrypted big data in cloud. IEEE Trans. Big Data **2**(2), 138–150 (2016)
10. J. Jebamalar Tamilselvi, C. BrillyGifta, Handling duplicate data in data warehouse for data mining. Int. J. Comput. Appl. **15**(4), (0975–8887) (2011)
11. J. Li, Y.K. Li, X. Chen, P.P.C. Lee, W. Lou, A hybrid cloud approach for secure authorized de-duplication. IEEE Trans. Parallel Distrib. Syst. (2014)
12. L.A. Zadeh, Fuzzy sets. Inf. Control **8**, 338–353 (1965)
13. L.A. Zadeh, The concept of a linguistic variable and its application to approximate reasoning-I. Inf. Sci. **8**, 199–249 (1975)
14. Y. Pachipala et.al., Managing the cloud storage using deduplication and secured fuzzy keyword search for multiple data owners Int. J. Pure Appl. Math. (2018)
15. Z. Elaggoune, R. Maamri, I. Boussebough, A fuzzy agent approach for smart data extraction in big data environment. J. King Saud Univer.—Comput. Info. Sci. **32**(4), 465–478 (2020)
16. R. Kaur, I. Chana, J. Bhattacharya, Data deduplication techniques for efficient cloud storage management: a systematic review. J. Supercomput. Int. J. Pure Appl. Math.·(2018) Published: 20 December 2017
17. V. Subramaniyaswamy, S. Chendthur Pandian, A complete survey of duplicate record detection using data mining techniques. Info. Technol. J. **11**(8), 941–945 (2012)
18. C. Liu, X. Liu, L. Wan, Policy-based deduplication in secure cloud storage. in *Proceedings Trustworthy Computer Services* (2013), pp. 250–262. 1007/978–3–642–35795–4_32
19. M. Kaczmarczyk, M. Barczyński et al., in *Conference: Proceedings of the 5th Annual International Systems and Storage Conference* (SYSTOR'12) (Haifa, Israel, 2012)

SIoT (Social Internet of Things): A Review



Saima Shahab, Parul Agarwal, Tabish Mufti, and Ahmed J. Obaid

Abstract In the age of digital change, IoT is a crucial technological trend nowadays. It is expected that the number of IoT devices will rise by 25.1 billion by 2025. In the IoT family, there is a subset that is SIoT (Social Internet of Things), which is a relatively recent concept. And a method of integrating IoT with social networking. SIoT is a simulation of human-to-human and object-to-object social networks where Humans are called intellectual and relational objects. They build their social network to accomplish common objectives such as enhancing accessibility, success, and productivity, as well as providing the services they need. The main contribution of this review article is to understand the concepts of SIoT. SIoT can be best described by its architecture which includes its components, the relationship.

Keywords SIoT (Social Internet of Thing) · IoT (Internet of Thing) · Social networks · Social objects · Social relationships

1 Introduction

The IoT (Internet of thing) is a component of the future internet, and it can be described as a dynamic universal network infrastructure with self-configuring abilities based on interoperable communication protocols and standard, in which physical and virtual things have their own identities [1]. In IoT things are expected to become an active participant in business, information, and social processes [2]. Interactions with these 'smart objects' over the Internet, like inquiring and changing their state of any information related with them, which take security and privacy concerns into account management and the trust management between the objects [3, 4]. Many challenges are faced by developers to work with IoT system. Due to the variability of communication protocols, IoT systems are highly susceptible to multiple degrees

S. Shahab · P. Agarwal (✉) · T. Mufti
Department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India
e-mail: pagarwal@jamiahamdard.ac.in

A. J. Obaid
University of Kufa, Najaf, Iraq

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_28

of heterogeneity [5]. Then the social networking concept is used in the IoT model to effectively address the challenges which IoT environment faces. Accepting these social features for an IoT paradigm has resulted in the birth of a new concept of the social network of smart things, services, or both known as Social internet of Things (SIoT), which will undoubtedly meet the needs of users, developers, and designers. SIoT brings an idea of sociology into communication. So, the emerging IoT areas use sociological ideas to promote multimedia information propagation [6].

2 SIoT

The term "Social IoT" refers to the different objects that can be found in one section of an IoT platform's social network [7]. The IoT experiment was conducted by Pew Research Centre in January 2014, that about 74% of adults spend their time on social networking sites [8]. So the conversations about the growth of the IoT and Social IoT, along with its outcomes are very essential. And the main objective of SIoT is to take advantage of social relationships between objects in an IoT environment to encourage successful knowledge exploration, promote scalability, trustworthiness, and enhance the communication. For example, Household garbage is collected by garbage collectors on a particular route and a specific schedule. But on days where the volume of trash is more or less than average, the collection route and schedule may need to be changed suddenly. So, the solution is connecting sensors to garbage bins, real-time data on garbage cans can be transmitted through the network to the control center. The data obtained from sensors is processed and sent to the garbage collectors, enabling them to prioritize the collection of complete containers and travel more effectively along their collection routes. The City of Santander, Spain has already accepted this approach [9].

2.1 History of SIoT

It's only in the past few years that people have started to learn more about the "social" part of IoT [10]. Back in the mid-1990s, the concept of the Internet was that of an e- commerce, and information services network. But then came YouTube, Facebook etc. and the concept of IoT was first introduced in 1999 when Aston Kevin from MIT introduced the word "Internet of Things"[11, 12]. Like this, the battle with IoT is trying to find an exceptional publicity message about how it can specifically enrich the human lives. It has been argued that those who are linked to the social network will provide substantially more accurate to answers the complicated problems than a person alone [10]. This thinking and suggestion is further seen as part of the late trend and redesigns the concept of IoT into SIoT. So, the SIoT is a "modern miracle moment for science"' Social networking sites, and it has drawn a vast number of researchers from a few regions.

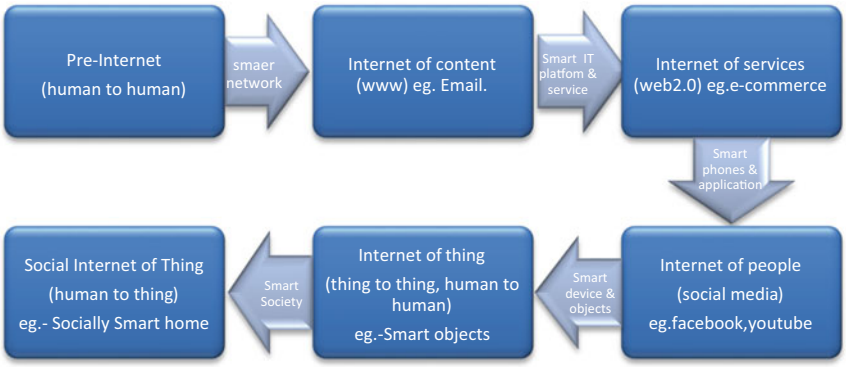


Fig. 1 Evolution of SIoT

2.2 SIoT: The Next Logical Step?

As we know the future ubiquitous computing will set in motion in a wide range of smart services and applications that will address the many challenges that individuals and organizations face in their everyday lives by enabling the people and things to be connected to anyone or anything, and anywhere, at any time [13]. With 'social networks' worlds is conceivable and power is growing. Currently, it's the first notion of the creation of SIoT derives from 2000 [14], SIoT mimics the nature of human social networks and explains how to connect and select friendships or choose a friend of a friend (FoAF) amongst various items to help and deliver a variety of high-quality services [15]. Then in 2001, Holm Quist et al. [16] became the first to bring forth the idea of social interaction between the devices of the IoT system [17]. Figure 1 Describes the Evolution of SIoT from the Pre-Internet (human to human communication).

3 Components of SIoT

The fundamental components of SIoT are: Architecture, Relationship Management, Trust /trustworthiness Management.

3.1 Architecture of SIoT

While there is no uniform architecture for SIoT, most publications suggested a three-tier architecture that includes. The base/object layer includes a database for storing

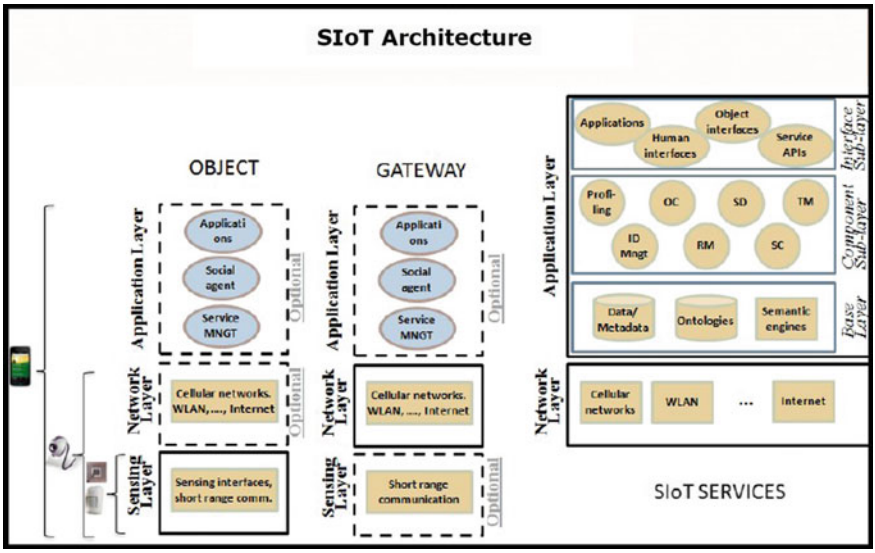


Fig. 2 Architecture of SIoT (Luigi Atzori 2012) [17]

data and handling a database on ontologies, semantic engines, and communications [18]. Next, the middle/ composite layer, this layer takes care of the interaction like object-toobject, social to-social, or object-to-social interactions in the pervasive setting. It also support tools for the basic and satellite components [23]. Then the upper/ application layer that ensures user engagement with SIoT applications. All consumer's applications and the interaction is conducted by the multimedia tools like audio, text, Service Programming Interfaces, Social Relationship Model, and Social Presence. Finally, the human is dedicated to communicating between different instances with SIoT servers to update their profile and the partnership between friends to discover/request services on the social network [18] (Fig. 2).

3.2 Relationship in SIoT

Relationships in a SIoT system can be either a User-to-Object Relationship or an Object-to-Object Relationship, depending on their specific affiliation. To have a SIoT application, the relationship types play a crucial role in communication and depend on the domain of an application. And these relationships are build and modified based on the characteristics of the objects.

User-to-Object Relationship

(OOR)Ownership Object Relationship it occurs between heterogeneous objects in Which the consumer of all objects is same, where the objects belong to the same

user. (SOR)Social Object Relationship here objects interact socially and the owner of the objects are different and come into contact with each other like sensors/objects belonging to friends in the social network [19]. (SIBOR) Sibling Object Relationship shall be formed between objects belonging to family member or friends. (GSTOR) Guest object relationship is occurred between things owned by users in a guest position.

Object-to-Object Relationship

(POR)Parental object relationship describes the relationship between the related objects unchanged over time. It occurs between homogeneous items that are normally from the same output batch. These items are all manufactured by the same company and were created about the same time. (CLOR) Colocation Object Relationship determined where objects live at the same location, in this relationship occurs between objects that are either homogenous or heterogeneous, but often in the same location, such as sensors, augmented objects, actuators, and other smart city. (CWOR) Cowork Object Relationship formed by products that work together to provide services for a shared IoT application in which smart objects collaborates like sensors, alarm at home [20]. (STGOR) Stranger Object Relationship occurs between objects that come into contact with each other in public or on the go. (GOR) Guardian Object Relationship, in which a vehicle's On-board Unit (OBU) become a kid to the super objects of roadside units (RSU), giving a new hierarchical relationship a special meaning. (SVOR) Service Object Relationship is created between the objects for coordinating the same service composition to fulfill the service request [21, 22].

3.3 Trust Management

Trust management is very important for SIoT models which deals with communication between the devices and humans and the lack of trust management leads to the loss of privacy issues, security, and accessibility, etc. objects should only share data and resources with items that are trustworthy to have a secure relationship, and a primary security goal in the SIoT is to distinguish between benign and malicious devices resulting in enhanced protection and safety of SIoT networks [23, 24].

4 Literature Survey

In [25], the authors described a new definition of social IoT as an all-encompassing interaction paradigm for sharing thoughts on the web of devices. In [26], the vision of Speaking Objects "things" communicating by argumentation was presented to demonstrate how various ways of human dialogue naturally meet Sit's cooperation and coordination requirements. In [27], it discusses potential IoT security studies and future threats for researchers to learn about and lead to their resolution. In [28],

they have proposed a shared platform for virtualization of the physical objects and making them accessible in the cyber-world while ensuring resource sharing, looked at the virtual object management, and the selection process for the SIoT platform and proposed a QoSaware object selection method to find the best service at the right time. In [29], so as to shorten the search procedure for a node in social networks, they suggested residual energies. This approach allows nodes in a constraint network to dynamically build a social network. It is a balance of skills in the collection of friendships and encourage rapid search. And the nodes decide to select the optimum path. As a result, the social network achieved is fully navigable and improves the network life. In [30], the authors they have built a social network, which are based on the social relationship with smart devices, called the social strength prediction model (SSPM), which indicates the social relationships among intelligent devices and predicts the strength of the relationships using co-usage data of the objects. In [31], the authors have focused on the KDI, a JTBbased Knowledge-based model, has provided much improved recommendations based on a consistent belief filtering system and the user input module embedded into the KDI platform. Which improves the quality decision in SIoT. In [32], they have suggested a new model for computing the trust between SIoT nodes that uses first-hand observation (direct trust) and second-hand advice (indirect trust), consistency, and node reliability. In [33], the authors describe a subjective trustworthiness management model that expands on the proposed solutions for P2P networks. They use feedback mechanism, integrity, consistency of the nodes, and assess the extent of confidence. Preliminary calculations demonstrate the advantages of the proposed model for the isolation of virtually every malicious node in a network. In [34], they have experimentally analyzed the object of SIoT network navigability. So, they first created nearby candidate objects based on their physical background, and interactions, in the real world, in social communities to enhance search path length. In [35], it considers the special OS specifications of IoT applications. The specific operating system (OS) selection for hardware devices in different applications is much more difficult so the best-suited operating systems for specific hardware platforms, device situations cannot be efficiently handled.

Advantages of SIoT:

- In SIoT, objects can crawl the IoT and use social relationships to find utilities and resources, this gives a scalable approach that is meant to be dependable and most notably and frees humans from doing so.
- The SIoT model offers a framework for the IoT that is close to human centric social networks in terms of networks, scalability, and services [36].
- It enables us to create a trustworthy relationship between objects and the information by holding the interactions between devices or objects that are “friends” [37].
- The current social network analysis tools could be extended and reused to fix all the issues related to SIoT, and the network structure can be checked by revealing the implicit correlation and treads among the objects [38].
- The SIoT will help recommender systems to locate related objects more quickly and even predict potential interactions between them [39].

Challenges in SIoT:

- Data Management huge amount of data should be, collected, organized and stored.
- Interoperability, Scalability (it should be flexible).
- Trust management (Lack of privacy and security).
- Heterogeneity (it should be diverse in character).
- Fault tolerance should be handy to SIoT devices. And E-Waste.

Application of SIoT:

- Social Gamification for improving engagement. Keeping track of industrial plants, environment. Administration facilities (like escalator and energy).
- Smart health-care services [40]
- In charge of smart houses. (Like providing automation and identification of co text.). Virtualized platforms, Naming services (like DNS), and conversion are also treated.
- Coordination strategies in a cooperating system in which cases, social entities, places, and data cohesively interact with one another.

5 Conclusion

This paper has extensively surveyed the SIoT (social internet of things) for beginners who are involved in SIoT Studies, as this paper will give you a clear view and ideas about the SIoT Its architecture, relationships, and trust management and applications and challenges implemented related to SIoT. However, objects create a network and behave intelligently to perform activities via sensors. These SIoT devices Sense their tasks and communicate with other devices if needed, extends their networks. In future work, we will Propose and discuss a framework that shall enable us to tackle the privacy and security issues, It is an important Issue related to SIoT need to be resolved. the SIoT system socialize with other technologies to achieve better results for complex problems like data handling, trustworthiness through collaboration with other technologies like machine learning, artificial intelligence, fog computing etc.

References

1. A. Kevin, That 'Internet of Things' things: in the real world things matter more than ideas. RFID J. (2009). http://www.rfidjournal.com/articles/view?4986(2009)
2. A. Khanna, S. Kaur, Internet of Things (IoT), applications and challenges: a comprehensive review. Wirel. Pers Commun. **114**, 1687–1762 (2020). https://doi.org/10.1007/s11277-020-07446-4
3. D. Kumar, T., Mufti, S.S Suhail, Internet of Things (IoT): a review from cloud prospective, in *1st International Conference on ICT for Digital, Smart and Sustainable Development,* vol. 1, pp. 76–82 (2019)
4. S.S. Sohail, T. Mufti, N. Sami, A Review paper on internet of things (IoT) Indian J. Appl. Res. **9**, 8 (2019)

5. A. Khelloufi, L. Atzori, R., Huang, H. Ning, et al., A Social-Relationships based service recommendation system for SIoT devices. IEEE Internet of Things J. **8**, 1859–1870 (2021). https://doi.org/10.1109/JIOT.2020.3016659
6. P. He, T. Tang, Community-Oriented multimedia content maximization mechanism in social Internet of Things. IEEE Access, 8, 1–1(2020). https://doi.org/10.1109/ACCESS.2020.2970453
7. https://www.gartner.com/document/2625419?
8. https://www.pewresearch.org
9. https://www.thesmartcityjournal.com/en/
10. http://postscapes.com/internet-of-things-history
11. N.B. Truong, H. Lee, B. Askwith, G.M. Lee, Toward a trust evaluation mechanism in the Social Internet of Things. Sensors. **17**, 1346 (2017). https://doi.org/10.3390/s17061346
12. N. Huansheng, T. Laurence, Y.Z. Yang, Y. Lu, The Internet of Things: from RFID to the next-generation pervasive networked systems. CRC Press, vol. 1 (2008)
13. A.M. Ortiz, D. Hussein, S. Park, S.N. Han, N. Crespi, The cluster between internet of things and social networks: review and research challenges. IEEE Internet Things J. **1**(3), 206–215 (2014). https://doi.org/10.1109/JIOT.2014.2318835
14. B.K. Tripathy, D. Dutta, C. Tazivazvino, On the research and development of social ,Internet of Things. Springer, p.8, (2016). https://doi.org/10.1007/978-3-319-30913-2_8
15. L. Atzori, A. Iera, G. Morabito, M. Nitti, The Social Internet of Things (SIoT)—When social networks meet the Internet of Things: concept, architecture and network characterization. Comput. Netw. **56**(16), 3594–3608 (2012). https://doi.org/10.1016/j.comnet.2012.07.010
16. L. Atzori, A. Iera, G. Morabito, SIoT: Giving a social structure to the Internet of Things. IEEE Commun. Lett. **15**(11), 1193–1195 (2011). https://doi.org/10.1109/LCOMM.2011.090911.111340
17. L.E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, H.W. Gellersen, Smartits friends: a technique for users to easily establish connections between smart artefacts. Springer, Heidelberg. **2201**, 116–122 (2001). https://doi.org/10.1007/3-540-45427-6_10
18. M.S. Roopa., R. Santosh, R. Venugopal, S. Iyengar, L. Patnaik et al., Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions. Comput. Commun. **139**, (2019). https://doi.org/10.1016/j.comcom.2019.03.009
19. A. Rehman, A. Paul, M. Gul, H. Junaid, S. Won-Hwa, et al., Exploiting Small World Problems in a SIoT Environment. Energies. **11**, 2089 (2018). https://doi.org/10.3390/en11082089
20. G.X. Lye., W.K. Cheng., T.B. Tan., C.W. Hung, Y. Chen., User trajectory analysis within intelligent Social Internet-of-things (SIoT). 1–2 (2019). https://doi.org/10.1109/ISPACS48206.2019.8986239
21. https://designwebkit.com/web-and-trends/social-iot/
22. https://understandingecommerce.com/a-new-era-of-iot-the-social-iot-social-network-oft hings/
23. R. Malekshahi, A.M. Rahmani, A. Sahafi et al., Social Internet of Things: vision, challenges, and trends. Hum. Cent. Comput. Inf. Sci. **10**, 52 (2020). https://doi.org/10.1186/s13673-020-00254-6
24. M. Nitti, R. Girau, L. Atzori, Trustworthiness management in the Social Internet of Things. IEEE Trans. Knowl. DataEng. **26**, 1253–1266 (2014). https://doi.org/10.1109/TKDE.2013.105
25. H. Lee, J. Kwon, Survey and analysis of information sharing in social IoT, in *8th International Conference on Disaster Recovery and Business Continuity (DRBC)*, pp. 15–18 (2015). https://doi.org/10.1109/DRBC.2015.13
26. M. Lippi, M. Mamei, S. Mariani, F. Zambonelli, An argumentation-based perspective over the social IoT. IEEE IoT J. **5**, 2537–2547 (2018). https://doi.org/10.1109/JIOT.2017.2775047
27. F. Raddad, R. Jayabrabu, M. Dinesh, An evolutionary study on the threats, trust, security, and challenges in SIoT (social internet of things). Mater. Today Proc. 2214–7853 (2020). https://doi.org/10.1016/j.matpr.2020.09.618
28. Z. Shamszaman, M.I.Ali, Enabling cognitive contributory societies using SIoT: QoS aware real-time virtual object management. J Parallel Distr. Comput. (2018). https://doi.org/10.1016/j.jpdc.2018.09.007

29. A. Zannou, A. Boulaalam, Nfaoui, SIoT: a new strategy to improve the network lifetime with an efficient search process. Future Internet **13**, 4 (2021). https://doi.org/10.3390/fi13010004
30. J. Jung, S. Chun, X. Jin, K. Lee, Quantitative Computation of social strength in social Internet of Things. IEEE Internet Things J. **5**, 4066–4075 (2018). https://doi.org/10.1109/JIOT.2018.2869933
31. W.K. Cheng, A.A. Ileladewa, T.B. Tan, A personalized recommendation framework for social Internet of Things (SIoT), in *International Conference on Green and Human Information Technology (ICGHIT)*, pp. 24–29 (2019). https://doi.org/10.1109/ICGHIT.2019.00013
32. M. Kowshalya, M.L. Valarmathi, Dynamic trust management for secure communications in social internet of things (SIoT). Sādhanā. **43**, 136 (2018). https://doi.org/10.1007/s12046018-0885-z
33. M. Nitti, R. Girau, L. Atzori, A. Iera, G. Morabito, A subjective model for trustworthiness evaluation in the social Internet of Things, in *IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications-(PIMRC)*, Sydney, NSW, Australia, pp. 18–23 (2012). https://doi.org/10.1109/PIMRC.2012.6362662
34. M.S. Roopa, D. Valla, R. Buyya, K.R. Venugopal, S.S. Iyengar, L.M. Patnaik, SSSSS: search for social similar smart objects in SIoT, in *Fourteenth International Conference on Information Processing (ICINPRO)*, vol. 35, pp. 1–6 (2018). https://doi.org/10.1109/ICINPRO43533.2018.9096686
35. B. Afzal, M. Umair, G.A. Shah, E. Ahmed, Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges. Futur. Gener. Comput. Syst. **92**, 718–731 (2019). https://doi.org/10.1016/j.future.2017.12.002
36. L. Militano, M. Nitti, L. Atzori, A. Iera, Enhancing the navigability in a social network of smart objects: a shapley-value based approach. Comput. Netw. **103**, 1–14 (2016). https://doi.org/10.1016/j.comnet.2016.03.007
37. Y. Sun, H. Xu, E. Bertino, D. Li, User preference based link inference for social network, in *2016 IEEE International Conference on Web Services (ICWS)*, pp. 188–195, (2016). https://doi.org/10.1109/ICWS.2016.32
38. N.M. Ahmed, L. Chen, An efficient algorithm for link prediction in temporal uncertain social networks. Inf. Sci. **331**, 120–136 (2016). https://doi.org/10.1016/j.ins.2015.10.036
39. L. Yao, Q.Z. Sheng, A.H. Ngu, X. Li, Things of interest recommendation by leveraging heterogeneous relations in the internet of things. ACM Trans. Internet Technol. **16**, 1–5 (2016). https://doi.org/10.1145/2837024
40. P. Agarwal, S.I. Hassan, S.K. Mustafa, J. Ahmad, An effective diagnostic model for personalized healthcare using deep learning techniques, in *Applications of Deep Learning and Big IoT on Personalized Healthcare Services*. IGI Global, pp. 70–88 (2020). https://doi.org/10.4018/978-1-7998-2101-4.ch005

STAT Simple Text Annotation Tool (STAT): Web-based Tool for Creating Training Data for spaCy Models



Darshita Kumar, Kshitija Choudhari, Pooja Patel, Shambhavi Pandey, Aparna Hajare, and Shubham Jante

Abstract In machine learning, text annotation is used to train models. Annotation is a precursor to named entity recognition (NER) in natural language processing problems. It is the labeling or highlighting of certain keywords, phrases or sentences through means of tags to help learning models better understand the complexities of human languages. During the annotation process, the features of the dataset are marked up using metadata tags. Annotation tools can make this process easier for users, reducing manual labor involved. A simple web tool has been developed which allows only authenticated users to manually upload and annotate text files and download the output in JSON format for internal use by the employees of optimum data analytics to prepare training data for spaCy models. Its UI is simple and intuitive, making it easy to use by the average user for NLP tasks. This paper discusses in detail about the need for STAT and its implementation aspects.

Keywords Text annotation · Named entity recognition · spaCy · JSON · Natural language processing

1 Introduction

Text annotation [1] is an aspect of natural language processing. It is not enough to provide computers with raw data, and it has to be prepared in such a way that computers can draw inferences and find patterns within the data. In text annotation, elements of the dataset are marked up using tags. Such that, machines can easily recognize the crucial words in a sentence. Text annotation is an essential requirement for preparing training datasets that can be used for NLP models. Due to the intricacy and complexity of human languages, labeling the keywords in each statement

D. Kumar (✉) · K. Choudhari · P. Patel · S. Pandey · A. Hajare
MKSSS's Cummins College of Engineering for Women, Pune, India

A. Hajare
e-mail: aparna.hajare@cumminscollege.in

S. Jante
Optimum Data Analytics, Pune, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_29

is paramount to ensuring that entire statements are understandable to the learning models.

One of the main applications of text annotation is named entity recognition (NER), i.e., the process of information extraction, chunking, and identification. Common categories that are used for this type of text annotation include organization, location, geopolitical entity, numerical values, month or time, and day of the week. It trains machine learning models to quickly recognize targeted entities in raw text-based data.

To perform text annotation, there is a need for a tool that is user-friendly and easy to understand. The tool should allow for the creation of custom entities, as opposed to standard predefined entities. It should let the user upload and delete text files for annotating and easy downloading of output files in the required format. STAT is the tool developed to meet these requirements.

The JSON output produced by STAT is provided as training data for "spaCy" [2] models. spaCy is a free open-source library for natural language processing in Python. It features named entity recognition, part-of-speech tagging, dependency parsing, word vectors, lemmatization, sentence boundary detection, tokenization, similarity, text classification, rule-based matching, training, and serialization. This results in spaCy being widely used for production-level code. STAT produces output in the form of JSON data which contain both content along with the tagged entities. This output can be directly fed to spaCy models as training data. Hence, STAT is extensively useful for creating training data for "spaCy" models. Figure 1 shows the simple user interface of STAT.

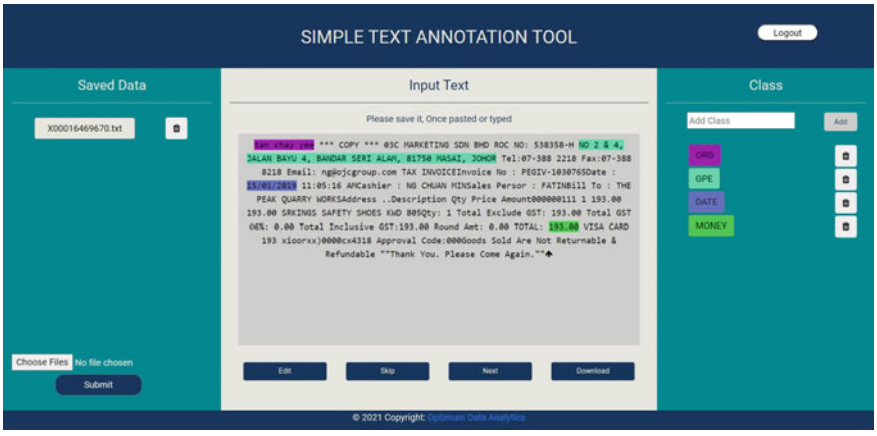


Fig. 1 Example of live annotation using STAT

2 Background

The presently available text annotation tools leave a lot to be desired like a simple user interface, ease of uploading multiple files, and download of annotated text. There is a requirement for a beginner-level tool that can be used without the need for extensive knowledge of the text annotation process which simultaneously has the features required to create annotated entities in JSON format. STAT was developed with the following key points in mind.

2.1 Custom Entity Classes

STAT allows users to create custom entities to label text files as per their requirements. There are no predefined entity classes.

2.2 Easy Upload and Deletion of Text Files

The process of upload and deletion of text files is intuitive and easy for the first time users to understand.

2.3 Easy Creation and Deletion of Entity Classes

The process of creation and deletion of custom entity classes is intuitive and easy for the first time users to understand.

2.4 Beginner-Level Friendly

STAT is simple to use because of its easy to navigate interface. The sections of the tool are self-explanatory. Furthermore, the landing page of the web app has instructions as to how one can use the tool.

2.5 For Internal Use

STAT was developed specifically for use by the employees of optimum data analytics.

3 Implementation

The front-end user interface of the tool is implemented using HTML5, CSS3, JavaScript, and Bootstrap4. The jQuery library of JavaScript has been used for easy implementation of JavaScript functionalities. The client communicates with the backend flask server using asynchronous JavaScript and XML (AJAX) which allows asynchronous messaging.

The following gives us the detailed description of the implementation of each module.

3.1 Login Module

For creating a secure tool which can only be accessed by intended users, the login functionality is implemented using Google Login API, Google APIs use the OAuth 2.0 protocol for authentication and authorization. Once a user comes to our application and presses the Google Login button, they are redirected to choose a Google account. Google ensures that the user has consented to pass along their email along with other information to our application. This is the authorization step of Google OAuth. When the user gives their consent, Google sends back some information to STAT that can be referenced later, effectively logging the user in.

3.2 Logout Module

The user can log out from the tool with the help of the logout button available in the upper right corner of the tool. Once logged out, the user returns to the landing page of the application.

3.3 Class Creation/Deletion Module

For creating custom entities, the user can utilize the rightmost pane of the tool. Entities with unique names can be created and also be deleted, if required. JavaScript arrays are used to store the entity names, and “random” function is used to generate the random colors for specifying the entities.

3.4 Database Module

An sqlite3 database is connected to STAT where the user can upload and delete text files. The files present in the database are visible in the left pane of the tool UI. When there is a file upload, an AJAX call is made to the flask server which uploads the data to the database and updates the user interface to display the file names, asynchronously. Once the file is annotated, the user can remove it from the database. The sqlite3 database stores the file name and the data of the file in the form of a blob. It is a centralized database which is shared by the authorized users of the tool.

3.5 Editor Module

The middle pane, as seen in Fig. 1, is where the user gets to annotate the text. The algorithm to find the start and end position of the highlighted entity is written in JavaScript. The file is then downloaded in JSON format.

4 Features

STAT aims to overcome the shortcomings of the existing tools described in Table 1. It does so with the help of five distinct features, and each of which have been described below.

Table 1 Shortcomings of existing tools

Tool name	Limitation
Brat	Annotating significantly longer text spans (i.e., paragraphs) turns out to be really inconvenient. The presentation of the user interface of the text file in brat is not necessarily the same as its original formatting [3, 4]
Docanno	Not suitable for all training models, used specifically for training arcgis.learn models Not beginner-level friendly Does not support data files with blank lines or blank fields [4, 5]
Inception	Requires that the user create an account (if they do not want to use a demo account) as a prerequisite to using the tool Complex interface with a lot of complex features which may be overwhelming for beginners [4, 6]

4.1 Multiple File Uploads

This text annotation tool allows users to upload single/multiple input text files at once. This allows the user to choose the text files from their local device that they want to annotate. The user does not have to upload a single file one at a time which saves a lot of time and makes the annotation process faster for the user. The user is only able to upload text files from their machine eliminating the chance of errors on the database side.

4.2 Security

The tool is accessible only to authorized users. It is secured with Google login, so only permitted Google accounts can access the tool.

4.3 Custom Entity Creation

The tool allows the creation of custom entities in order to annotate data in text files.

4.4 Download of Labeled Entities

STAT allows the download of labeled entities in the uploaded text in JSON format. The reason we require the output data in JSON format is so that we can parse the data and convert it to spaCy format with ease. The advantage with JSON format is that it can be parsed in any environment, and changes to this format can be made in very few edits to convert it to a different format.

4.5 Supports ASCII Format

The tool allows users to upload data in ASCII format, which accounts for special characters in texts.

5 Conclusion

Simple text annotation tool was created out of a need for an annotation tool that specifically met our project requirements, i.e., easy to understand user interface, creation of custom entities, producing output files in JSON format, and features that the currently available tools lacked.

6 Future Scope

The tool can also have additional features for preprocessing of the input data; for example, there can be an optical character recognition step performed if the user wants to upload an image file as input which will convert the image to text file and then be used for annotation. There can be an addition for the different format of input files available for annotation like jpeg, doc, and docx in the future scope.

References

1. L. Ambalina, (2019). https://lionbridge.ai/articles/an-introduction-to-5-types-of-text-annotation/
2. Spacy, (2020). https://spacy.io/
3. Brat, (2020). https://brat.nlplab.org/
4. F. Gringel, (2020). https://dida.do/blog/the-best-free-labeling-tools-for-text-annotation-in-nlp
5. Doccano, (2021). https://doccano.herokuapp.com/
6. Inception, (2021). https://inception-project.github.io/

Credential-Based Authentication Mechanism for IoT Devices in Fog-Cloud Computing



Hala S. Ali and R. Sridevi

Abstract While the number of devices is potentially increased in IoT system, cloud computing will face several challenges such as mobility support, distribution and location awareness, transmission delay, as well as the security threats. Substantially, fog computing is recently introduced as an extension of the cloud to address these tremendous challenges. Fog nodes are located geographically closer to IoT devices in order to shift the cloud services partially at the edge of network. However, IoT devices are resource-constrained and unable to secure themselves, and hence, they can be effortlessly hacked. Therefore, this paper proposes a credential-based authentication mechanism at the fog layer to provide the security requirements of IoT applications (e.g., confidentiality, privacy preserving, integrity and access control). Furthermore, simulations are conducted to evaluate the performance of the proposed approach using *iFogSim* simulator and *Java Cryptography Architecture (JCA)* library. The results show that the proposed mechanism ensures confidentiality of the secret key, privacy-preserving of the device attributes, in addition to detect the compromised IoT device.

Keywords Cloud computing · Fog computing · IoT · Security · Authentication · Privacy-preserving · Public key · Secret key · JCA · KCG · iFogSim

1 Introduction

As the growth of Internet of things (IoT) devices is rapidly increasing, the computing technologies are improving to meet the various user requests. However, the enhancement of computing included shift from the traditional personal computing to the client-server computing model that has been developed completely to appear as a new computing technology called cloud computing [1]. The cloud data centers

H. S. Ali (✉) · R. Sridevi
Jawaharlal Nehru Technological University, Hyderabad, India
e-mail: eng.hala.s.ali@gmail.com

R. Sridevi
e-mail: sridevirangu@jntuh.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_30

provide large domain of the services in a flexible manner guarantees the availability of the provided services and utilize the virtualization technology to serve the users' requests [2].

Nonetheless, cloud technology has several drawbacks in supporting the mobility, distribution, and location awareness of IoT devices in addition to the transmission delay and the security attacks. Therefore, a new computing technology called fog computing has been proposed in 2012 by cisco [3] to address the shortcomings of the cloud technology by bringing the computing resources and services at the network edge closer to the IoT devices. The fog technology not only reduces the network latency and support the mobility and the geo-distribution [4], but also enhance the quality of service along with the security and privacy in the IoT environment [5].

However, many methods have been suggested in the state-of-the-art [6–8] as security solutions include authentications, encryption, access control, and preventing techniques at the fog layer. Moreover, the authentication is a necessary requirement to protect the IoT data against the security breaches. Unfortunately, the limited resources capacities of the IoT devices pose a challenge to implement the required security operations [9]. Hence, this problem can be addressed through shifting the heavy operations to the fog nodes to provide the required security and privacy services to the IoT devices [10]. Therefore, this paper introduces a novel credential-based authentication mechanism at the fog layer. The contributions of this article are summarized as follow:

1. Propose a centralized authentication mechanism based on the attributes of the IoT devices.
2. Establish a secure end-to-end communication between the IoT and the fog layer by generating a secret key and distributing it securely using a public-key cryptography scheme.
3. Analysis how the proposed approach achieves the confidentiality, integrity, privacy-preserving as well as, detecting the compromised device.

The rest of this paper is organized as follow. The related work is discussed in Sect. 2. The fog-cloud computing system model is introduced in Sect. 3. Section 4 presents the proposed credential-based authentication approach, while Sect. 5 shows the simulation results of executing the proposed method. Finally, we conclude our work with suggest future directions in Sect. 6.

2 Related Work

Several authentication methods have been proposed for fog-cloud commuting paradigm. The authors in [9] proposed a security service at the fog layer provides confidentiality, authentication, and non-repudiation for the IoT device without considering the privacy-preserving. In [10], a decentralized authentication method has been proposed using the blockchain technique in a fog-cloud environment with a

smart contracts to authenticate the users' access to the IoT devices based on generated tokens. The proposed method achieved integrity, availability, and confidentiality in addition to prevent the DoS, replay, and eavesdropping attacks. The authors in [11] also used the fog nodes with smart contract to authenticate the requests of users for accessing the IoT devices without considering a trust third party. The proposed lightweight authentication method achieved the data privacy-preserving comparing with [10].

A new mutual authentication method of IoT devices in fog environment proposed in [12]. The handshake step in the proposed method is similar to that used in TLS protocol. Beside that , the challenge-response function, nonce, and response time are used as authentication factors to implement the mutual authentication. In [13], the authors proposed a mutual authentication protocol not only between the fog and IoT layer, but also between the fog and cloud layer. The IoT device authenticate itself to the nearby fog node based on its virtual identifier, while the fog node authenticate itself with a central authority at the cloud layer. The proposed protocol is secured against many attacks (e.g., replay attack, user and fog impersonation attack, MITM attack, brute force attack) and assurances the confidentiality, data integrity as well as privacy-preserving. While in [14], the authors proposed a mutual authentication between the fog servers and users only. The proposed method supposed that all the end users and fog devices are registered with a central authority located at the cloud layer. In addition, the authentication protocol depended on the user's virtual identifier and a challenge-response function. Their scheme is resist against many attacks (e.g., eavesdropping attack, MINM attack and replay attack) and meets the security requirements in fog-cloud environment.

Unlike the previous authentications methods, we propose a fog-cloud architecture involves a central fog node as a trust third party responsible for generating the keys and credential for both of the IoT and fog devices. We aims to authenticate the IoT device to protect the fog and cloud layers from the attacks. Our authentication scheme depends on many attributes of the device (Id, User name and Password) which are blinded to implement the privacy-preserving. Moreover, we ensure secure distributing of the secret key between the fog and IoT layer. While our work ensures the privacy of IoT device by blinding its real attributes, our architecture includes a trusted third party responsible for generating the secret key and distributing it securely between the IoT and fog layer.

3 Fog-Cloud System Model

The fog-cloud architecture consists of three layers (IoT devices layer, fog layer, and cloud layer) as depicted in the Fig. 1. The IoT devices layer also known as perception layer which includes several types of distributed devices (such as sensors, actuators, smart watches, smart phones and vehicles, etc.). Each IoT device has many attributes (User name, Password, Location, Ip address,etc.). These attributes are submitted to the fog layer to get the corresponding credential. The fog layer in turn includes a

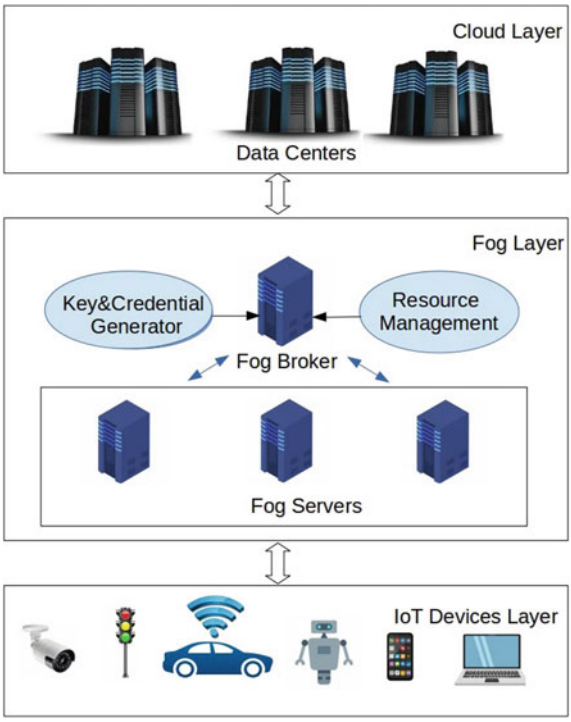


Fig. 1 Fog-Cloud Computing Architecture

set of fog servers provides several types of services to the IoT devices, where the fog server has information about all the connected IoT devices with it. In addition, the fog layer includes a high performance central fog node called fog broker. The fog broker responsible for managing the fog servers and IoT devices based on the gathering information about them. The fog broker also works as a key and credential generator (KCG) to generate the private/public keys and session keys along with the credentials to the other devices. In addition, it ensures secure delivery of the session key to the intended device. The cloud layer has data centers with high processing capacity to serve the IoT devices. Where the IoT devices and the fog servers connect with the cloud layer through the fog broker. That is why the fog layer should verify the authentication of the IoT devices before processing their tasks by the fog or cloud layer.

The IoT device is defined as $d_i = (Id_dT, un_d, pw_d, ks_d, pr_d, pu_d, c_d)$. Where Id_d is the unique identifier of the IoT device, un_d and pw_d are the user name and password assigned to the IoT device, respectively, ks_d is the secret key shared between the IoT device and the fog server which is connected with it, pr_d is the private key of the IoT device, and it is known only by the device itself and the *KCG*, pu_d is the public key of the IoT device, and it is knows by all the other devices, and c_d is the device credential generated by the *KCG*. Each fog server is represented as $f = (Id_f, pr_f, pu_f)$ where Id_f is the unique identifier of the fog server, pr_f is the

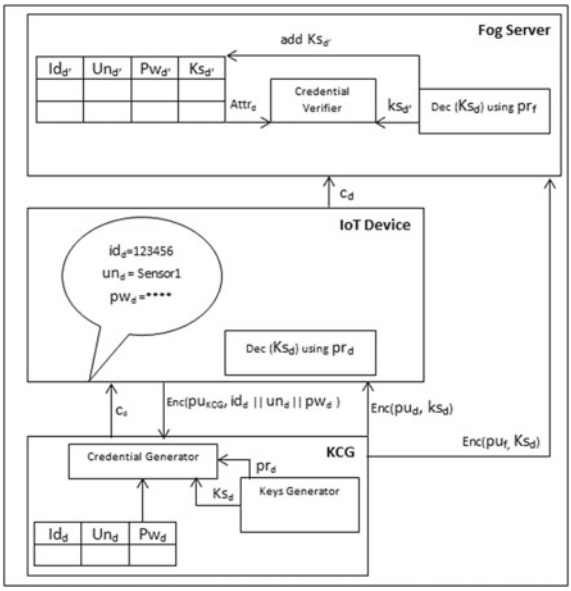


Fig. 2 The proposed authentication mechanism of IoT devices

private key of the fog server, and it is known only by the server itself and the *KCG*, pu_f is the public key of the fog device, and it is knows by all the other devices, while pr_{KCG} and pu_{KCG} are the private key and the public key of the *KCG*. We aim in this work to authenticate the IoT devices before serving them by the fog and cloud to avoid the security risks that could infect the processing servers by exploiting the IoT vulnerabilities.

4 The Proposed Authentication Mechanism

This section describes first how to generate credential for the IoT device based on its attributes. We assume that the private/public key pairs of the IoT devices are generated by the *KCG* and distributed in some secure way to the IoT devices. Figure 2 illustrates the proposed IoT device authentication process. Both of the public-key and secret-key schemes are used in the authentication process, while the secret-key scheme later is used to enable an secure end-to-end communication between the IoT and fog layer after the authentication process, while Fig. 3 shows the sequential steps of the proposed authentication mechanism followed by scheduling the tasks of the authenticated IoT application between the fog and cloud layer according to the decision algorithm and task scheduling algorithm mentioned in [15].

The IoT device requests the *KCG* to generate the corresponding credential through sending its attributes encrypted by the public key of the *KCG*. *KCG* in turn decrypt the request using its private key, generates a random secret key for the IoT device

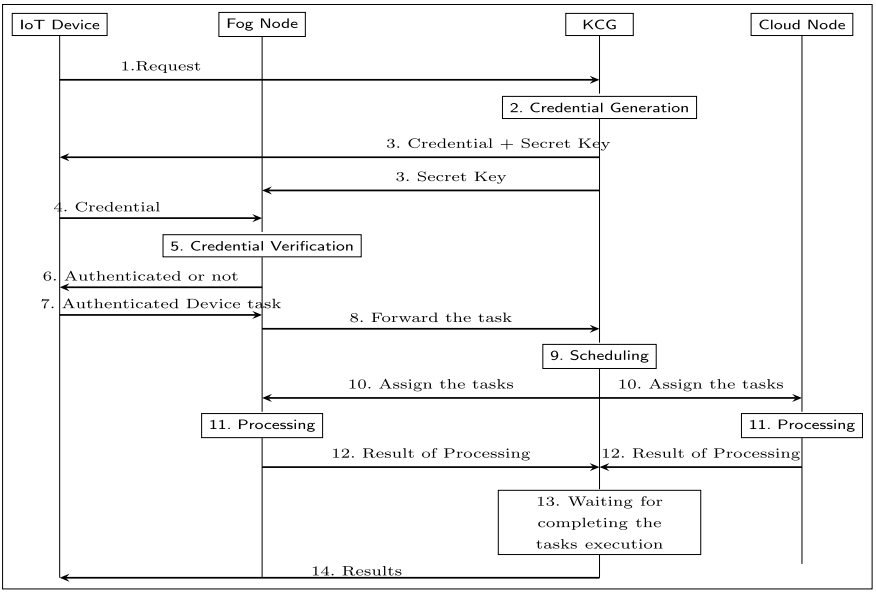


Fig. 3 Task processing sequence in the fog-cloud architecture

and delivers it securely to the interconnected fog server and IoT device encrypted by the the public key of fog server and the public key of IoT device, respectively. *KCG* also generates a attributes-based credential consists from six items by modifying the algorithm (1) in [16], where $I1$ is a hash value of the hashed selected secret key along with id, user name, and password of the IoT device. $I1$ helps the fog server to verify whether the credential and the secret key submitted by its owner or not . $I2$ is a hash value of the $I1$ with the hashed id of IoT device, and it is essential to prevent the collusion attack. $I3$ is the encrypted IoT device attributes by the secret key, and it helps the IoT device and fog server to ensure that the secret key is not compromised. $I3^*$ is a one-way accumulator used to verify if the IoT device is a member of a specific set of IoT devices or not . $I4$ is the validation time of the credential.$I7$ is the signature of the hash value of the $I1$, $I2$, $I3^* and I4$. Comparing with the proposed algorithm algorithm (1) in [16], we calculate $I1$ and $I3$ using the secret key between the IoT device and fog server rather than a shared key between the IoT device and KCG. We assume that *KCG* is trusted third party so $I5$ and $I6$ not using here. This algorithm preserves the privacy of IoT devices information through applying the hash and encryption operations on the device identifier and attributes. Algorithm 1 explains the modified algorithm.

KCG submits the generated credential c_d and the secret key K_d to the corresponding IoT device encrypted by the public key of it. The secret key K_d is also sent to the fog server encrypted by the public key of fog server. Where, both of IoT device and fog server decrypts the secret key using the private key. However, the fog server

Algorithm 1 Credential Generation

Input id_d,un_d, pw_d,
Output c_d
Predefined pu_d,pr_d ks_d
1: $I1 = h(h(k_d)||id_d||un_d||pw_d)$
2: $I2 = h(I1||h(id_d))$
3: $I3 = E(Ks_d, un_d||pw_d)$
4: $I4 = validation\ time$
5: $I3^* = H(H(...(H(ks_d, h(un_d), h(pw_d)))))$
6: $I7 = Sign(Ks_d, H(I1, I2, I3^*, I4))$
7: $Credential = (I1, I2, I3, I3^*, I4, I7)$
8: **return** $Credential$

has registered information about its IoT devices which are: the unique identifier $id_{d'}$, user name $un_{d'}$, password $p_{d'}$, and the associated secret key $ks_{d'}$ with the IoT device. The fog server uses this information to verify the IoT device credential based on the modified algorithm (2) in [16] . Unlike the algorithm (2) in [16], algorithm 2 presents the modified algorithm where ($I1$,$I2$) items are recalculated according to the stored information by the fog server and compared with the received credential items ($I1$, $I2$) if they are equal or not. $I3$ is decrypted to check the integrity of the received attributes by comparing them with those registered by the fog server. $I3$ is also useful for verifying the integrity of the secret key.

Both of these modified algorithms are used for authenticating the IoT device, while the authors in [16] used the algorithm (1) and the algorithm (2) to generate the public/private key pairs for the IoT devices.

5 Simulation and Results Analysis

5.1 Simulation Environment

We use the *iFogSim* simulator [17, 18] to model the fog-cloud environment. This simulator extends the *CloudSim* simulator classes to simulate the IoT and fog devices based on java programming language. *iFogSim* supports management of fog and cloud resources, scheduling the IoT tasks, mobility of IoT devices, heterogeneity of fog devices, and security of the fog-cloud architecture in addition to measure the metrics of performance (processing time, latency, energy consumption and resource utilization cost). Furthermore, *" Java Cryptography Architecture (JCA)"* is used to implement the proposed authentication mechanism, where it is considered as the main part of the Java platform which has a set of APIs for key management, encryption/decryption, certificate generation, and validation in addition to provide functions to generate the digital signature and validate it. In this work, we used *"Data Encryption Standard (DES)"* as the symmetric encryption algorithm, *"Rivest–Shamir–Adleman (RSA)"* algorithm as the asymmetric encryption

Algorithm 2 Credential Verification

Input $id_{d'}, un_{d'}, pw_{d'}, ks_{d'}, c_d$
Output $auth$
Predefined pu_d
Compute $I1^{'} = h(h(Ks_{d'})||id_{d'}||un_{d'}||pw_{d'})$
if $I1^{'} == I1$ **then**
    $auth == 1$ & Continue
else
    $auth == 0$
end if
if $h(I1^{'}||h(id_{d'})) ==$ I2 **then**
    $auth == 1$ & Continue
else
    $auth == 0$
end if
Decrypt $I3$ with the $Ks_{d'}$ to get the attributes un_d, pw_d from the credential
if $(un_d == un_{d'})\&\&pw_d == pw_{d'})$ **then**
    $auth == 1$ & Continue
else
    $auth == 0$
end if
if $I4$ is valid **then**
    $auth == 1$ & Continue
else
    $auth == 0$
end if
if $(H(H(...(H(Ks_{d'}, h(un_{d'}), h(pw_{d'})))))) == I3^{*}$ **then**
    $auth == 1$ & Continue
else
    $auth == 0$
end if
if Verify Signature$I7$ is true **then**
    $auth == 1$ & Continue
else
    $auth == 0$
end if
return $auth$

algorithm,(*"Digital Signature Algorithm (DSA)"*) for constructing the digital signature and verifying it and *"SHA-256"*hash function which is applied on the IoT device attributes to get anonymous credential for this device.

5.2 Results Analysis

All of the confidentiality, privacy preserving, integrity, and access control are achieved by the proposed mechanism. The shared secret key between the fog server and IoT device is issued by the trust third party *KCG* and transmitted securely to

```
*******************************KCG***********************************************
The recieved encrypted attributes by the KCG K7hN9MRMEhsLgxJcKnkvsQNlnuz5Jc+hzT877PVemtw1tB0Ba
The recieved attributes by the KCG after decrypting using its private key are sensor1 halapass
The recieved IoT device id is  6
The recieved IoT device name is sensor1
The recieved IoT device password is halapass
generated sectert key by KCG is com.sun.crypto.provider.DESKey@18793
I1 is 63272e0a0ea31f0eb77c9fa288424724599a7498769978e6ea0b88595c2f76db
I2 is a3ce762472172aa99d2768c5ee47f9d7f09cf2601132aa7b6da2824d1c7d5499
I3 is ZHvRNkOR08tGbuJQOHFSww==
I4 is 50
I3* is -4170026585922722816
 I7 after signiture is 0<▯iÔÙÕê©u?7»▯à▯/▯ ²]F¹t®£nWç▯Cs-ØBPlg%.ÒpÁ€š▯▯>ðA▯-ŸÂÇ¦¾C
The secret key encrypted by the public key of IoT device is UrkqREO31kaZ8QC7TuoYifM+wASAY3o3nT
The secret key encrypted by the public key of fog device is TqgFr6AMFnqYFhZg5pECSWbCicc9nwxz4O
```

Fig. 4 Key and credential generation by *KCG*

both of them by encrypting it using the public key of the fog server, public key of the IoT device, respectively. Therefore, only the intended fog server and IoT device can get the secret key by decrypt it using the corresponding private key. This secure transmission of the secret key makes it invulnerable against the attackers, and it can be used later for encrypting the data between the fog and IoT device. On the other hand, the IoT device attributes are hidden by using the hash functions, which helps in preserving the privacy and preventing the linking attack. Moreover, the validation time of the generated credential preventing the replay attack. So, if we suppose that the IoT device can be compromised by an attacker which modifies the device attributes and asks the *KCG* for generating a credential. The *KCG* will generate a shared secret key between the fog server and compromised IoT device. After that, the attacker can send the modified credential to the connected fog server which in turn uses the registered information for verifying the recieved credential and detecting the attack. Thus, only the authenticated IoT device has access to the services provided by the fog and cloud servers based on its credential as a proof.

Our proposed architecture includes three sensors, three fog devices where each one is connected with a sensor device, one fog broker, and one cloud node. Each sensor has id, user name, and password as attributes. Figure 4 shows how the *KCG* decrypts the submitting request by the IoT device which includes its attributes. It also show how the *KCG* generates credential and secret key for the IoT device encrypted by the public key of the IoT device and by the public key of the fog server, where the received sensor attributes by the *KCG* are: *Id=6, username= sensor1 , password= halapass*.

RSA algorithm is used to encrypt the secret key using the public key of each the IoT device and fog server as illustrated in Fig. 5.

Figure 6 shows receiving the secret key by both of the IoT device and fog server and decrypting it using the corresponding private key, where the secret key should be same at the IoT device and fog server.

On the other hand, the fog server calculates credential of the IoT device based on the stored information and compare it with the received credential if it is matching or not. We observe that the stored password of the sensor device is *password1*, while the receiving password is *halapass*. It means that the sensor device compromised by

```
try {
    cc = generate_cred(attributes,ev.getSource(),ev.getDestination());
    key=cc.kk;
    sensor_ecipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");
    Sensor s=TestApplication.sensorById.get(ev.getSource());
    FogDevice f=TestApplication.deviceById.get(s.getGatewayDeviceId());
     try {
        fog_ecipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");}
     catch (NoSuchAlgorithmException | NoSuchPaddingException e) {
        e.printStackTrace();}
     try {
        fog_ecipher.init(Cipher.ENCRYPT_MODE, f.pub);}
     catch (InvalidKeyException e) {
        e.printStackTrace();}
    sensor_ecipher.init(Cipher.ENCRYPT_MODE, s.pub);
    String key_s= key.toString();
    String shared_key = encrypt(key_s);
    String shared_key2 = encrypt2(key_s);
    System.out.println("The secret key encrypted by the public key of IoT device is "+shared_key);
    System.out.println("The secret key encrypted by the public key of fog device is "+shared_key2);
    send(ev.getSource(), CloudSim.getMinTimeBetweenEvents(), FogEvents.SENSOR_SHARED_KEY,shared_key);
    send(ev.getSource(), CloudSim.getMinTimeBetweenEvents(), FogEvents.SENSOR2_CREDENTIAL,cc);
    send(s.getGatewayDeviceId(), CloudSim.getMinTimeBetweenEvents(), FogEvents.SHARED_KEY,shared_key2);
} catch (Exception e)
{e.printStackTrace(); }
```

Fig. 5 Encrypting the secret key using *RSA* algorithm

```
**********Receiving the secret key by the fog device fog1**********
Decrypting the secret key by the fog device fog1 using its private key  is com.sun.crypto.provider.DESKey@18793
**********Receiving the secret key by the IoT device sensor1**********
Decrypting the secret key by the IoT device sensor1 using its private key  is com.sun.crypto.provider.DESKey@18793
Submitting the credential to the fog server : fog1
--------------------------------------------------------------------------------
**********Receiving the secret key by the fog device fog2**********
Decrypting the secret key by the fog device fog2 using its private key  is com.sun.crypto.provider.DESKey@fffe7a39
**********Receiving the secret key by the IoT device sensor2**********
Decrypting the secret key by the IoT device sensor2 using its private key  is com.sun.crypto.provider.DESKey@fffe7a39
Submitting the credential to the fog server : fog2
```

Fig. 6 Receiving the secret key by the IoT and fog device

```
**********Fog Server**********
Recieved IoT device credential
The stored IoT device id is 6
The stored IoT device username  sensor1
The stored IoT device password  Password1
The calclated I1 based on the stored IoT device attributes is 00e9f929246340f69aca6eal
The calclated I2  by the fog device is 8713fb2d6590880e67f7e47d93ce884833412af67d9ba6
Result of decrypting the received I3 using the secret key is : sensor1halapass
The calclated I3* based on the stored IoT device attributes'  is -4170120644531961856
The received I1 of sensor1 is not matching with the calculated I1 by the fog device
The received I2 of sensor1 is not matching with the calculated I1 by the fog device
The received I3* of sensor1 is not matching with the calculated I3* by the fog device
signature verifies: false for sensor1
Compromised IoT device
```

Fig. 7 Verifying the credential by the fog device

attacker who modified its password as shown in Fig. 7. And this attack detected by the fog server using the credential verification algorithm.

6 Conclusions

In this paper, we have proposed an authentication mechanism to secure the IoT devices before serving them by the fog and cloud servers. We have depended on the attributes of IoT device to generate the corresponding credential which used to authenticate it. The proposed mechanism achieved many security goals such as confidentiality by using the secret key, privacy preserving by keeping the IoT device attributes hidden, and integrity of the data along with the access control. The simulation experiment has shown how the proposed mechanism ensured secure distribution of the secret key, protection the device attributes from the eavesdropping in addition to detect the compromised IoT device. In future work, we plan to implement the proposed mechanism in a real environment to analyze the system behavior and compare it with other authentication approaches to achieve better results. Another direction of this research is to optimize our method to reduce the security-related overhead. In addition to considering the mobility of IoT devices via implementing a mutual authentication between the fog servers.

References

1. M.A. Thomas, R.T. Redmond, H.R. Weistroffer et al., Moving to the cloud: transitioning from client-server to service architecture. J. Service Sci. (JSS) **2**(1), 1–10 (2009)
2. N.M.S. Almurisi, S. Tadisetty, Classification of virtualization techniques for iot-based heterogeneous wireless sensor network. J. Critical Rev. **7**(14), 795–807 (2020). https://doi.org/10.31838/jcr.07.14.143
3. S.B. Nath, H. Gupta, S. Chakraborty, S.K. Ghosh, *A Survey of Fog Computing and Communication: Current Researches and Future Directions*. arXiv preprint arXiv:1804.04365 (2018)
4. G. Zhang, F. Shen, Z. Liu, Y. Yang, K. Wang, M.T. Zhou, Femto: Fair and energy-minimized task offloading for fog-enabled iot networks. IEEE Internet Things J. **6**(3), 4388–4400 (2018)
5. G. Rahman, C.W. Chuah, Fog computing, applications, security and challenges, review. Int. J. Eng. Technol. **7**(3), 1615–1621 (2018)
6. S. Khan, S. Parkinson, Y. Qin, Fog computing security: a review of current applications and security solutions. J. Cloud Comput. **6**(1), 1–22 (2017)
7. A.V. Dastjerdi, H. Gupta, R.N. Calheiros, S.K. Ghosh, R. Buyya, Fog computing: Principles, architectures, and applications, in *Internet of Things*. (Elsevier, 2016), pp. 61–75
8. K.K.R. Choo, R. Lu, L. Chen, X. Yi, *A Foggy Research Future: Advances and Future Opportunities in Fog Computing Research* (2018)
9. N. Abbas, M. Asim, N. Tariq, T. Baker, S. Abbas, A mechanism for securing iot-enabled applications at the fog layer. J. Sensor Actuator Netw. **8**(1), 16 (2019)
10. R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, K. Salah, A user authentication scheme of iot devices using blockchain-enabled fog nodes, in *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*. (IEEE, 2018), pp. 1–8
11. K. Pallavi, V.R. Kumar, Authentication-based access control and data exchanging mechanism of iot devices in fog computing environment. Wireless Personal Commun. **116**(4), 3039–3060 (2021)
12. L. Loffi, C.M. Westphall, L.D. Grüdtner, C.B. Westphall, Mutual authentication for iot in the context of fog computing, in *2019 11th International Conference on Communication Systems & Networks (COMSNETS)*. (IEEE, 2019), pp. 367–374

13. S. Singh, V.K. Chaurasiya, Mutual authentication scheme of iot devices in fog computing environment. Cluster Comput., 1–15 (2020)
14. A.B. Amor, M. Abid, A. Meddeb, A privacy-preserving authentication scheme in an edge-fog environment, in *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*. (IEEE, 2017), pp. 1225–1231
15. H.S. Ali, R.R. Rout, P. Parimi, S.K. Das, Real-time task scheduling in fog-cloud computing framework for iot applications: a fuzzy logic based approach, in *2021 International Conference on COMmunication Systems & NETworkS (COMSNETS)*. (IEEE, 2021), pp. 556–564
16. X. Yao, H. Kong, H. Liu, T. Qiu, H. Ning, An attribute credential based public key scheme for fog computing in digital manufacturing. IEEE Trans. Industrial Informatics **15**(4), 2297–2307 (2019)
17. R. Mahmud, R. Buyya, Modelling and simulation of fog and edge computing environments using ifogsim toolkit, in *Fog and Edge Computing: Principles and Paradigms* (2019), pp. 1–35
18. H. Gupta, A. Vahid Dastjerdi, S.K. Ghosh, R. Buyya, ifogsim: a toolkit for modeling and simulation of resource management techniques in the internet of things, edge and fog computing environments. Softw.: Pract. Experience **47**(9), 1275–1296 (2017)

NAYAN-DRISHTI: A Revolutionary Navigation/Visual Aid for the Visually Impaired



Salil Fernandes, Jordan D'souza, Anthony Kattikaren, and Dipti Jadhav

Abstract The project/proposed product hinges on three domains of computational technology, i.e., machine learning, convolutional neural networks, and Internet of Things. The aim of the project is to invent a product that is helpful to the disabled section of society as ideally as possible try to as well as to acquaint ourselves with the much talked about and ever-growing domains of computer technology. The main functions that our proposed product will offer are detection of the obstructing object and alerting via a speaker (along with classification and distance of the object from the user) and a navigation system (which obtains live data of the current location of the user with the help of the UBLOX GPS module). The proposed product is designed in such a way so as to provide an all in one multitasking and hassle-free solution to our user and to ease the burden that comes along with the disability of blindness. The proposed product is touted as a boon to our users since it not only will help them in identifying the obstructions ahead them but will also help them to navigate from their current location to their destination with freedom and no fear.

Keywords Convolutional neural networks (CNN) · Rectified linear unit (ReLU) · Batch normalization (BN)

1 Introduction

We sometimes wonder how the disabled section in our society manages to perform tasks that look impossible pertaining to their disability. We have to ponder as to how efficiently can they perform their day-to-day tasks and how well can they communicate with normal people. Keeping in mind the difficulties they face, their ability to perform such tasks, and how to ease the fear related to it, technology has advanced in many fields.

Blindness can basically be classified into three types:

S. Fernandes (✉) · J. D'souza · A. Kattikaren · D. Jadhav
Don Bosco Institute of Technology, Mumbai 400070, India

D. Jadhav
e-mail: dipti.dbit@dbclmumbai.org

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_31

Complete blindness, night blindness, and color blindness.

The proposed product will function accordingly as explained below using the following computing domains:

1. Convolutional Neural Networks: The product will take an input from the surrounding environment of the user and convolve it for a better prediction of the obstructing object which will be done using machine learning.
2. Machine Learning: The product with the output image can predict the object that is in hindrance to the user's path with the help of pre-trained datasets.
3. Global Positioning System: The user will be able to communicate his/her destination to the software, and the software will guide the user to the destination. The UBLOX GPS module plays an important role in communicating the satellite in space to obtain the real-time location of the user.
4. Internet of Things (IoT): Our project consists of Raspberry Pi, GPS module, camera module, etc., that will be effectively used in processing data, capturing images, displaying location of the person, etc.

2 Literature Survey

2.1 Survey of Existing Systems

"Electronic walking stick for the blind" published in the year 2018; the use of optical sensors has been highlighted. This is a modern concept of a walking stick which is completely digital. These sensors essentially convert light reflected from any surface and convert them into electric signal and act as response to the stimuli and inform the blind person via a speaker on the handle about the obstacle. The object aimed to give voice assistance to the user and was able to deliver in various cases [1].

"Portable Blind aid Device" published in the year 2019; it highlights the use of a mobile-based project in which the user can switch his wireless device into blind-assistance mode with the help of a button. With the help of the camera, GPS, and a cloud-based architecture, it will be able to give the real-time location of the user and also make him aware of his surroundings and also plan to include an advanced image recognition algorithm to recognize the faces of stranger and to store them [2].

"Intelligent glasses for the blind" published in the year 2016; the device is smart glass which uses a camera, an ultrasonic sensor, and an electronic touchpad to assist the blind person. Using a mobile device, one can activate the glass, and the camera will capture and convert the 3D image into a spatial matrix and give appropriate outputs. The touchpad gives light electric shocks to make the user aware of the obstacles. Future scope was to add a walking cane with a button to give the user audio output of the real-time surroundings [3].

"Object Identification for Visually Impaired." published in the year 2016; a simple image recognition system that makes use of camera to recognize images, an ultrasonic sensor to detect obstacles is explained. The camera captures the images, and if the

image can be recognized by the images in the dataset, then the device gives an audio output using a speaker that will be attached to the users clothing. Future upgrades include to introduce face recognition and to use a wireless camera [4].

"Real-Time Objects Recognition Approach for Assisting Blind People" published in the year 2017; an object recognition project is depicted that with the help of speeded up robust features (SURF), light machine learning is able to give accurate information about the objects captured. Using GPS and image recognition, it gives 90% accurate results. It makes use of a database, and using machine learning algorithm, it is able to identify the objects [5].

"EarTouch: Facilitating Smartphone Use for Visually Impaired People in Mobile and Public Scenarios" published in the year 2019; a blind aid device uses ear gestures like long swipe, tap, and slide for operating the various function on the smartphone. Making use of one-hand gestures and ear-touch feature, it enables the user to use the device with ease. And, it gives out audio output through the inbuilt speakers. The device was able to read the gestures accurately and activate the respective functions when the user wanted it [6].

"An Ultrasonic Navigation System for Blind People" published in the year 2017; it introduces with us another device for object detection which not only uses an ultrasonic sensor but also includes an accelerometer, footswitch, microcontroller, and vibration pad. User is made aware of the obstacle and closeness f it by different degree of vibrations and also through an audio output [7].

"Mobile Blind Navigation System Using RFID" published in the year 2015; the paper introduces a mobile-based communication device which makes use of the Wi-Fi and GPS to determine the user's location. And also makes use of RFID tags in the surroundings to give more accurate location to the user and guide them by giving appropriate instructions. The user makes use of a smart walking cane and RFID-handled reader [8].

"Voice assisted system for the blind" published in the year 2015; the paper introduces us with a simple object/obstacle detector which makes use of an ultrasonic senor, microcontroller, mp3 module, and SD card. The sensor sends the distance measured, and the microcontroller depending the proximity limit, it is programmed and sends an output to the mp3 module. It makes use of depth sensing for avoidance of pot holes, etc., for the user to walk with smoothness and comfort with normalcy [9].

"Virtual-Blind-Road Following Based Wearable Navigation Device for Blind People" published in the year 2019; the paper depicts a navigation device specifically for the indoor environment which makes use of simultaneous localization and mapping (SLAM). The device tries to give the person the best path to an indoor destination by keeping track of the positions of previously encountered obstacles. It makes use of PoI graph to store new points in the route to the destination, and using A* algorithm on the PoI graph, it finds the shortest and optimum path to the destination. Obstacle distance is measured by an ultrasonic range finder and provides audio output [10].

2.2 Limitations of the Systems on Research Gap

All the above proposed papers that we have researched 90% success rate in the field and in all test cases although with certain setbacks too. All devices are capable of giving the required results, but the reactions time in real-world is less which the devices are not able to keep up with. For real-time outputs, more complex and advanced system and cloud-based architecture is required which is difficult on a limited budget. In image recognition, few projects were not able to identify objects in the dark or night. The components used in few projects are fragile and prone to damage. Hence, when used by a user could get damaged. And, using strong equipment makes the project expensive.

2.3 Problem Statement and Objective

Our product introduces a three-way combined solution system that will serve as a navigation aid for the blind:

1. To ease the difficulty and uncertainty faced by the blind or any visually impaired person when they have to walk from one place to another. A simple task like walking is scary for blind people owing to the fact that they just do not know what obstacles, whether dangerous or not, may be in front of them.
2. Through our project, we hope to create a product that makes navigation a safer and simpler task for blind people. Object detection and recognition are the core concept which our project revolves around.
3. Our project domain is machine learning, and we have decided to make use of the concept of a convolutional neural network built using TensorFlow to process image data and perform the object recognition task after being trained with datasets.

2.4 Scope

Our project aims to implement three main features:

(1) Object recognition using a camera attached to the pi module, and using our machine learning domain and implementing convolutional neural network (CNN) break down the images into 2D frames and train the algorithm to identify various objects in the surrounding.
(2) Object detection using an ultrasonic sensor which can detect obstacles at a distance of 4 m and sends an alert to the user if the proximity of the object is within a certain given range.

(3) Giving the real-time location of the user using a GPS module that is programmed to communicate with the satellite and on a press of a button gives the user his/her location.

3 Models and Setups

For object detection, we have used a convolutional neural network to perform object recognition on a given image. With respect to sensing the distance of a user from a given obstacle, we have utilized the concept of ultrasonic distance sensing.

3.1 Object Detection and Recognition

The primary goal of our project is to perform image analysis to lead to object recognition which would enable a blind person to get a sense of his/her environment. By understanding what objects surround them, blind people can make better decisions about where they are and in what direction they should move. We have used the convolutional neural network (CNN) model to implement object detection and recognition. Convolutional neural networks are a family of deep learning algorithms that take parts of images as inputs, apply certain weights, and biases and differentiate one part of the image from another. Most images nowadays are RGB images meaning that there are three channels to the image. CNNs make it easier to understand the image by capturing the spatial and temporal dependencies by using filters is different levels or depths. It offers faster analysis by reducing the number of parameters and reusing weights.

Under CNNs, there are several architectures that come into the picture like the faster R-CNN model, mask R-CNN inception model, and the SSD ResNet models to mention but a few. In our project, we are using a Raspberry Pi-3 model B + to program and execute our programs. Due to limited memory of 1 GB RAM and lower processing power available, we have to make use of a neural network which is computationally less intensive but without making a compromise in accuracy. The architecture which suited this purpose is the SSD MobileNetv2 architecture (Figs. 1 and 2).

The architecture uses the concept of depth-wise convolutions. Depth-wise convolution is a type of convolution wherein a single convolutional filter is applied to each input channel. In the regular.

2D convolution performed over multiple input channels, the filter is as deep as the input, and lets us freely mix channels to generate each element in the output. In contrast, depth-wise convolutions keep each channel separated from each other. In general, the steps used to perform a depth-wise convolution are:

1. Break up the input and filter into channels.

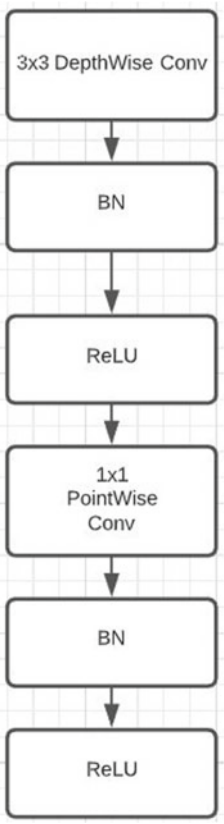


Fig. 1 Single convolution layer in MobileNet

2. Convolve each input with the appropriate filter and combine the convolved outputs.

A depth-wise convolution consists of a depth separable convolution and a point-wise convolution. Spatial separable convolution works mainly with the spatial dimensions of an image and kernel which are the width and height. (The third dimension is called depth which is the number of channels of each image and is not taken into account by spatial separable convolutions). A spatial separable convolution breaks a kernel into two smaller kernels. The most common case would be to divide a 3×3 kernel into a 3×1 and 1×3 kernel. In place of performing a single convolution by 9 multiplications, we perform two convolutions with 3 multiplications each to get the same result. With fewer multiplications, computational complexity goes down, and the network is able to run more efficiently. Unlike spatial separable convolutions, depth-wise separable convolutions use kernels that are not divided into two smaller kernels. The depth-wise separable convolution is so named because in addition to spatial dimensions, it deals with the depth dimension—the number of channels—as well. An input image can have 3 channels: RGB. After a few convolutions, an image

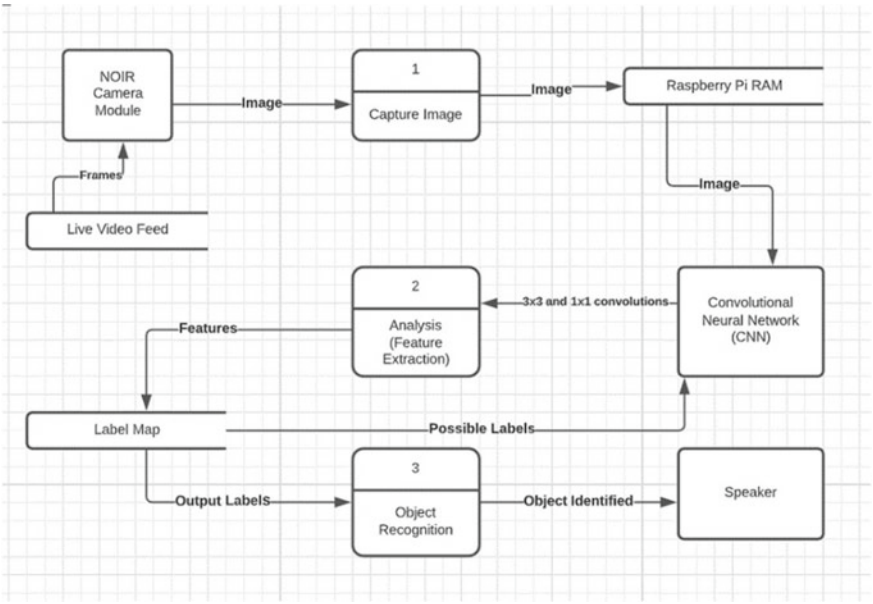


Fig. 2 Data flow diagram for object recognition

may have multiple channels. An image with 64 channels would have 64 different versions of the same image. Analogous to spatial separable convolution, a depth-wise separable convolution divides the kernel into two kernels that do two convolutions: a depth-wise convolution and a pointwise convolution.

3.2 Dataset Used

The COCO dataset has been used to train our MobileNet. CNN for object detection and recognition. COCO in short is a dataset used for training object detection, segmentation, and captioning networks. COCO stands for common objects in context which means that images are taken from everyday objects to prepare the dataset. It has approximately 330,000 images with more that 200,000 of them labeled.

3.3 Activation Function Used

For each convolutional layer of the architecture, the ReLU activation function has been used along with batch normalization, the rectified linear activation function also called ReLU is the most commonly used activation functions in artificial neural

networks. It returns a 0 as output for any negative input. If it receives a positive value x as input, it returns x as the output. So, in general, this function is given as an equation $f(x) = \max(0, x)$.

Batch normalization is a deep learning technique that normalizes the output of each sublayer. It allows for fast processing and deep network training by reducing internal covariate shift.

3.4 Obstacle Distance Sensing

For the purpose of sensing the presence of an obstacle and sensing the distance between the obstacle and person, an ultrasonic sensor is being used. The input for this would in fact be an object placed in front of the sensor. The output is a distance reading if the object is in the sensor's accurate range. By means of a wireless Bluetooth speaker, an audio warning will be sounded stating that the obstacle is nearby (Fig. 3).

The ultrasonic sensor has four pins:

a. VCC which is used to take the power supply.
b. TRIG which will on receiving the input signal from the Raspberry Pi will send out the ultrasonic pulse.
c. ECHO which will gather the echo pulse from the obstacle and send the signal that the obstacle has been detected back to the Raspberry Pi.
d. GND which provides general grounding to the sensor.

For exchanging signals and for the program to receive readings from the sensor, the GPIO pins of the Raspberry Pi were connected with the pins of the sensor. We have used the HC-SR04 ultrasonic sensor to perform this functionality. The accurate range of this sensor is 2 cm to 400 cm which means that it can correctly measure distance between a user and obstacle when the obstacle is no less than 2 cm and no more than 00 cm away from the sensor. Extra caution had to be taken when

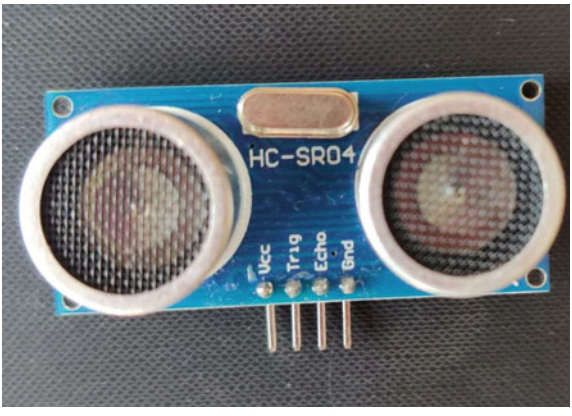


Fig. 3 Ultrasonic sensor

implementing the circuit between the sensor and GPIO pins. The ultrasonic sensor operates at 5 V, and this voltage was supplied by connecting GPIO pin 1 to the VCC pin of the sensor. Since all the GPIO pins (except for pin 1) operate at 3.3 V and the signals sent by the sensor at 5 V, care has to be taken to lower the voltage. To do this, we made use of a voltage divider circuit implemented on a breadboard. We used 560 Ω and 1000 Ω resistors to lower the 5 V echo signal to a 3.3 V signal.

3.5 Location Sensing

In order to allow the blind person to know where exactly he/she is when navigating outdoors, a GPS sensor has been used. The Ublox Neo 6 M GPS module allows for easy interfacing with the Raspberry Pi (Figs. 4 and 5).

The antenna once attached to the sensor allows for GPS data to be received. The antenna has to be left exposed to the sky in order for a satellite to lock onto it and start transmitting GPS data. There are three pins that are used to take the received data from the module:

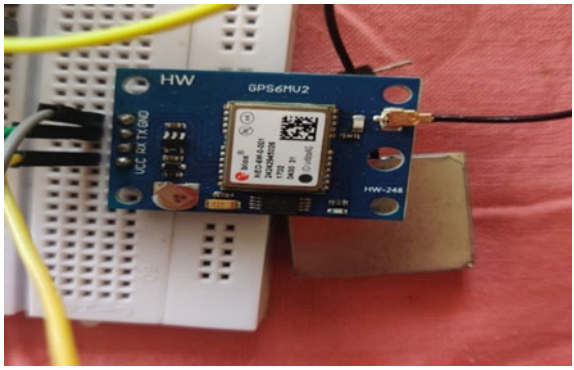


Fig. 4 GPS module

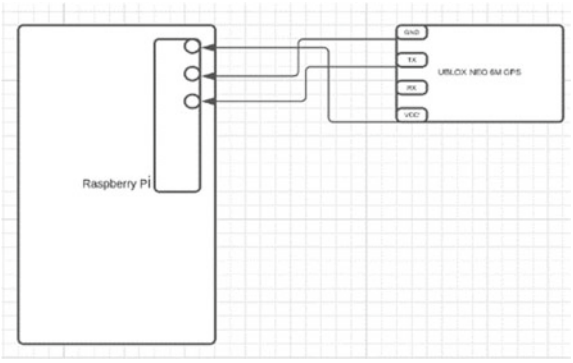


Fig. 5 Diagrammatic location sensing setup

a. GND: This pin is connected to pin 3 of the Pi for providing electrical grounding.
b. VCC: This pin is connected to pin 1 of the Pi which provides a 5 V power supply.
c TX: The transceiver pin of the module is connected to the RX pin of the Pi which is pin 5. RX is the receiver pin of the Pi which will transfer received GPS data to the serial port to be read by the Python program.

In Python, the GeoPy, PyNMEA2, and GeoPandas libraries have been used. The GPS module receives location data in the form of NMEA sentences. In the Python code, the geographic position, latitude/longitude (GPLL) sentence has been extracted and used to obtain latitude and longitude coordinates of the module's current location. Reverse geocoding, i.e., coordinates to address have been performed by the program to obtain the address. As usual, this location address is sounded to the blind person by means of the Bluetooth speaker.

3.6 Wireless Sound

The wireless Bluetooth chip that comes with the Raspberry Pi has been used to provide audio messages. A Bluetooth speaker is connected to the Pi with the help of this chip. For the purpose of making use of Bluetooth, several packages had to be installed first, namely: Bluez, Alsa, Bluetooth Manager, and PulseAUDIO.

Since our device aims to help blind people navigate, audio messages have to be delivered. This is the primary reason for using a wireless speaker. It is possible for blind people to get visual cues about their environment; hence, audio hints have to be delivered to inform them.

In the object detection and recognition feature, once an object is successfully detected, the speaker delivers a message for, e.g., "cup detected."

In the obstacle sensing feature, whenever the ultrasonic sensor senses the obstacles distance to be less than 10 cm, a message is sounded, e.g., "careful obstacle is 10 cm away."

In the location sensing feature, the speaker sounds the address of the current location obtained by reverse geocoding the coordinates.

4 Mathematical Model

4.1 Object Detection and Recognition

In each convolutional layer, the first layer is a pointwise convolution followed by ReLU. The second layer is a depth-wise convolution, and the third is another pointwise convolution but without any nonlinearity.

Input	Operator	Output
H × W × K	1 × 1 conv, ReLU	H × W × TK
H × W × TK	3 × conv S = s, ReLU	$\frac{H}{s} \times \frac{W}{s} \times TK$ s s
$\frac{H}{s} \times \frac{W}{s} \times TK$	1 × conv	$\frac{H}{s} \times \frac{W}{s} \times K'$

T is called the expansion factor, s is called the stride, and H and W are the height and width of the image, respectively. For our MobileNet, the depth-wise convolution applies a single filter to each input channel. The pointwise convolution then applies a 1X1 convolution to produce a linear combination of the outputs the depth-wise convolution. All layers in MobileNet consist of a 3X3 depth-wise separable convolution except for the first layer which has a full convolution. A final average pooling reduces the spatial resolution to 1 before the fully connected layer. Counting depth-wise and pointwise convolutions as separate layers, MobileNet has 28 layers.

4.2 Ultrasonic Distance Sensing

We have assumed the speed of sound to be approximately 340 m per second or in other words 34,000 cm per second. To calculate distance between user and obstacle, only the distance in one way has to be calculated since the time interval being measured is from the instant the ultrasonic pulse is sent to the instant the echo is received (Figs. 6 and 7).

Let, t be this time interval. Therefore, the formula for distance is,

$$d = (t * 34000)/2 \tag{1}$$

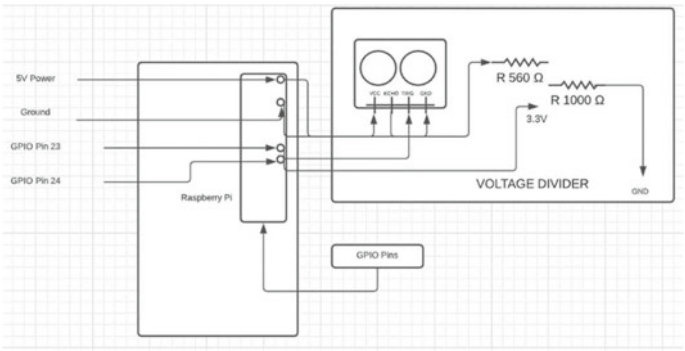


Fig. 6 Diagrammatic ultrasonic sensing setup

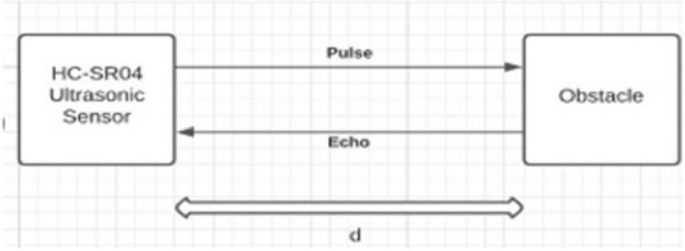


Fig. 7 Distance calculation

5 Results

5.1 Object Detection and Recognition

The frames per second (FPS) can be improved by manually changing the resolution of the detector. For objects that the model was trained for, the detections and recognitions were instant and highly accurate which is a very good result considering that the program was executed on the Raspberry Pi with only 1 GB of memory.

5.2 Obstacle Distance Sensing

In the program, we preset the range for which an alert message is to be given. Whenever the distance sensed was less than 10 cm, an alert is generated. The range can be manually changed in the program.

5.3 Live Location Sensing

This program enables the GPS module to acquire the signal from the orbital satellite and latch onto it. After the latching of the signal, it detects the location of the user and informs the user about the current location (Figs. 8 and 9).

6 Future Scope

To get more accurate obstacle/distance sensing results, a sonar sensor can replace the ultrasonic sensor as it has a larger sensing range. Whenever the Raspberry Pi foundation manages to integrate more RAM onto the computer board, the neural network can be trained a lot faster and give speedy and accurate predictions. If

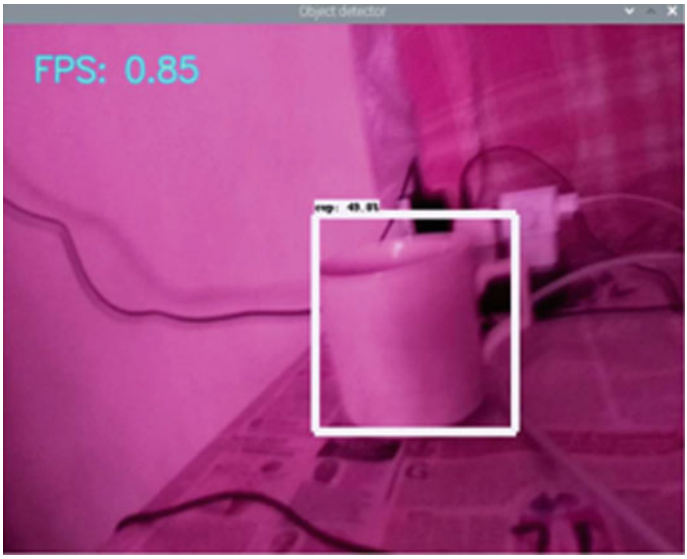


Fig. 8 Object recognition output

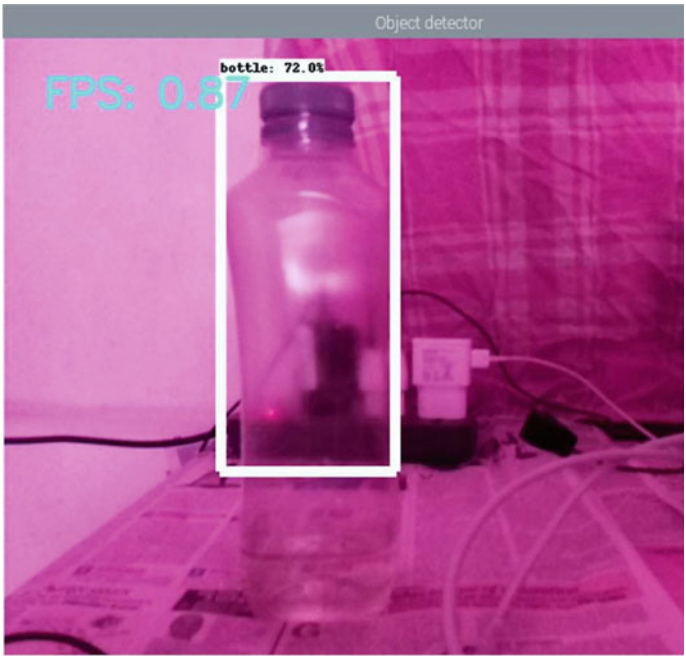


Fig. 9 Object recognition output



Fig. 10 Ultrasonic distance output depicting an alert for distances less than or equal to 10 cm

our prototype is manufactured and improved on by a professional company, the resulting product would change the lives of visually impaired people forever. The functionalities of the proposed system can also be increased from the proposed three to as much as we can in order to benefit the user even better. One such functionality can be a guided software to use the smartphone according to the user's comfort (Figs. 10 and 11).

7 Conclusions

Through the results depicted in the above section, it is clear that our object detection was overall a success in terms of efficiency and accuracy. The system could differentiate between basic objects easily with an efficiency rate ranging between 75–98% depending on the rate of frames per second. On testing the object distance measurement, we found out that the system was again efficient in displaying/sounding an alert as the object was nearing the user. An alert message will be sounded when the user is around 3-5 m from the obstructing object. But here, for test purposes, we



Fig. 11 Live location detection

chose 5 cm as our minimal limit to sound an alert message. Thus, object detection and object recognition were successfully implemented.

References

1. C.-S., Hsieh, Electronic walking stick for the blind. U.S. Patent No. 5,097,856, 24 Mar. 2010
2. E. Evanitsky, Portable blind aid device. U.S. Patent No. 8,606,316, 10 Dec. 2013
3. H.O. Cervantes, Intelligent glasses for the visually impaired." U.S. Patent No. 9,488,833. 8 Nov. 2016
4. A. Jothimani, S. Edward, G.K. Divyashree, Object identification for visually impaired. Indian J. Sci. Technol. 9.S1, 2016
5. J.S. Zraqou, W.M. Alkhadour, M.Z. Siam, Real-Time objects recognition approach for assisting blind people, 2017
6. R. Wang, C. Yu, X.-D. Yang, W. He, Y. Shi, EarTouch: facilitating smartphone use for visually impaired people in mobile and public scenarios, in *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019)*, May 4–9, 2019, Glasgow, Scotland Uk. ACM, New York, NY, USA, 13 pages (2019). https://doi.org/10.1145/3290605.3300254
7. M. Bousbia-Salah, A. Redjati, M. Fezari, M. Bettayeb, An Ultrasonic Navigation System For Blind People, in *Conference on Human Factors in Computing Systems (CHI '11), ACM*, New York, NY, USA, pp 3247– 3256 (2007). https://doi.org/10.1145/1978942.1979424. https://www.researchgate.net/publication/251851635
8. R. Sammouda, A. AlRjoub, Mobile Blind navigation system using RFID, 2015. https://ieeexplore.ieee.org/document/7353325
9. A. Noorithaya, M.K. Kumar, A. Sridevi, Voice assisted system for the blind, 2015. https://doi.org/10.1109/CIMCA.2014.7057785
10. J. Bai, S. Lian, Z. Liu, K. Wang, D. Liu, Virtual-Blind-Road following based wearable navigation device for blind people, 2018. https://ieeexplore.ieee.org/document/8307352
11. K. Simonyan, A. Zisserman, Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556 (2014)

Hygieia: Smart Health and Sanitizing Dispenser

Vaibhav Tiwari, Sudharm Kalamdani, Rohit Raut, and P. K. Rajani

Abstract Coronavirus (COVID-19), one of the deadliest pandemic diseases of the century, escalated at such a fast rate that around 25 million people around the world got infected. The impact of the virus made it a compulsion for the people to wear masks and apply sanitizer at regular intervals. Thus, for the safe and hygiene buying process of masks, sanitizer and other pharmaceutical products, an idea of a cashless and contactless dispenser was brought up named Hygieia. Hygieia is the name of the Greek goddess of health and sanitization. The purpose of this project is to make the buying process fast as well as ensure the safety of the customers by using digital payment methods. The customer can place the order with the help of speech instead of touching the keypads which is observed in most of the vending machines. Cashless payment option is also provided which is making this product a smart and viable automated dispenser.

Keywords COVID-19 · Coronavirus · Hygieia · Dispenser · Masks · Sanitizers · Cashless · Contactless

1 Introduction

The Coronavirus 2019 (COVID-19) has been declared pandemic by the World Health Organization (WHO). To prevent the virus from spreading further, a global coordinated effort is needed. A pandemic is described as a disease that occurs in a large geographic area and affects a large percentage of the population. While more evidence is still being gathered, current information suggests that human-to-human transmission is taking place. COVID-19 transmission paths are also unknown. Nowadays, however, proof from alternative Coronaviruses indicates that the disease might unfold

V. Tiwari (✉) · S. Kalamdani · R. Raut · P. K. Rajani
Pimpri Chinchwad College of Engineering, Pune, India

P. K. Rajani
e-mail: rajani.pk@pccoepune.org

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_32

through giant respiratory droplets and direct or indirect contact with infected secretions. Transmission may happen in crowded areas and indoor rooms with poor ventilation, particularly among infected people who spend a lot of time with others, such as in a shopping mall, restaurant, or other public location. Additionally, airborne transmission happens in medical care procedures. Thus, for the safe and hygiene buying process of masks, sanitizers and other pharmaceutical products, an idea of a cashless and contactless dispenser was the need of the hour [1–3].

2 Motivation

Coronavirus (COVID-19) has disrupted daily life and slowed the world economy. Thousands of people have been infected by this pandemic and are either sick or dying as a result of the disease's dissemination. Vaccines are not yet effective for this new infectious disease that is affecting humans for the first time. Thus, comprehensive measures such as extensive grooming procedures such as frequently sanitizing and/or washing hands, carrying masks, social distancing and so on are emphasized. COVID-19's effects on everyday life are already widespread and have far-reaching implications. Healthcare is one of the groups. Thus, for smooth conduction of the buying process and ensuring the safety of the customers visiting the shops, an idea was brought up to make a Smart Dispenser which would work completely on the basis of contactless and cashless payment. The customer can buy the products in hardly 2–3 min thus avoiding crowded markets and face to face interactions (Fig. 1).

The above figure shows that around 84% of the total population of India wears masks. India ranks among the top ten global mask adoption countries. Taking the usage of masks into account, the mask dispenser is perfectly suitable for this situation

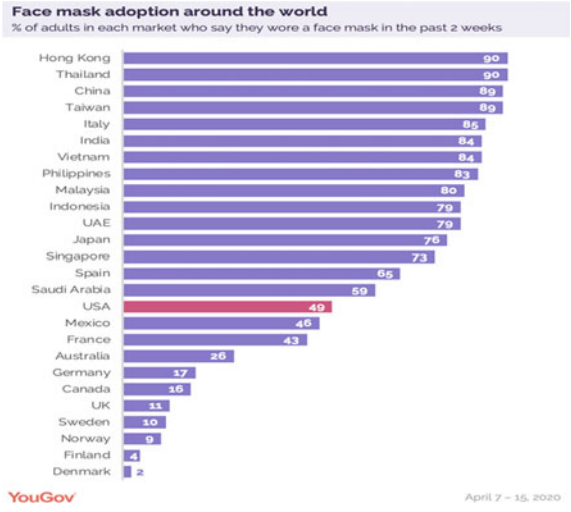


Fig. 1 Statistics showing the usage of mask around the world

in which people have considered masks as their need of living. In the near future, the usage of masks will increase rapidly.

3 Methodology

Hygieia: Smart Dispenser has two main sections. The first is the order by speech and the second being cashless payment, i.e. simply scan the QR code for the payment process [2]. Once a customer places his order such as the number of masks and/or sanitizers, the machine captures the customer image and the order details for further recommendation if in case the customer visits again [4]. After successful payment, the masks and/or sanitizes are dispensed according to the order. This machine can be installed at any public place like railway station, bus stand, airport, medical shops, etc. for the ease of the customers. The inputs for this device are mic, camera, PIR sensor, IR sensor and ultrasonic sensor. The controller used is Raspberry Pi 3 Model B+. Output device is motor. The input, i.e. product order, is taken from mic, and the image captured is taken from the camera. The speech is then processed using Raspberry Pi using a speech to text algorithm. Before the order is placed, with the help of an ultrasonic sensor, the availability of the products will be checked (Fig. 2).

According to the order, once the payment is done, the order is then dispensed using the motors. The order may be an N95 mask and/or sanitizer sachets. The PIR sensor

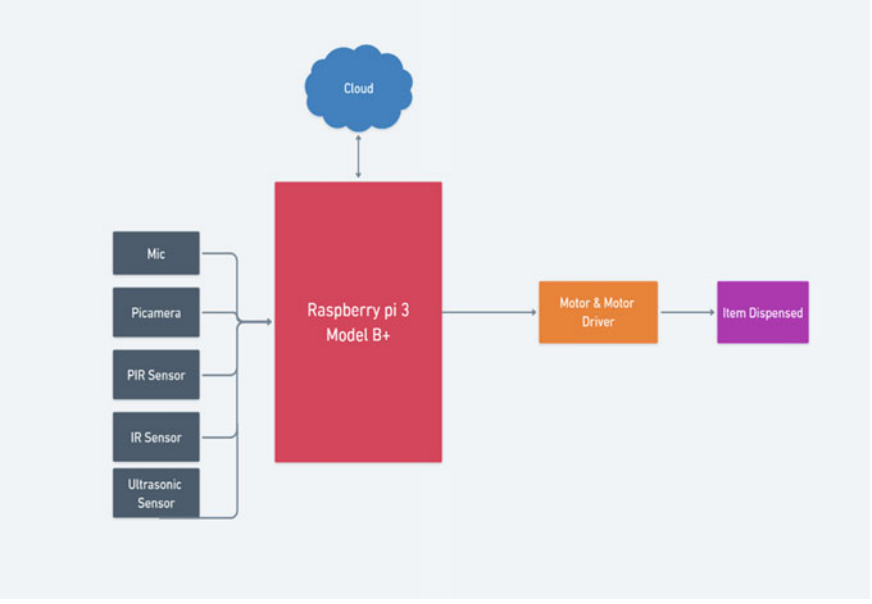


Fig. 2 Block diagram of proposed model

detects if there is any person standing in front of the dispenser. The IR sensor detects whether or not the product is dispensed. Also, after the order has been delivered, ultrasonic sensors will be used again to check the stocks. During the dispensing process, if a particular tray gets empty, the motor for that tray would be stopped, and at the same time, another motor that assists in delivering the same item will begin its operation. As the whole process is contactless and cashless, by installing this machine on a bus stand, railway station, airport, etc., the buying process of the products becomes safe and healthy, thereby reducing the chances of infections.

3.1 Hardware Specifications

The physical body of the entire project needs to be manufactured such that it becomes sturdy as well as lightweight. Sheet metal is metal that has been moulded into small, smooth parts by an industrial process. Sheet metal is one of the most popular metal-working materials, and it can be sliced and twisted into a wide range of shapes. Sheet metal is used to make a wide range of household products. Very thin sheets are referred to as foil or leaf, while parts thicker than 6 mm (0.25 in) are referred to as plate steel or "structural steel".

Raspberry Pi 3 Model B+. It will be used to perform image processing using various algorithms, to identify the faces of the ones using the facility. Additionally, it would be connected to a screen, so that the user will be able to interact with the machine. All the actuating mechanisms like motor rotation, sensor activation and deactivation are controlled by Raspberry Pi.

LCD screen. The RPI 3.5″ LCD screen is being used so that the order interpreted by the machine can be displayed, along with QR code for the same order.

IR sensor. PIR sensor is mainly used to save power. The machine will wake up if a customer comes in proximity with the machine. For the rest of the time, the machine will be in the sleep mode. As soon as the customer approaches the machine, the IR sensor detects the customer and sends an activation command to the Raspberry Pi. The Raspberry Pi wakes up and turns on the LCD screen.

MIC. This product works on the principle of contactless order reception. Thus, to take orders from the customer, a mic has been installed. This mic takes the speech input from the user and transfers it to the Raspberry Pi. The Raspberry Pi then decodes the speech and scrapes out the important words like mask, sanitizer and the quantity of each item. The order format is as follows:

1. "For mask, say 1 and for sanitizer say 2".
2. Provide your quantity. Example—"say 6".

Ultrasonic Sensor. This sensor is placed at the back of the machine. Once the order is placed, the machine checks if the stock is present or not. This is done using the ultrasonic sensor. The sensor shoots a beam of ultrasonic waves towards the front

Table 1 Mapping of distance and stock

Distance(in cm)	Stock	
<3 cm	4 (Full stock)	
3.2–6 cm	3 nos	
6.2–8 cm	2 nos	
8.2–10 cm	1 nos	
>10.2 cm	0 (No stock)	

panel. If the distance obtained is less than the tray, then stock is present. But if the wave hits the front panel, then we can say that the stock is empty. Depending upon the distance obtained, the stock present is displayed on the screen. If the stock is empty, then order is cancelled, else, the machine continues ahead (Table 1).

L298N Motor Driver and Johnson motor. Once the bill of the order is generated, a QR code is displayed on the LCD screen. The customer then pays the amount by scanning the QR. Once the payment is successful, the Raspberry Pi provides an activation command to the L298N motor driver to turn on the motor. The motor rotates until the product is dispensed. The design consists of four motors which control the movement of springs which controls the dispensing mechanism of products. There are two two trays, each with two different partitions, and each tray holds two different items, i.e. sanitizers and masks (Fig. 3).

To drive these four motors, 2 L298N motor drivers are being used. An ultrasonic sensor is being used to check the availability of the products in the tray. It would be mounted above the motors, just above the height of springs. Near the chute, an IR sensor will be installed. This will be used to check if there is any choke in the dispensing area. This product can store up to five masks and sanitizer sachets per tray.

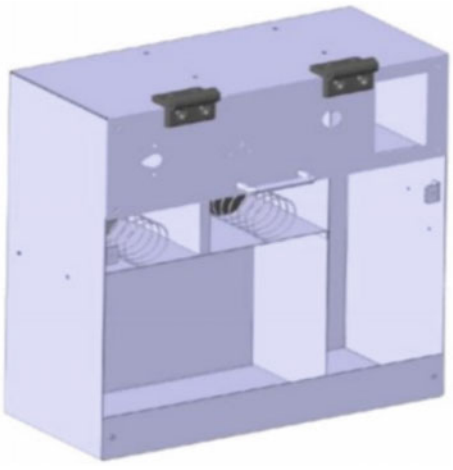


Fig. 3 CAD model of the machine

3.2 Software Specifications

The complete program is written in Python programming language. Python language was used because it supported multiple libraries for example speech recognition and OpenCV. The most important part of this dispenser is the order by speech. Google-based API of speech recognition is open source and supports Python. These libraries had to be implemented on Raspberry Pi as well. Since Raspberry Pi also supports Python, it was decided to implement all the functionalities in Python language.

Razorpay Payment Gateway. In India, Razorpay is a payment solution that helps companies to make and receive payments. It accepts credit cards, debit cards, netbanking, UPI, and common wallets as well as other payment methods. According to the order placed, a payment link is generated using the Razorpay API. This payment link is then embedded into a QR code so that when the user scans the QR code, the customer is redirected to the payment gateway. Once the payment is done, a response in the form of JSON is received. This response includes the status of the payment. If this status value is true, and then the motor starts dispensing the product. At regular intervals, the status flag gets checked until the payment is completed.

Speech Recognition. Speech recognition is a Python language-based library for conducting speech recognition online and offline, with support for a variety of engines and APIs. This library is capable of recording the voice through the mic and converting it into a stream of text which can be used for processing and placing the order for masks and sanitizers.

4 Result and Analysis

Results of the implemented project are as follows. Fig. 4 shows the software result. When the customer places the order, the product and the quantity value is extracted from the speech. Using these values, the total amount is calculated. Taking this amount as the parameter, a request in the form of JSON is sent to the Razorpay server with the help of its API. As a response, it receives JSON data consisting of a short URL. This URL is then embedded into a QR code and is displayed on the LCD screen.

Once the QR code is displayed on the LCD, the customer then scans it using any UPI app, example—Google pay, Phone pay, Paytm, etc.

Fig. 5a shows that once the QR code is scanned, the customer is redirected to the Razorpay payment gateway. As shown in Fig. 5b, the customer is provided with 4 options: Card payment, UPI, netbanking, wallet payment.

As shown in Fig. 6, the payment was completed successfully. Thus, an activation command was sent to the motor driver from the Raspberry Pi. The specific motor started to rotate resulting in the dispensation of the masks and/or sanitizers. It was observed that to dispense a single product, the motor took 2.32 s approx.

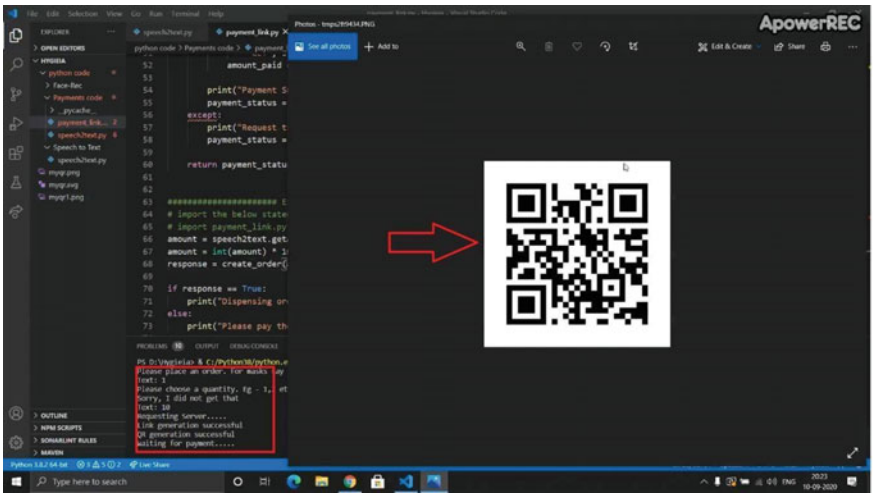


Fig. 4 QR code generation

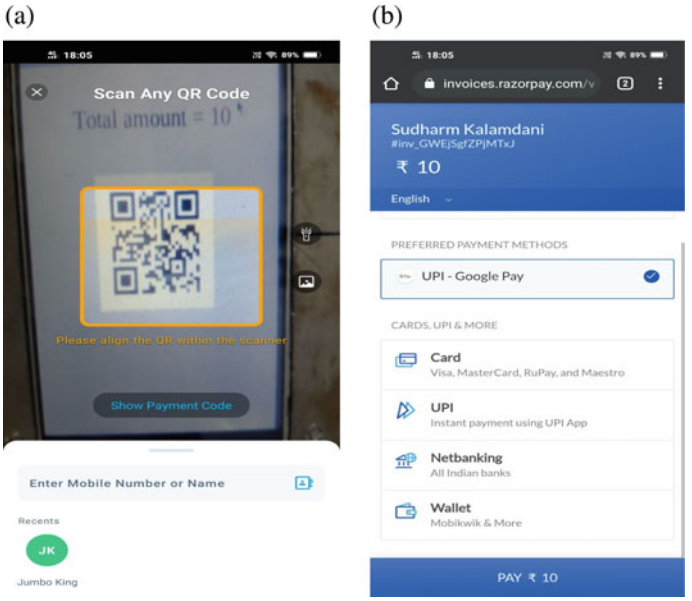


Fig. 5 a Scanning, **b** payment started

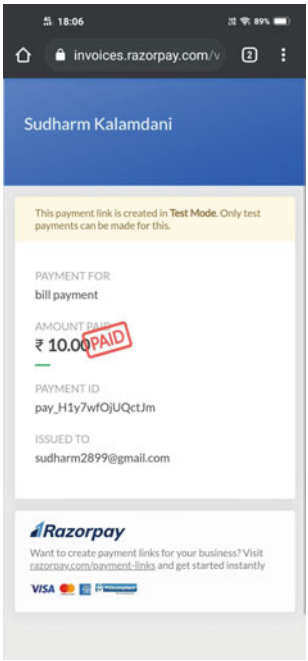


Fig. 6 Payment completed

5 Conclusion

Hygieia delivers different varieties of masks and/or sanitizer sachets available at any given time, with primary focus being the medical sector. The system designed here is a prototype, which can dispense five masks and/or sanitizer sachets. There is still scope for adding more features and making it completely industry ready. With an emphasis on social distancing and hygiene during COVID-19 pandemic, online contactless payment methods have been used, by which any user can easily pay for their orders. This product can be used in public places such as schools, colleges, bus stands and railway stations for fast and easy access to masks and sanitizers. Apart from that, partnering with the government and private pharmaceutical firms and hospitals would be needed to establish this product. Thus, Hygieia is a smart technology that assists the people to tackle the COVID-19 situation.

6 Future Scope

The future scope for Hygieia includes suggesting nearest vending machines/shops, if short on stock. It can also suggest the orders based on previously placed orders. Face recognition can be done in this project to capture the images of the customer and store it in the database for further order recommendations. Captured image can

be transmitted, and if error occurs, it can be concealed with appropriate concealment algorithms [5], thus reducing the buying time of the customer. It can suggest masks based on containment zones. According to the customers' order patterns, reminders can be sent to their mobiles at regular intervals.

References

1. W. Alam, F. Sultana, J.B. Saba, A.C. Kofi, IOT based smart vending machine for Bangladesh, in *2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON)*, Dhaka, Bangladesh, pp. 73–76 (2019). https://doi.org/10.1109/RAAICON48939.2019.36
2. P. Desai, B. Pattnaik, S. Dey, T.S. Aditya, K. Rajaraman, M. Aarthy, All Time medicine and health device, in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, Coimbatore, India, 2019
3. C. Hsu, Y. Lin, Y. Shiue, C. Sun, New generation artificial intelligent vending machine system based on LoRaWan IOT network, in *2019 IEEE International Conference on Consumer Electronics—Taiwan (ICCE-TW)*, YILAN, Taiwan, pp. 1–2 (2019). https://doi.org/10.1109/ICCE-TW46550.2019.8991716
4. V. Kanagasabapathi, K. Naveenraj, V. Neelavarnan, S. Naveen Raj, Automatic chocolate vending machine, in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, Coimbatore, India, pp. 584–587 (2019). https://doi.org/10.1109/ICACCS.2019.8728319
5. P.K. Rajani, A. Khaparde, Video error concealment using block matching and frequency selective extrapolation algorithms, in *Proceedings Society of Photo-Optical Instrumentation Engineers (**SPIE**)10443, Second International Workshop on Pattern Recognition*, 104431C (2017)
6. V.P. Semenov, V.V. Chernokulsky, N.V. Razmochaeva,The cashless payment device for vending machines—Import substitution in the sphere of vending, in *2017 International Conference "Quality Management, Transport and Information Security, Information Technologies"*, St. Petersburg, pp. 798–801 (2017). https://doi.org/10.1109/ITMQIS.2017.8085948https://doi.org/10.1109/ITMQIS.2017.8085948

Designing an Algorithm to Support Optimized Crop Selection by Farmers



Mayank Phadke, Mridula Goel, Rishabh Bajpai, and Nishchay Mehta

Abstract In recent years, India has seen markets develop for a wide range of new crops, many of which have not been traditionally cultivated in the region. Various factors affect the productivity and profitability of crops, and farmers often have limited know-how regarding the suitability of new crops and varieties to soil and weather conditions, the requirement of fertilizers and other inputs, and cultivation practices. Their knowledge about market conditions is also lacking in such cases. In addition, even among conventional crops, hundreds of varieties with different characteristics are now available to farmers. In order to make informed decisions regarding crop and variety selection, a large amount of information must be processed. This information is often highly technical and is unavailable in regional languages. With an ever-expanding number of crops, varieties and processes, as well as rapidly changing climatic and market conditions, knowledge transfer through established agricultural extension services has become inadequate. The growth in mobile phone usage over recent years can promote the use of mobile applications for this purpose. Such an application can process agricultural information to help farmers make informed decisions regarding crop selection and help them achieve greater productivity and profitability. This paper discusses the frameworks used to develop *Krishi Mitr* (Farmer Friend), a mobile application that can enable farmers to select crops that are best suited to their soil and weather while factoring in the costs of inputs and labor, sustainability, pests and diseases, as well as market conditions. The variables that are included in arriving at the selection, the crop-selection algorithm, and the deployment of the *Krishi Mitr* mobile application has been detailed in this paper.

M. Phadke (✉) · M. Goel · R. Bajpai · N. Mehta
Birla Institute of Technology and Science, Pilani, K.K. Birla Goa Campus, Goa, India
e-mail: f20170625@goa.bits-pilani.ac.in

M. Goel
e-mail: mridula@goa.bits-pilani.ac.in

R. Bajpai
e-mail: f20170121@goa.bits-pilani.ac.in

N. Mehta
e-mail: f20170511@goa.bits-pilani.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_33

Keywords Farmers · Crop selection · Optimization algorithm · Mobile application · India

1 Introduction

India's agricultural sector has been plagued by low productivity, declining farm sizes, marginal landholdings, dependence on uncertain weather conditions, volatile prices, and an inadequate supply of labor [1]. Producing more food from less land, while making efficient use of natural resources, labor, and water will be a huge challenge in the coming years [1, 2]. Increasing globalization and commercialization has led to diversification in production and consumption and have provided access to several modern farming technologies, seed varieties, and even new crops. Markets for new kinds of agricultural commodities have emerged [3]. Over 350 distinct agricultural commodities are now produced in India, and many of the crops cultivated have many varieties. These varieties have distinct yields, varied crop cycles, and different levels of resistance to specific pests, diseases, or weather events. Export markets for a number of new crops have emerged. All such developments present farmers with the opportunity to increase farm productivity and grow their incomes [4].

However, to adequately leverage these advances, a robust information transfer framework needs to be in place. The solutions provided must be easy to use for a large number of Indian farmers. In India, the responsibility of disseminating agricultural information and practices has been placed upon public-sector agricultural extension services [5]. However, these services have failed to facilitate the transfer of technologies and modern practices to the farm level and account for only a small percentage of farmers' information sources [6, 7]. Thus, there exists a gap when it comes to knowledge transfer regarding good agricultural and crop management practices, selection of technologies relevant to the farm's geographical conditions and cropping system, appropriate quantities of agricultural inputs and their timely use, as well as contingency plans to deal with extreme weather events [8].

To address this problem, we have developed Krishi Mitr (Farmer Friend) as a mobile application. This application enables a farmer to select an optimal crop and variety based on productivity and profitability. The selection factors in the suitability of the crop to the farmer's soil and climate, crop duration, irrigation, soil conservation, probability of extreme weather events, and the cost of cultivation (fertilizer, pesticide, manure, harvesting, and transport costs). The design and implementation of this mobile application, its use-cases, benefits to farmers as well as future scope and limitations are discussed in the following sections.

2 Literature Survey

2.1 Factors that Affect Crop Selection

A large number of factors related to climatic and soil conditions, agricultural inputs, available labor (household and hired), seed availability, prices, specific government policy measures, along with the farmer's experience interact to influence the selection of crops, crop varieties, and cropping practices. These factors can be classified into five broad categories—natural resources, agricultural inputs and technologies, financial factors, policy factors, and household factors [3, 8].

Natural Resources. The amounts of primary soil nutrients—nitrogen, potassium, phosphorous, and organic carbon affect the growth of crops, and these are integral aspects of soil health. Micronutrients like Zn, B, S, Cu, Fe, and Mn also affect the yields [9]. Target yield equations can be used to calculate nutrient requirements for a crop based on existing levels in the soil and have been found to produce higher yields [10] while also using resources efficiently and maintaining soil fertility. Studies have found increases of 30 to 60% in crop yields when crop selection factors in soil health [11]. In recent years, soil conservation and sustainability have gained importance. Soil management can help to improve soil health and lead to greater sustainability [12].

The amount and schedule of rainfall, as well as temperature patterns, affect the yield and sowing time of most crops. Besides temperature and humidity, crop yields are affected by pest and disease infestations, extreme weather events such as wet or dry spells, cold waves, heat waves, droughts, cyclones, hail, frost, and floods, especially at critical stages of a crop [8].

Agricultural Inputs and Technologies. Careful selection of agricultural inputs like seeds, fertilizers, crop protection products (pesticides, herbicides, fungicides, insecticides) can lead to markedly higher yields. A large number of available crop varieties differ in their yields, growing periods, and resource requirements, and some of these are relatively resilient to pests, diseases, or weather events [13].

Indian farmers often rely on conventional agricultural practices and knowledge, and thus, the past and present experience of farmers has been an important factor in the selection of the crops and cropping systems. Cropping system options, post-harvest storage and processing facilities, labor inputs, scope for mechanization, and access to, and the applicability of modern technologies are all factors that can elevate productivity and influence crop selection [8].

Financial Factors. Landholding size affects the profitability and economies of scale associated with raising crops, while the availability of agricultural credit and insurance impacts the risks a farmer can take. The costs of agricultural inputs like seeds, fertilizers, pesticides, insecticides, herbicides, fungicides, and manure, as well as the cost of labor (human, animal and mechanical) and transportation, can impact the profitability of crop [14].

In recent years, the quantity of exports from India has grown significantly, with export-grade produce often attracting markedly higher rates. Thus, farmers need to factor in the global demand in addition to demand in local markets to increase profits [15]. Enhancing farm productivity needs to be coupled with profitable market outcomes to improve farmer income.

Policy Factors. Several policy measures related to subsidies, exports, imports, international quality standards, the quality and availability of extension services, as well as the availability of formal cultivation guidelines provided by these services can impact the profits and productivity associated with the cultivation of crops [16].

Household Factors. Income requirements, as well as food self-sufficiency needs of the farmer, household labor availability, literacy, risk-taking ability, and other demographic factors can have a substantial impact on the crops and processes that the farmer chooses [8].

2.2 Applications of Machine Learning (ML) in Crop Optimization

One of the primary applications of machine learning (ML) in agriculture has been to predict crop yields for farmers. The two most popular ways of applying ML have been to use soil nutrient information to predict crop yield using decision tree-based algorithms [17–20], and to use remote sensing data to create images to feed a convolutional neural network (CNN) [21] linked with long short-term memory (LSTM) networks to improve results [22, 23]. These methods require large amounts of farm-level data. However, there are no major studies in the Indian landscape that focus on collecting farm-level data. Data collection for crop yield prediction has been at the district or state level. Farm-level studies have been attempted in countries like Vietnam [17] and Pakistan [18] with encouraging results.

2.3 Applications of ICT in Agriculture

Information that is context-specific rather than generic and broad-based could help to increase farm productivity for marginal and small agricultural landholders [24]. Reliable, easily available, quality information to support farmers' decision-making can also reduce knowledge seeking and learning costs [25]. Studies on the development impact of mobile phone usage have concluded that mobile phones contribute to greater efficiency for farmers [26].

3 *Krishi Mitr* Mobile Application and Crop-Selection Algorithm

The *Krishi Mitr* mobile application has been designed to select the optimal crop for a farmer based on a number of variables. To obtain the optimal crop and variety, the fit of various crops and varieties to numerous farmer-specific agricultural and financial variables is considered, and then these crops and varieties are provided scores based on this fit. The structure of the application and the algorithms for optimal crop selection are discussed in subsequent sections. The first stage of the application is the generation of the user profile, and the data generated therefrom is applied in the crop-selection algorithm, which has three components- Natural Resource module, Agricultural Inputs and Technologies module, and Agricultural Finances module.

3.1 User Profile

In order to enhance accessibility and cater to India's semi-literate and literate farmers, the *Krishi Mitr* mobile application works with minimal user-data entry. The information provided by the farmer is supplemented with data from *Krishi Mitr*'s databases. This data flow is described in Fig. 1. The user profile has four components: location profile, farm profile, weather profile, and crop profile. During onboarding, the farmers

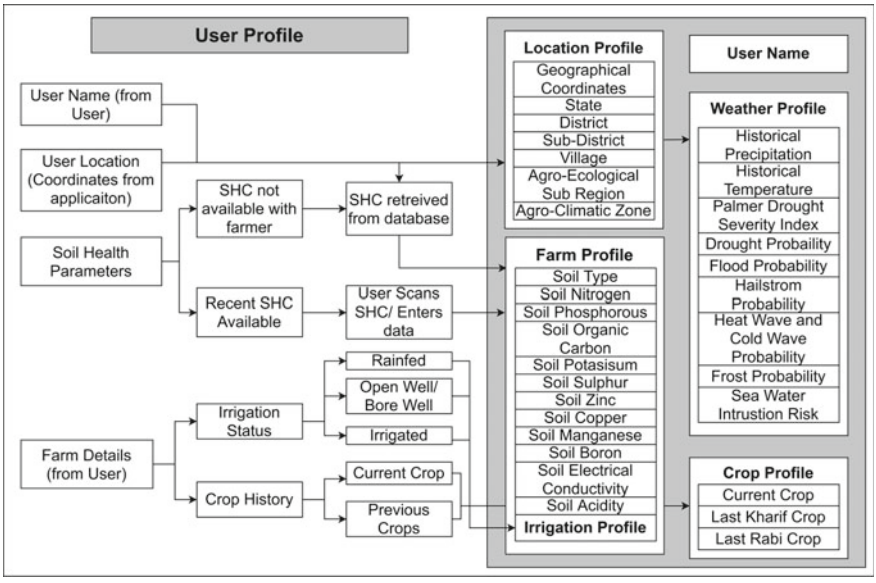


Fig. 1 Flowchart for generation of user profile

are required to provide their name and access to their location using Google Location Services. Based on the farmer's location (longitude and latitude), their district, sub-district, and village are determined,[1] and this is used to determine agro-climatic and agro-ecological zones [27]. These details constitute the location profile.

In case the farmer has conducted soil health tests recently, the farmer is required to provide this information, either by scanning the image of the government-issued soil health card (SHC) or by entering these details. If this data is unavailable to the farmer, the SHC data is retrieved from *Krishi Mitr's* cloud databases.[2] This is supplemented with farmer-provided information about the irrigation status of the farm. These details determine the farm profile. Based on the farmer's location profile, the application determines the farmer's weather profile, which is based on historical data,[3] current data[4] as well as weather predictions. This information is stored in cloud databases and includes data regarding precipitation, temperature, drought severity, and other climatic factors, as well as probabilities of extreme weather events.[5] To determine the crop profile, the farmer needs to provide details regarding the crops that the farmer has previously grown, and is currently cultivating.

3.2 Natural Resources Module

The first stage of the crop-selection algorithm is optimization based on natural resources and is described in Fig. 2. Through this module, the performance of various crops is calculated based on a range of factors, and scores are determined. The farm profile is used to match the type of soil in the field with the soil type most suited for each crop to refine the list of feasible crops. The adequacy of soil nutrients needed to achieve the target yield for any crop or variety is calculated based on targeted yield equations[6] and similarly, micronutrient requirements are also computed. Similarly, the weather profile is matched with the needs of the crop and the scores are calculated, as shown in Fig. 2. This module eliminates incompatible crops and determines fitment scores for the feasible crops based on the soil nutrient requirements, climatic factors, and irrigation. Special attention is given to the sustainability of cultivation in the scores as well, by prioritizing crops that require minimal chemical fertilizers.

[1] Source: Local Government Directory (https://lgdirectory.gov.in).

[2] Source: Soil Health Card (https://soilhealth.dac.gov.in).

[3] Source: TerraClimate Data (https://climate.northwestknowledge.net/TERRACLIMATE).

[4] Source: OpenWeather API (https://openweathermap.org/api).

[5] Source: Agriculture Contingency Plans- Department of Agriculture Cooperation & Farmers Welfare (https://agricoop.nic.in/agriculture-contingency-plan-listing).

[6] Source: ICAR-Soil Test Crop Response Studies (STCR) (https://aicrp.icar.gov.in/).

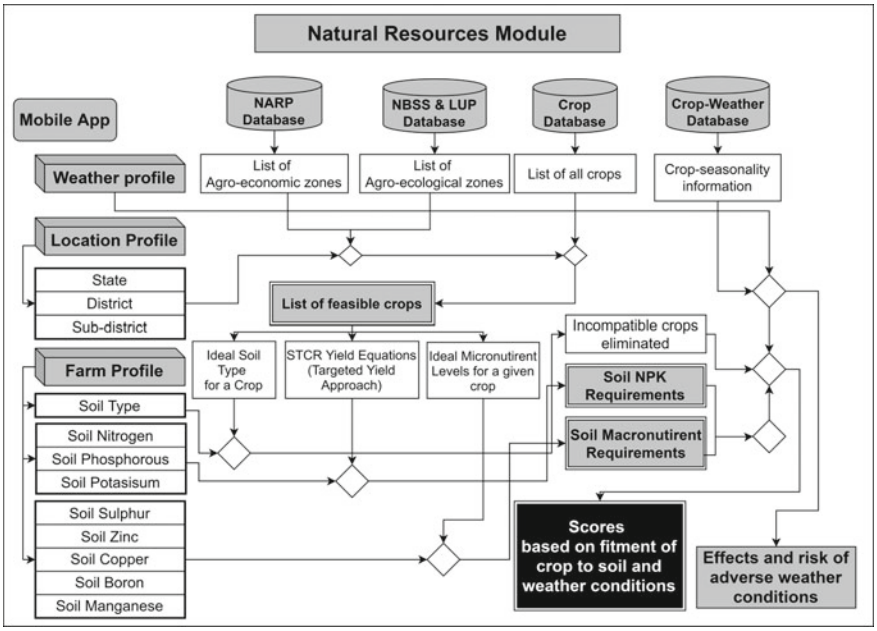


Fig. 2 Flowchart for natural resources module

3.3 Agricultural Inputs and Technologies Module

The Natural Resources module determines the list of feasible crops, the soil nutrient requirements for the crop, and the pests and diseases that crops in the region are susceptible to. This data is used in the Agricultural Inputs and Technologies module, as shown in Fig. 3. Through the Fertilizer database,[7] the algorithm determines the quantities of fertilizers required to satisfy nutrient requirements, while also factoring in the availability of the fertilizers.[8] Similarly, the Pesticide database is used to determine the quantity of pest and disease treatments required, based on probable pests and diseases. The Cost of Cultivation[9] database is then leveraged to determine the amount of human, animal, and mechanical labor required. Through the Package of Practices database,[10] the algorithm retrieves the post-harvest storage and processing

[7] Source: List of Fertilizers Notified Under FCO Schedule - I A-Central Fertilizer Quality Control & Training Institute (https://cfqcti.dacnet.nic.in/indfert.html).

[8] Source: Integrated Fertilizer Management System (iFMS)- Department of Fertilizers, Ministry of Chemicals & Fertilizers (https://urvarak.nic.in/).

[9] Source: Cost of Cultivation/Production & Related Data- Directorate of Economics and Statistics-Ministry of Agriculture and Farmer Welfare (https://eands.dacnet.nic.in/).

[10] Source: Package of Practices- Department of Agriculture & Cooperation and Farmers Welfare (https://farmer.gov.in/mpopreports.aspx).

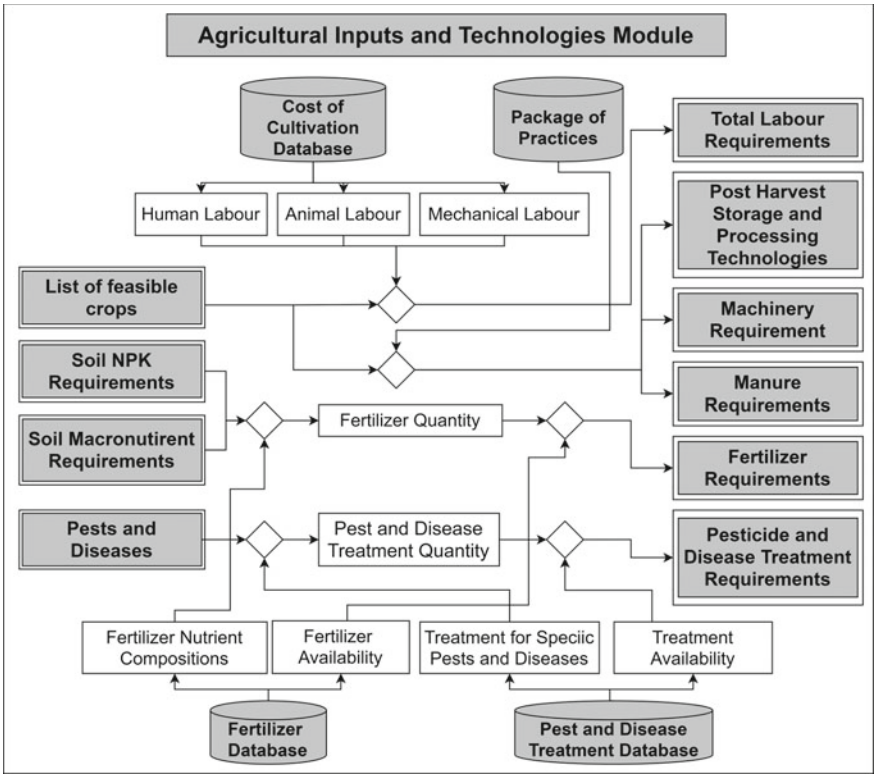


Fig. 3 Flowchart for agricultural inputs and technologies module

technologies as well as the machinery requirements for the crop. This data is then utilized to determine the costs of these inputs in the agricultural finances module.

3.4 Agricultural Finances Module

From the two previous modules, the quantity of agricultural inputs is determined. Based on these requirements and the costs of these inputs, the total costs involved are determined and the design of the agricultural finances module is given in Fig. 4. Based on the location of the user, the agricultural marketplaces in proximity to the

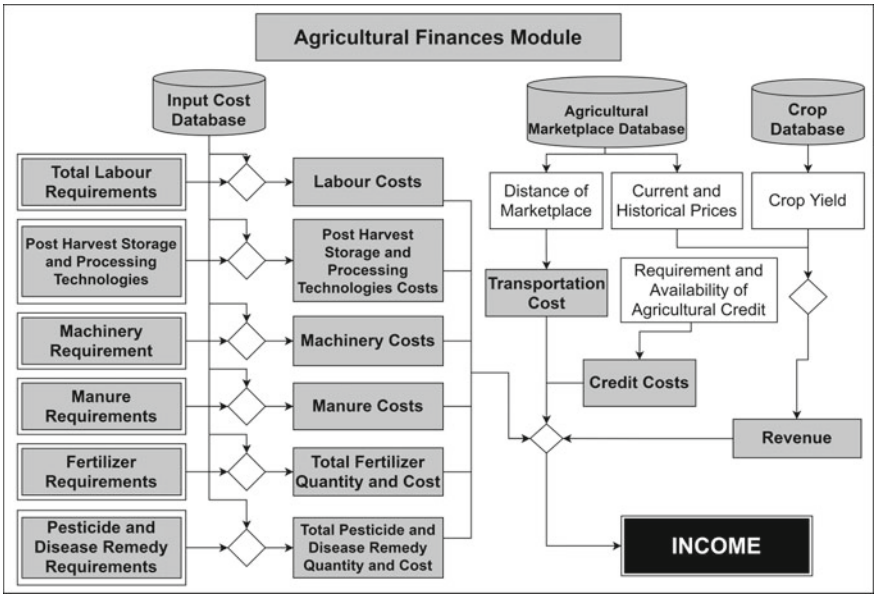


Fig. 4 Flowchart for agricultural finances module

farmer are identified, and the current[11] and historical prices[12] of the selected crops and agricultural commodities at these marketplaces are considered. Based on the distance between the farm and the marketplaces, the cost of transportation is determined. The target yields[13] for the crops and the respective crop prices determine the revenue earned by the farmer, and when the total cost of cultivation is subtracted from this, the farmer's income is determined.

3.5 Determining the Final Recommendations for Farmers

The final recommendations provided to the farmer are based on the scores in the natural resources module and the income estimated by the agricultural finances module. The incomes and scores are ranked and the optimal crops and varieties are presented to the farmer. To support the farmer through the process of raising the

[11] Source: API for Current Daily Price of Various Commodities from Various Markets (Mandi)- Ministry of Agriculture and Farmers Welfare- Department of Agriculture, Cooperation and Farmers Welfare- Directorate of Marketing and Inspection (DMI).

[12] Source: Variety-Wise Prices of Various Agricultural Commodities- Ministry of Agriculture and Farmers Welfare- Department of Agriculture, Cooperation and Farmers Welfare- Directorate of Marketing and Inspection (DMI).

[13] Source: ICAR-Soil Test Crop Response Studies (STCR) (https://aicrp.icar.gov.in/).

crops, the farmer is provided additional information about cultivation practices that can facilitate better productivity.

4 Deployment of the *Krishi Mitr* Mobile Application

The *Krishi Mitr* application has been deployed in the form of an Android application and some of the screens of this application are shown in Fig. 5. Compatibility has been retained for API levels 23 and above (i.e., Android Marshmallow or later) and the bulk of the processing is run on an AWS Lambda instance. This approach keeps the whole system serverless and hence immensely scalable. The Lambda code uses DynamoDB to store and process data. The request between the server and the application is handled through a RESTful Application Programming Interface (REST APIs), and this client–server model helps in expanding the services to multiple types of clients in the future [28].

The application handles some sensitive personal data like the user's mobile number and farm equipment information. To handle the privacy concerns that arise when working with such data, we adopt the following procedures. The APIs work on an HTTPS protocol, to ensure each message is encrypted. The requests are handled by Amazon's API Gateway which when combined with AWS Web Application Firewall (WAF) prevents exploitative attacks that may try to steal user information. As an added level of security, each service on the REST API framework works with its own identity and access management (IAM) profile to compartmentalize the work of each module so that an exploited module cannot be used to perform tasks outside its intended use. The entire cloud architecture works on a virtual private network so that only the lambda instance which resides inside it can communicate with the databases and no outside requests can be made to any components of the system.

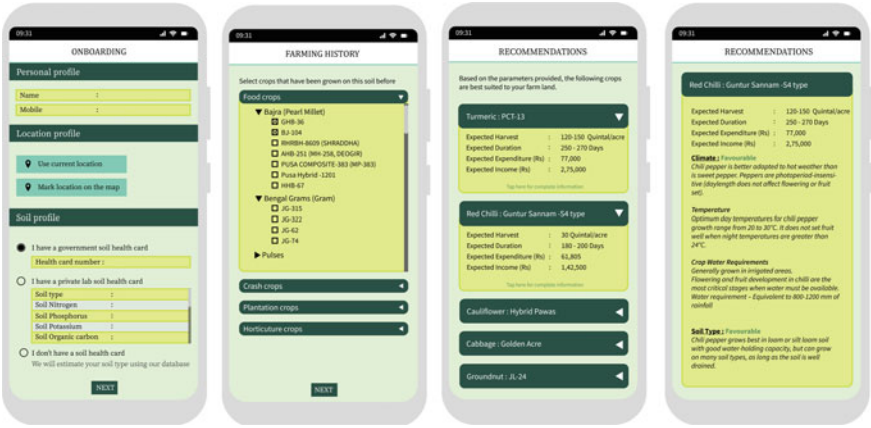


Fig. 5 Selected screens from the *Krishi Mitr* mobile application

5 Limitations and Future Scope

Among the five types of factors that determine crop selection (as discussed in Sect. 2.1), the algorithm discussed above addresses the first three. Policy factors and household factors have not been addressed, and integrating these factors will further enhance the accuracy and relevance of the recommendations provided.

In the current algorithm, the yields for crops are taken to be the target yields provided by ICAR and other agricultural research institutes. Employing machine learning with remote sensing data to feed a convolutional neural network (CNN) linked with long short-term memory (LSTM) networks can help to predict crop yields accurately, and implementing this into the application can further enhance the recommendations provided to farmers [22].

Governments, NGOs, and some firms are making efforts to make soil tests more accurate and easily available. As the quality and frequency of soil test data improve, the accuracy of the recommendations provided by the *Krishi Mitr* application will also increase.

6 Conclusion

The Indian agricultural sector has faced stagnating productivity and diminishing profit margins [29]. Rapidly changing climates and volatile markers have added to the pain of India's farmers. The emergence of markets for an increasing number of crops, and the development of several new crop varieties and cultivation processes have enabled farmers to dramatically increase their incomes through careful, knowledge-backed selection of crops and varieties. A mobile application supported by a backend server can enable farmers to make these decisions efficiently by easily processing the large amounts of information required to select the crop and variety. The *Krishi Mitr* Android mobile application is an effort in this direction and can help farmers improve farm yields and agricultural income by selecting an optimal crop based on a variety of factors. The numerous variables factored in for this decision-making process have been discussed in this paper. The design of the crop-selection algorithm, and its three decision modules have been demonstrated and the corresponding flowcharts have been specified. Additionally, the deployment of these algorithms into a mobile application has also been discussed.

The *Krishi Mitr* application can be used by agricultural extension services, NGOs, and Farmer Producer Organizations (FPOs) and individual farmers to help determine the profit-maximizing crop according to their soil, climate, and numerous other factors. By combining emerging knowledge and technologies with the experience of India's farmers, *Krishi Mitr* aims to enable India's farmers to sustainably increase their profit margins and help accelerate the development of the agricultural sector.

References

1. T. Deshpande, State of Agriculture in India, PRS Legislative Research, 2017. [Online]. Available: https://prsindia.org/policy/analytical-reports/state-agriculture-india
2. The World Bank Group, India: Issues and Priorities for Agriculture, 2012. https://www.worldbank.org/en/news/feature/2012/05/17/india-agriculture-issues-priorities. Accessed 22 Apr 2021
3. C. Hazra, Crop diversification in India, in *Papademetriou MK, Dent Frank J, Editors. Crop diversification in the Asia-Pacific region Food and Agriculture Organization of the United Nations*, pp. 32–50, 2001
4. Ministry of Agriculture & Farmers Welfare, Department of Agriculture, "Agricultural Statistics at a Glance 2018," Government of India, Ministry of Agriculture & Farmers Welfare, Department of Agriculture, Cooperation & Farmers Welfare, Directorate of Economics and Statistics, New Delhi, 2018. Accessed: Apr. 22, 2021. [Online]. Available: https://agricoop.gov.in/sites/default/files/agristatglance2018.pdf
5. V.K. Sajesh, A. Suresh, Public sector agricultural extension in India-A note, Rev. Agrarian Stud. 2016
6. A. Upadhyay, G. Papnai, S.P. Singh, Challenges of agricultural extension system in India: review and a view, *Agriways: a multi disciplinary journal Research and education development society,* vol. 1, pp. 49–53, 2013. ISSN 2321-8614
7. P. Paolo Ficarelli, C.J. Glendenning, The relevance of content in ICT initiatives in Indian agriculture, in *International Food Policy Research Institute (IFPRI)*, IFPRI Discussion Paper 01180, 2012. [Online]. Available: https://www.ifpri.org/publication/relevance-content-ict-initiatives-indian-agriculture
8. P. Chandra Shekara et al., *Farmer's Handbook on Basic Agriculture.* 2nd ed. Navsari, Gujarat, India: Desai Fruits & Vegetables Pvt. Ltd., 2016
9. T. Liliane, C. Mutengwa, Factors affecting yield of crops, 2020
10. ICAR, *Four Decades of STCR Research—Crop Wise Recommendations (AICRP on STCR).* Bhopal: Indian Institute of Soil Science
11. S. Wani, K. Anantha, K. Garg, Soil Properties, Crop Yield, and economics under integrated crop management practices in Karnataka, Southern India, *World Development*, vol. 93, 2017, https://doi.org/10.1016/j.worlddev.2016.12.012
12. K. Tuğrul, Soil management in sustainable agriculture, 2019
13. Organisation for Economic Co-operation and Development, Adoption of technologies for sustainable farming systems: Wageningen workshop proceedings, Paris, 2001
14. Ministry of Statistics and Programme Implementation, Manual on Cost of Cultivation Surveys, MoSPI, New Delhi, 2008. [Online]. Available: mospi.nic.in/sites/default/files/publication_reports/manual_cost_cultivation_surveys
15. D. Kahan, *Managing Risk in Farming* (Food and Agriculture Organization of the United Nations, Rome, 2008)
16. A High-Level Expert Group (HLEG) on Agriculture Exports, "Growing India's agricultural exports through crop-specific, state-led plans," Jul. 2020. [Online]. Available: https://fincomindia.nic.in/writereaddata/html_en_files/fincom15/StudyReports/HLEG%20Report_Agriculture_vF.pdf
17. P. Charoen-Ung, P. Mittrapiyanuruk, Sugarcane Yield grade prediction using random forest with forward feature selection and hyper-parameter tuning, pp. 33–42 2019
18. I. Ahmad, et al., Yield Forecasting of spring maize using remote sensing and crop modeling in Faisalabad-Punjab Pakistan. J. Indian Soc. Remote Sens. **46**, 2018. https://doi.org/10.1007/s12524-018-0825-8
19. P. Filippi et al., An approach to forecast grain crop yield using multi-layered, multi-farm data sets and machine learning. Precision Agric. **20**, 1–15 (2019). https://doi.org/10.1007/s11119-018-09628-4
20. X. Xu et al., Design of an integrated climatic assessment indicator (ICAI) for wheat production: a case study in Jiangsu Province, China. Ecol. Ind. **101**, 943–953 (2019). https://doi.org/10.1016/j.ecolind.2019.01.059

21. T.V.N. Rao, S. Manasa, Artificial neural networks for soil quality and crop yield prediction using machine learning, Int. J. Future Revolution Comput. Sci. Commun. Eng. **5**(1), 2019
22. S. Sharma, S. Rai, and N. Krishnan, *Wheat Crop Yield Prediction Using Deep LSTM Model*. 2020
23. A. Wang, C. Tran, N. Desai, D. Lobell, S. Ermon, *Deep Transfer Learning for Crop Yield Prediction with Remote Sensing Data*. 2018, p. 5
24. A. Samaddar, Traditional and posttraditional: a study of agricultural rituals in relation to technological complexity among rice producers in Two Zones of West Bengal, India. Cult. Agric. **28**, 108–121 (2008). https://doi.org/10.1525/cag.2006.28.2.108
25. R. Llewellyn, Information quality and effectiveness for more rapid adoption decisions by farmers. Field Crop. Res. **104**, 148–156 (2007). https://doi.org/10.1016/j.fcr.2007.03.022
26. A. Rashid, L. Elder, Mobile Phones and development: an analysis of IDRC-Supported projects, EJISDC: Electr. J. Inf. Syst. Dev. Countries **36**, 2009. ISSN 1681–4835. https://doi.org/10.1002/j.1681-4835.2009.tb00249.x
27. A. Balasubramanian, *Agro-Ecological Zones of India*. 2013
28. L. Fennelly, *Handbook of Loss Prevention and Crime Prevention*, 6th ed. Butterworth-Heinemann, 2019
29. A.C. Dhas, Agricultural crisis in India: the root cause and consequences, University Library of Munich, Germany, 2009. [Online]. Available: https://ideas.repec.org/p/pra/mprapa/18930.html

Security in Industrial Control Systems Using Machine Learning Algorithms: An Overview



Pallavi Arora, Baljeet Kaur, and Marcio Andrey Teixeira

Abstract Since tiny pocket-sized individual gadgets (e.g., smartphones) together with big computing appliances or solutions (e.g., cloud computing or net banking) are pervasive in today's world, innumerable data bytes are created, stored, interchanged, yielded, and used to produce results in particular applications every minute. As a result, protecting data, computers (gadgets), as well as consumer anonymity in cyber sphere comes out to be a top priority for oneself, businesses, and governing bodies around the world. Machine learning (ML) is becoming popular in cybersecurity in recent years, with applications such as intrusion disclosure and biometric-based customer validation. However, both the training and testing phases of machine learning algorithms are prone to attacks, resulting in significant performance drops and security breaches. This paper intends to provide an overview of challenges faced by machine learning solutions for ICS and IIoT devices. It also presents thorough discussion of literature regarding security concerns of IIoT.

Keywords Machine Learning · ICS · Security · Internet of Things

1 Introduction

Industrial Control System (ICS) is a broad concept which embraces a wide range of control systems, comprising supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and additional control system configurations including programmable logic controllers (PLC). An ICS is a collection of

P. Arora (✉)
IK Gujral Punjab Technical University, Kapurthala, India

B. Kaur
Guru Nanak Dev Engineering College, Ludhiana, India
e-mail: baljeetkaur@gndec.ac.in

M. A. Teixeira
Federal Institute of Education, Science, and Technology of São Paulo, Catanduva, SP, Brazil
e-mail: marcio.andrey@ifsp.edu.br

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_34

devices (without wire or with wire) and control components (e.g., electrical, mechanical, hydraulic, and pneumatic) that work together to achieve a variety of industrial goals (e.g., producing, transportation of material or power). A typical ICS includes a variety of control loops, Human–Machine Interfaces (HMIs), and distant analysis and sustenance equipment, all of which are designed using a set of network protocols.

SCADA systems collect statistics deriving out of and issue directions to topographically distant ground bases to track as well as manage various Industrial Control System components. SCADA and DCS systems are often linked to work in tandem. Despite the fact that a DCS controls the operation of the industrial plant, it has got to correspond alongside the SCADA system in order to align generation productivity alongside dissemination and dispensation requirements. ICSs seemed withheld from the World Wide Web for a significant time, until recently. Communication between remote components took place over private networks using custom protocols such as Modbus RTU, Modbus TCP, or Wi-Fi, Zigbee, etc. Nevertheless, lately, various sectors are perceiving the perks which might be descended from the Internet as well as Information Technology (IT) environment, such as cloud computing [1].

The commercial enterprises gadgets used in ICS previously aren't having Internet connections. That is to say, the devices were connected internally but not externally. With this perspective, the ICS intercommunication decorum was created devoid of safety frameworks such as cryptography and safety layers leading to an increase in the risk of ICS attacks due to internet connectedness. Established IT remedies at primary supervision bases solitarily protect as well as reinforce the ICS installation's inlying foundation, leaving remote gadgets unguarded to malicious hacks. ICS previously relied on protection through the consistency of being challenging to comprehend. While the usage of open-source framework mechanisms has made ICS fragile to malicious attacks and network malware infiltration. The haphazard installation of software, cryptography, and virus security applications provides a pseudo sense of safety to system administrators.

The Industrial Internet of Things (IIoT) refers to a set of industrial equipment's that is configured with sensors and is linked to networks to collect and share data. For many businesses, the combination of industrial IoT and intelligent automation has become a boon, enabling machines to perform activities that previous waves of automation couldn't. On the other hand, as industrial computers have been attached to the Internet, the number of cyber-attacks has increased. Studies have been carried out to prevent attacks in ICS networks, and include the use of machine learning algorithms to detect attacks in the ICS network [2, 3].

2 Attacks on IIoT

A cyberattack is a noxious and intentional endeavor by an individual or association to penetrate the data arrangement of another individual or association.

Typically, the intruder hopes to gain advantage by compromising the victim's network [4]. Figure 1 depicts several types of cyber-attacks.

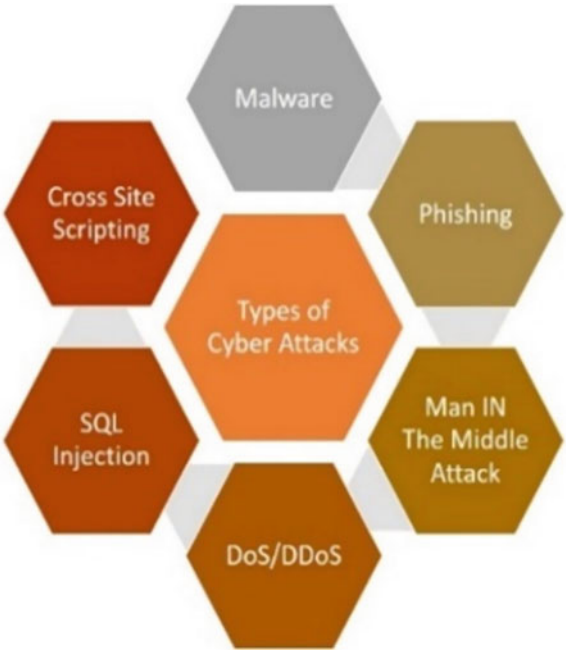


Fig. 1 Types of cyber-attacks

- Malware: Malware infiltrates a network by exploiting a vulnerability, such as when a user clicks on a malicious link or email attachment, it installs harmful software. Malware can do the following after it has gained access to the system: Connection to critical network elements is disabled (ransomware), Malware or other potentially dangerous software is installed. By transmitting data from the hard disc, it obtains information invisibly (spyware) and certain components are disrupted, rendering the device inoperable.
- Structured Query Language (SQL) injection: A SQL injection happens when an attacker injects malicious code into a server that uses SQL, forcing the server to disclose details it would not usually reveal. An attacker may perform a SQL injection by typing malicious code into a search box on a compromised website.
- Phishing: Phishing is the method of transmitting forged emails that seem to come from a trustworthy source. The aim is to steal personal information such as credit card numbers and passwords, or to infect the victim's computer with malware. Phishing is becoming a pretty popular cyber-threat.
- Man-in-the-middle attack: Eavesdropping attacks, also known as man-in-the-middle (MitM) attacks, occur when an attacker inserts himself into a two-party conversation. The attackers will then filter and steal data after interrupting the traffic. MitM attacks usually begin in one of two ways: (a) When using unsecure public Wi-Fi, attackers can position themselves between a visitor's device and the network. The visitor unintentionally gives the intruder all of his details; (b)

Once malware has infiltrated a computer, the intruder will install software that will process all the victim's data.

- Denial-of-service attack: During a denial-of-service attack, data is flooded into devices, servers, or networks in order to exhaust resources and bandwidth. Consequently, valid demands are unable to be fulfilled by the system. This attack can also be launched using multiple compromised computers. That is called a distributed-denial-of-service (DDoS) attack.
- Cross-Site Scripting (XSS): The injection of malicious code into a compromised web application is known as cross-site scripting (XSS). In contrast to other web attack vectors (such as SQL injections), XSS does not explicitly target the application. Instead, it is the web application's users that are at risk.

3 Machine Learning in ICS Security

Machine learning methods can provide valuable security knowledge for a variety of physical problems and realistic contexts. Strategies in automated machine learning are more standardized, organized, and master able. Such opportunities create new avenues for responding to the challenge of reliably developing as well as managing upcoming manufacturing network systems in a secure manner [5].

SCADA systems, for example, have very repetitive communication patterns. A restricted collection of read and write prompts is often replicated in kind of a ring. The operation of gas pipelines proposed by [6], for example, loops the same two commands. It starts by writing the components of the all register and then controls itself with coils. The system's calculated state is then read using a Modbus read command. Many ICSs, especially SCADA systems, use the Modbus protocol. It includes a master/slave specification that prohibits the slave from making any requests for information. It just listens to the master's orders. Data is transferred via serial lines (Modbus RTU/ASCII) or Ethernet (Modbus TCP). A set of two responses follows these two commands. As a consequence of this consistency, a set of directives appears wherein all interface attributes are the same and every one of the four packages is just the same size. Such a dearth of diversity is to be anticipated. Machine learning algorithms may take advantage of these standard patterns to construct models of natural state and identify odd anomalies.

3.1 Intrusion Detection System

The Intrusion Detection System is a typical framework for keeping track of and checking activities in a computer network environment for signs of possible threats and detect suspicious activities. An IDS is a tool or software program that detects such intrusions. The introduction of machine learning has enhanced the performance of IDS and facilitated the detection of unintended intrusions (Fig. 2).

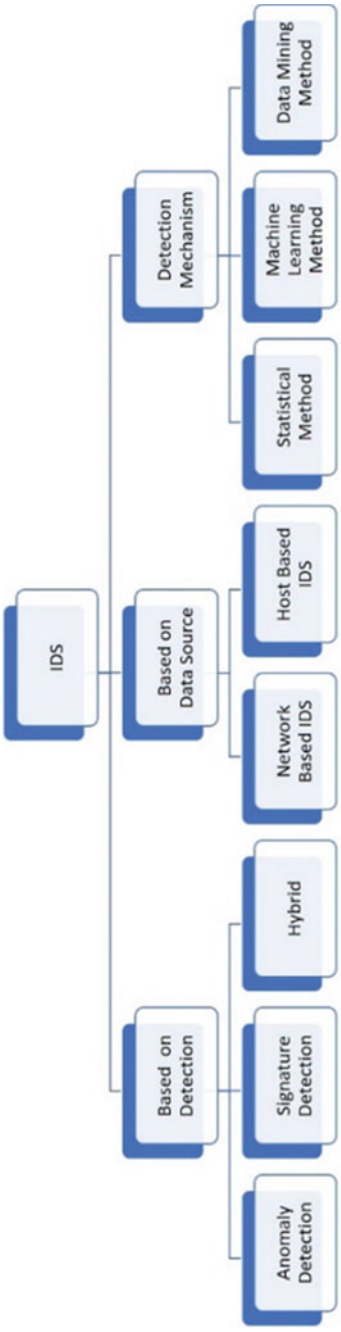


Fig. 2 Taxonomy of intrusion detection systems

There are three main categories of cyber analytics for intrusion detection systems. Misuse-based, anomaly-based, and hybrid-based detections are available [7]. For the detection of known threats, signature/misuse-based detection is used. The normal behavior is monitored using anomaly-based detection and distinguishes between irregular network and device behavior. Finally, the hybrid-based detection approach improves detection accuracy by combining both misuse-based and anomaly-based techniques. Attackers could be able to exploit bugs in these conventional defense approaches, putting the user's security against unknown and emerging threats in jeopardy. The amount of data in cyberinfrastructure is immense. Unauthorized access to the data is attempted by criminals. It is crucial to understand the patterns and behaviors of intrusions and assaults. As a result, machine learning methods are critical in detecting and predicting potential intrusions and assaults.

Network Intrusion Detection Systems (NIDS) track traffic from all devices entering and exiting the network at the network level. The NIDS analyses the traffic in order to spot trends and suspicious activities, after which an alert is sent. The following are some of the benefits of NIDS: With limited downtime, NIDS can be easily integrated into an existing network. Attackers can go undetected, and they are often impervious to direct attacks. They cannot always manage huge amounts of traffic and cannot analyze encrypted data or broken packets, to name a few drawbacks. HIDS tracks device data and looks for malicious behavior on a single host, unlike NIDS, which watches the entire network. HIDS will take snapshots and raise an alarm if they alter maliciously over time. The following are some of the benefits of a host-based IDS: HIDS can read encrypted data packets and detect threats that are difficult to detect. Audit logs provide information that can be used to track device and application program changes. The following are some significant drawbacks: They are also vulnerable to a direct attack on the host's operating system. It can use up a lot of disk space, putting a strain on the host's resources.

Internal changes (e.g., a virus inadvertently downloaded by an employee and spreading within your device) can be detected by a host-based intrusion detection system, while a network-based IDS can detect malicious packets when they reach your network or suspicious activity on your network, such as flooding attacks or protocol-specific attacks.

4 Literature Review Regarding IIoT Security

In our previous published work [8], different machine learning (ML) algorithms such as Random Forest (RF), Support Vector Machine (SVM), Decision Tree (DT), Artificial Neural Networks (ANN), K-Nearest Neighbors (KNN), and Naive Bayes (NB) are evaluated, and their efficiency metrics are recorded for attacks detection against ICS. The result demonstrates excellent machine learning algorithm execution in detecting assaults, as well as a low erroneous alert rate, implying that it accurately identifies normal traffic. Table 1 illustrates an overview of various machine learning techniques to detect intrusion and their associated performance metrics.

Table 1 A comparison of ML models for IDS and associated performance metrics

Year	References	Dataset	Learning model	Attack types	Metrics used for evaluation		
					Accuracy	Precision	Recall
2021	[8]	Customized	RF, SVM, DT, ANN, KNN, and NB	Reconnaissance, response injection, command injection, DoS	x	–	–
2020	[9]	Customized	Adaboost, J48, SVM,NB,RF	DDoS	–	x	x
2019	[10]	Customized	RF, DT, KNN, LR, SVM, ANN, NB	Backdoor attacks, SQL Attack, command injection attack	x	–	–
2018	[11]	KDD, Cup'99 and NSL-KDD	Deep neural network	Normal, DoS, Probe, R2L, U2R	x	x	x
2018	[12]	NSL-KDD	Deep learning Approach	Normal, DoS, Probe, R2L, U2R	x	x	x
2018	[13]	NSL-KDD	SVM (Linear), SVM (RBF), RF, and ELM	–	x	x	x
2017	[14]	Weka minable arff format	OneR, Naïve Bayes, Random Forest, J 48	–	–	x	x

The Industrial Internet of Things (IIoT) is a key part of building manufacturing facilities, providing interconnection and information via different sensors and electronic controls with universal networking and data capabilities. For IIoT implementation and industrial automation, cyber defense is a big concern. Safety concerns have now been prioritized by IIoT suppliers. [15]. The following literature shows importance of security in IIoT systems.

Authors in [16] have divided safety problems in IIoT systems into two sections based on a survey of recent research work on IIoT security: (a) safety issues which apply to IoT as well as IIoT, and (b) safety issues unique to manufacturing structure. Data protection, Cyber-Physical Systems (CPS) safety, development of keys for gadgets linking, and data control are among the most recent research interests on these security challenges. To address the security issues that IIoT has introduced to conventional industry systems, new security designs and practices are needed. Privacy protection is among the most serious challenges with both IoT and IIoT. Researchers

are developing more reliable and realistic attestation schemes for inexpensive and reserve restrained IIoT packed up gadgets. How to handle massive deployments of devices effectively and safely is the budding problem in the IoT/IIoT circumstance. Blockchain technology may be a potential option for handling IoT/IIoT products, as it has been widely utilized for authorized identification verification, possession monitoring, and product surveillance. To ensure good scalability and lightweight architecture, the authors in [14] suggested a moment authentication protocol, a credential protocol for accelerated transfer validation, and a Distributed Throughput Management (DTM) framework for the blockchain network that handled transfers among IoT devices.

In [17], the research article gives an outline of the IIOT, its evolvement, remolding into IIOT, structure, casebook, and applications of IIOT in industry. The goal of this research is to assess the current state of IIOT in the current situation and make few recommendations for potential research worker. As a result, a framework that uses IIOT should also examine the above technique/technology for protection. The authors have also discussed various applications of IIoT in business areas and considers predictive monitoring maintenance to be most important one. Machine learning is used to integrate quite so many objects tracking as necessary, including motion, heat, moisture, pressure, power, and so on. Some machine learning algorithms are capable of foreseeing failure. Every business strives to have as few injuries, environmental incidents, safety incidents, and breakdowns as possible. A computer's detectors will check the device's wellbeing pieces of information and send out warnings if appropriate, but they cannot predict why or when the system will malfunction. Rather than just reporting results, forecasting sustenance's goal is to develop a system that can provide reliable possibility predictions. In future works, the authors suggested more research to be done on the security problems surrounding IIOT.

Authors in [1] examine the transition of the ICS from stand-alone platforms to cloud-based frameworks. They looked at how business and academic institutions have contributed to the development of stable ICSs, with an emphasis on the usefulness of machine learning methods to ICS computer safety. The research could aid in addressing the challenges of securing industrial processes, particularly as they migrate to cloud environments.

The rapid growth of Internet interdependencies has resulted in an increase in cyber-attack events, many of which have catastrophic and dangerous repercussions. Malware is the most common tool used to carry out malicious intents in cyberspace, either by exploiting existing vulnerabilities or by taking advantage of unique features of technological developments. The development of more innovative and effective malware defense mechanisms is seen as a pressing need in the cybersecurity sector [18].

5 Conclusion

The cybersecurity of ICS and IIoT devices is paramount. There is still a significant gap in ensuring proper protection for these technologies, that's why focusing on the industrial side of IoT technology is critical. Machine learning solutions have been widely used to maintain a secure environment in ICS and IIoT applications. However, the prevalent cyber-risks of ICS and conventional IT systems vary due to structural discrepancies and divergent interests. As a result, special consideration must be given to IIoT protection. A literature review of existing anomaly-based approaches for SCADA systems that use machine learning was presented and also demonstrates security concerns encompassing IIoT. Our future work will include the generation of secured machine learning models in ICS and IIoT networks to detect and mitigate the attacks on these networks.

References

1. D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin, Cybersecurity for industrial control systems: a survey. Comput. Secur. J. **89**, 1–10 (2020)
2. K. Shaukat, S. Luo, V. Varadharajan, I.A. Hameed, M. Xu, A survey on machine learning techniques for cyber security in the last decade. IEEE Access **8**, 222310–222354 (2020)
3. H. Chen, M. Hu, H. Yan, P. Yu, Research on industrial internet of things security architecture and protection strategy, in *International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*. IEEE, Jishou, China, pp. 365–368 (2019)
4. J. Sengupta, S. Ruj, S.D. Bit, A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. J. Netw. Comput. Appl. **149**, 1–20 (2020)
5. F. Hussain, R. Hussain, S.A. Hassan, E. Hossain, Machine learning in IoT security: current solutions and future challenges. IEEE Commun. Surv Tutorials **22**(3), 1686–1721 (2020)
6. W. Zhang, X. Cao, D. Hu, Q., C., Liang, P., Qin, Y.: Research on FPN-based security defense model of oil and gas SCADA network. Computional Intelligence in Industrial Application, 1 ed., CRC Press (2015).
7. J.M.A. Jabraeil, B. Bahrami, A. Heidari, P. Allahverdizadeh, F. Norouzi, IoT Security, in *Towards the Internet of Things. Springer International Publishing*, Cham, pp 33–83 (2020)
8. P. Arora, B. Kaur, M.A. Teixeira, Evaluation of machine learning algorithms used on attacks detection in industrial control systems. J. Instit. Eng. (India): Series B, **102**(3), 605–616 (2021)
9. S. Sen, K.D. Gupta, A.M.D. Manjurul, Leveraging machine learning approach to setup software-defined network (SDN) controller rules during DDoS attack, in Uddin M.S., Bansal J.C. (eds.), *Proceedings of International Joint Conference on Computational Intelligence.* Springer Singapore, Singapore, pp. 49–60 (2020)
10. M. Zolanvari, M.A. Teixeira, L. Gupta, K.M. Khan, R. Jain, Machine learning based network vulnerability analysis of industrial Internet of Things. IEEE Internet Things J. **6**, 6822–6834 (2019)
11. N. Shone, T.N. Ngoc, V.D. Phai, Q. Shi, A deep learning approach to network intrusion detection. IEEE Trans. Emerging Topics Comput. Intell. **2**(1), 41–50 (2018)
12. M. Al-Qatf, Y. Lasheng, M. Al-Habib, K. Al-Sabahi, Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. IEEE Access J. **6**, 52843–52856 (2018)
13. I. Ahmad, M. Basheri, M.J. Iqbal, A. Rahim, Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection. IEEE Access J. **6**, 33789–33795 (2018)

14. R. Das, T.H. Morris, Machine learning and cyber security, in *2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE).* IEEE, Kolkata, pp 1–7 (2017)
15. A. Hassanzadeh, S. Modi, S. Mulchandani, Towards effective security control assignment in the Industrial Internet of Things, in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT).* IEEE, Milan, Italy, pp. 795–800 (2015)
16. X. Yu, H. Guo, A survey on IIoT security, in *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS).* IEEE, Singapore, pp. 1–5 (2019)
17. A. Karmakar, N. Dey, T. Baral, M. Chowdhury, M.D. Rehan, Industrial Internet of Things: a review, in *International Conference on Opto-Electronics and Applied Optics (Optronix).* IEEE, Kolkata, India, pp. 1–6 (2019)
18. J. Jang-Jaccard, S. Nepal, A survey of emerging threats in cybersecurity. J. Comput. Syst. Sci. **80**, 973–993 (2014)

Channelising Digitalisation Amidst COVID-19 Outbreak: Case of Multichannel ICTs in Pakistan



Bisma Iftekhar and Hasnain Bokhari

Abstract The Coronavirus outbreak in 2020 brought the world to a standstill. In the aftermath of COVID-19, communication technologies were greeted as exquisite mode of virtual interaction and collaboration. However, COVID-19 soon started stripping several sectors off their digital pride by exposing under-digitalisation, rate of technology adoption and/or infrastructural gaps particularly in low-income countries. This paper looks at Pakistan's approach towards ICTs and digitalisation particularly during the pandemic. The paper highlights the alternative channels of communication that has led to an increasing number of electronic services despite the reduced teledensity and broadband penetration. The paper explores the case of branchless banking as well as the role of digital identity that has been crucial for health, education and social sector in Pakistan.

Keywords ICTs · eGovernment · COVID-19 · Multichannel

1 Introduction

The Coronavirus outbreak brought the lives to a standstill and the lockdowns announced in March 2020 to reduce the pandemic forced several people to stay at and work from home. In the aftermath of Covid-19, information and communication technologies (ICTs) and digitalisation were greeted as exquisite mode of virtual interaction and collaboration. During the early days of lockdown, there seemed to be an unparalleled enthusiasm about ubiquitous ICTs and "ease" of working from home. However, COVID-19 soon started stripping several sectors off their digital pride by exposing under-digitalisation, rate of technology adoption and/or infrastructural gaps [1]. Within the education sector, schools were the worst hit as the

B. Iftekhar (✉)
Willy Brandt School of Public Policy, University of Erfurt, Erfurt, Germany
e-mail: bisma.iftekhar@uni-erfurt.de

H. Bokhari
University of Erfurt, Erfurt, Germany
e-mail: hasnain.bokhari@uni-erfurt.de

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_35

teaching staff and the pupils struggled with the technological apertures. This situation was even worse for middle- and low-income countries where ICT standards and infrastructure are still in developing phase and digital divides are rampant. COVID-19 threw several low-income countries under the bus as the informal economic sector(s) came under serious jeopardy. Pakistan is among those low-income countries whose 60 million labour force also largely engages in the informal economy [2]. As the sixth most populous country, Pakistan is struggling to provide basic necessities to its 50 million population living below the poverty line [3]. Ambushed with already inflating economy, COVID-19 brought Pakistan further down its knees, and it found itself on a crossroads before stumbling upon Coeckelbergh's [4] vehement reminder, Digitise or Die!

The extent to which it holds true for Pakistan is worth exploring. Is the success of the transition to the "new normal" contingent upon how quickly any country responds and adapts to the growing need of digitalisation? Does the access to and dependency on ICTs serve as a prerequisite to contribute to the fight against pandemic? As Tim Unwin rightly reminds us, if ICTs have to be used as a tool for development and social change, then it is critical to have a people-centric approach towards technologies [5]. As in the case of several other countries, COVID-19 also exposed Pakistan's prevalent digital standards. As the lockdown sent the country of 212 million population packing, it was the ICTs that, to a large extent, served as the propelling force in holding the society together and assist in functioning of the state. However, Pakistan's ICT standards or its eGovernment performance are largely under-documented. It has been 20 years since the first national IT policy in Pakistan was promulgated in 2000. Since then Pakistan has gone through several technological transformations. The United Nations' eGovernment survey ranking of past 20 years identifies the ICT situation in Pakistan by grouping it among the least connected in the world with a fixed broadband penetration rates below one per cent. Interestingly, Pakistan has a high eParticipation index of 0.5238 and eGovernment Development Index of 0.4183 in 2020. The fact that Pakistan ranks high for its online services index ranking 0.6294 despite a low Telecommunications Infrastructure Index of 0.2437 is notable [6] (Table 1).

How Pakistan managed to rank high in online services index makes it an interesting case for not only academic curiosity but also for its efforts in the aftermath of COVID-19. Hereinafter, this paper focuses on Pakistan's approach in channelising ICTs and eGovernment amidst the Coronavirus outbreak. In doing so, the paper briefly looks at Pakistan's journey towards digital identity that has opened doors for eGovernment

Table 1 Comparison of Pakistan's ICT development indices [6]

Index	2010	2012	2014	2018	2020
eParticipation index	0.171	0.132	0.333	0.5	0.523
eGovernment development index	0.275	0.282	0.258	0.356	0.418
Telecom infrastructure index	0.025	0.123	0.117	0.152	0.243
Mobile subscribers per 100 inhabitants	49.74	59.2	67.06	70.65	72.56

applications. The paper wishes to explore those alternative ICT channels that are assisting in the provision of electronic public services such as via mobile phones and/or digital hubs. Towards the end, this paper wishes to highlight how both the Internet and the alternative communication channels are at play particularly during the pandemic.

2 Contextualising Digitalisation and Digital Identity in Pakistan

At the beginning of new millennium, manual methods of payment and public services dominated in Pakistan. The promulgation of first IT policy in 2000 served as a precursor to the broadening Internet infrastructure, eGovernment adoption by the public sector and to incentivise foreign investors to start mobile network operations. For decades, Pakistan did not maintain digital citizen database [7]. It was only after the formation of National Database Organisation (NDO) in 1990s when recording and handling an electronic citizen database commenced. NDO was later renamed National Database Registration Authority (NADRA) as an attached department under Federal Interior Ministry. That marked the first step towards digitalisation of Pakistani citizens [8]. NADRA embarked on its eGovernment services by first developing Computerised National Identity Cards (CNICs). Unique digital identity enabled NADRA to explore eServices beyond CNIC and also collaborate with other public and private sector organisations. For instance in 2008, the federal government engaged NADRA to provide biometric solutions for the social safety net programme named Benazir Income Support Programme (BISP) to provide cash transfers to 4.7 million households living below the poverty line [9].

Similarly, NADRA also developed biometric verification methods that are used for banks for opening customer account. This level of digitalisation offered NADRA to increase its digital capacity along with a chance to review and understand Pakistan's IT infrastructure and digital literacy. Given the limited number of Internet users in early 2000s, NADRA pitched the idea of a stand-alone ATM-styled kiosk machine in 2005. It was a multilingual machine that used CNIC card as an authenticator to make digital payments such as for utility bills or funds transfer. Though unique in its concept, the kiosk machine did not draw much attention. Nevertheless, it opened the door for an alternative thinking towards approaching online services. For eGovernment solutions to work in a country like Pakistan where oral communication is more dominant than the digital, the online and eGovernment services had to include a human factor. NADRA gradually excused itself from kiosk machines, and in 2006, it moved its focus towards commercialising the software used in kiosks thus paving the way for eSahulat project. It provided eSahulat licences to local retailers that would help people with electronic public services. Parallel to these developments, mobile network operators (MNOs) gradually started their operations in Pakistan [10]. Between 1998 to 2008, Pakistan went on to have from two MNOs to five

national and international telecommunication providers. Between 2000 and 2015, the Internet users remained under 2 million, whereas the mobile phone subscription crossed 110 million [11]. NADRA's eSahulat inspired MNOs to also engage in commercial payments and funds transfer via mobile phones. MNOs collaborated with private banks that functioned as a banking channel whereas 2G enabled mobile phones worked as a front-end device. Eventually, the era of branchless banking in Pakistan arrived in 2008 and to date the MNOs thrive with both their digital services as well as mobile payment mechanisms [12]. Pakistan moved from web-based feature to exploring several options in the alternative channels of electronic public service delivery.

3 Digital Dividends Amidst COVID-19 Outbreak

3.1 Branchless Banking on the Rise

NADRA as a public sector entity in Pakistan continued to consolidate its position in digital services particularly in the digitalisation of civil registry system and by developing other eGovernment solutions relying on the digital identity model. In the private sector, it has been MNOs and banks that have shown dominance in digitalisation of financial services. As the Coronavirus started to play havoc in Pakistan, it was the informal economic sector, the daily wagers, masons or domestic helpers whose bread and butter came at risk due to the lockdowns. Within this scenario, mobile phones positioned themselves as more omnipresent than the Internet, given more than 160 million subscribers [13]. As the financial institutions stood closed, reliance on mobile banking mechanisms increased. The branchless banking methods available on 2G/3G/4G networks served as a saviour. Given the unpresecendented situation, the State Bank of Pakistan waved off the transaction charges on digital payments for all banks and mobile phones. The demand for and reliance on branchless banking significantly grew during the lockdown period as the number of transactions saw a considerably increase of 12% (see Fig. 1). The value of transactions for branchless banking in the last quarter of 2019 was 1,197,115, whereas this amount increased up

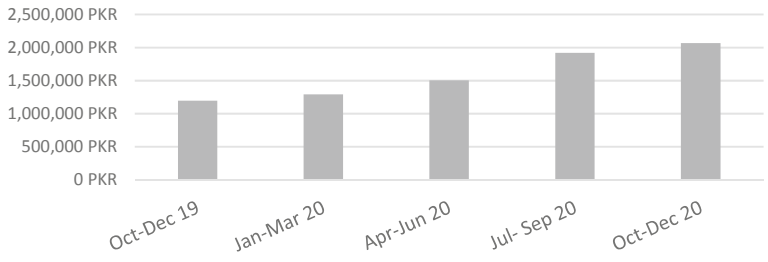


Fig. 1 Rise in branchless banking transactions [14]

to 2,069,307 in the last quarter of 2020. The increase in quarterly transaction over the span of one year increased by 73% [14].

3.2 Digitalisation of Poverty Data for Cash Disbursement

Branchless banking served as a temporary relief, it was, however, the fate of those living below the poverty line that went into a major disarray due to the lockdowns. The livelihood of over 60 million was at stake who earned money on day to day basis [15]. This is when the federal government decided to undertake immediate cash disbursements by reengaging NADRA who had previously worked on the Benazir Income Support Programme (BISP). A National Coordination Committee (NCC) was formed to make BISP COVID-19 responsive to deliver one-time emergency cash assistance to 16.9 million families at risk of extreme poverty [16]. The existing beneficiaries were paid PKR 12,000 (~USD 75) in one instalment which would provide them four months' benefits [9]. The NCC engaged with NADRA to develop a system through which BISP database and poverty score card could provide the government a clear result of potential beneficiaries. NADRA introduced the concept of wealth proxies to ensure transparency by cross verifying the poverty status of every potential beneficiary. The wealth proxies include the asset ownership, travelling history, income tax returns or government employment status to determine their eligibility. The BISP database corresponds to the poverty score card that has various indicators with respect to gauging financial health of the family. The cut-off score to be eligible for the unconditional grant is 16.17/100. For COVID-19, however, the cut-off score was relaxed to 36 which could mean an addition of seven million beneficiaries to the BISP database [9]. The final list of beneficiaries goes through further filters and criteria defined by the State Bank of Pakistan. As a result of these verifications, a database of potential beneficiaries for whom payment mechanism was set up through branchless banking platforms of two commercial banks and over 1500 biometrically adjusted ATMs [17]. The government launched a dedicated SMS service through which people could apply for cash by sending their identity card number to an SMS code 8171 [18]. To make it more inclusive, anyone trying to help could send multiple messages in order to cater to the population without a cellphone. The result of this service reached an overwhelming figure. Within a month after lockdown, the government received approx. 22 million SMS on its allocated number, whereas about one million were either invalid or ineligible. Similarly, out of these valid 21 million citizens, there were about 16 million new citizens who also came within the formula devised for the poverty scorecard [19].

3.3 The Health Story—Telehealth via Digital Hubs and Apps

Two months prior to the first case of COVID-19 reported in Pakistan on February 26, 2019, the Government of Pakistan initiated a "Digital Pakistan" programme in December 2019 with a motivation to bring together various stakeholders for a "digitally progressive and inclusive Pakistan" [20]. Priorities of the programme had to shift in wake of this pandemic and Digital Pakistan initiative extended its collaboration for various public sectors such as health and education. During the lockdown, several hospitals reorganised their medical protocols and focused on allocating isolation and quarantine rooms. This also meant that the outpatients departments had to be closed down and daily visiting patients had to be restricted. The situation takes a worrying turn as around 50% of total population in Pakistan does not get direct access to a doctor in their community [21]. Digital Pakistan initiative started looking for ICT solutions that could assist the health sector. Digital Pakistan partnered with a telehealth initiative "Sehat Kahani" (lit. Health Story) [22]. Launched in 2017 by two female doctors, Sara Khurram and Iffat Zafar, Sehat Kahani partnered with a MNO and follows a two-modular approach comprising electronic hubs and telemedicine mobile application. eHubs are run by Sehat Kahani staff who connect patients to a licenced female doctor on a video link via laptop or tablet using mobile 4G network. The patients pay the online consultation fee via network provider's branchless banking mechanism. The second alternative is for the clientele with a smart phone who can download the Sehat Kahani mobile app that can also record their medical history. The patients have an option to select the doctor according to their own preference and book an appointment with them or they can also request immediate consultation as well. The user can then through audio or video call get consultation and can have the summary of the meeting/prescription sent to them via email. The payments system is either via online bank transfer or mobile money as in eHubs. Till January 2020, the twenty-six eHubs of Sehat Kahani had successfully surpassed over 120,000 online consultations [23]. However, since the pandemic's initial period, the online consultations suddenly increased and more than 32,000 online consultations were managed through this application after the lockdowns. The doctors are joining this platform on daily basis, and to make Sehat Kahani more inclusive, a telephone helpline has also been established for people who don't own a smart phone [24].

3.4 Going Old School—Television to Save the Next Generation

Between March and September 2020, almost 50 million students had to stay at home as schools and colleges remained closed [25]. Few private schools whose clientele could afford the digital gadgetry moved to e-learning but the majority of schools and their pupils neither had digital equipment nor preparation. Unclarity about pandemic forced the government to think of out-of-the-box solutions and employ a holistic

strategy to educate its future generations. That is when the government started to consider alternative channels of digital communication for remote learning that could complement the time lost due to school closures. The government realised that more than 70% of the households in Pakistan have access to television [25]. The Federal Ministry of Education and Professional Training (FMEPT) collaborated with Pakistan Television (PTV) to start a 10-h TV programme through an initiative called "Teleschool" which on a daily basis covers curriculum for grade one to 12 [26]. On emergency grounds, the FMEPT partnered with local educational institutions which provided their educational content for free.

On its part, the government tried to ensure the inclusivity of Teleschools by providing the educational content through PTV's satellite, cable and terrestrial networks [26]. Since television is only one-way information, the FMEPT also collaborated with MNOs to launch a dedicated SMS service via number 8228 through which parents and pupils alike could receive updates and class schedules [27]. In addition, Teleschool also planned to use the two-way SMS service to send to students the multiple-choice questions that could help in monitoring the learning curve and assessment of student engagement. Through television's existing network, Teleschool could reach millions of remote area students who, for the lack of Internet facilities or infrastructure, felt constrained due to this pandemic [28]. The Gallup conducted short-term assessment and found out that nearly 1 in 3 Pakistanis accessed the Teleschool with more than 70% population satisfied with its educational content. Digital Pakistan initiative also collaborated with the FMEPT to assist in developing web-based e-learning modules for the clientele that has the digital capacity and equipment to access.

4 Conclusion

The Coronavirus outbreak has continued to jolt the healthcare system of the world. The damage to the financial and employment market due to the COVID-19 has been unprecedented. The situation for the low-income countries like Pakistan has been even worse, as this paper tried to show. The ICTs have, to a large extent, served as the gluing force in at least enabling people to communicate and collaborate digitally. Nevertheless, the COVID-19 has also exposed several shortcomings in the ICT infrastructures and outreach. The examples from Pakistan can be taken as a blueprint that has an evolving ICT infrastructure and where web-based eGovernment services do not have a wider outreach. Branchless banking as well as initiatives in education and health sector provide a very timely reminder that for low-income and under-digitalised countries, multichannel electronic public services work assumes a leading role in eGovernment conception. Cash transfer, digital health and Teleschool initiatives have of course not been without challenges. These ranged from weak digital infrastructure and exclusion, logistical as well as capacity constraints. For eGovernment solutions to work, it is important to understand the prevalent communication patterns in the society and people-centric approach for modern ICTs to function. For

growth of ICT solutions, the Teleschool initiative highlights an important aspect that electronic public services do not necessarily need to be an agency specific initiative. These services instead flourish in their content, outreach and capacity with more collaborative and multi-agency and stakeholder models. The case of cash disbursement, based on poverty scorecard, signifies the role and importance of data analytics in the public sector that enabled NADRA to help government distribute cash grants among the population living below the poverty line. Similarly, the lessons learnt from Teleschool and Sehat Kahani initiatives indicate the significance of monitoring the performance of digital content and beneficiaries associated with it. For ICT initiatives to succeed, identification of benchmarks and evaluation is indispensable for their sustainability.

References

1. UNCTAD, Coronavirus reveals need to bridge the digital divide, https://unctad.org/news/coronavirus-reveals-need-bridge-digital-divide, last accessed 2020/10/28
2. ILO, The Islamic Republic of Pakistan Decent Work Country Profile, https://www.ilo.org/wcmsp5/groups/public/---ed_mas/---program/documents/ genericdocument/wcms_562091.pdf. Last accessed 2020/10/28
3. UNOCHA, Humanitarian Response Plan for Covid-19 Pandemic 2020, https://www.unocha.org/covid19. Last accessed 2020/10/28
4. M. Coeckelbergh, The Postdigital in Pandemic Times: a Comment on the Covid-19 Crisis and its Political Epistemologies. Postdigital Sci. Educ. **2**, 547–550 (2020)
5. T. Unwin, A critical reflection on ICTs and 'development,' in *Reclaiming Information and Communication Technologies for Development*, 1st ed., Oxford University Press, New York (2017)
6. United Nations, UN eGovernment Surveys, https://publicadministration.un.org/en/Research/UN-e-Government-Surveys. Last accessed 2020/10/28
7. H. Bokhari: Information and Communication Technologies in Pakistan. History and Analysis of Electronic Public Services (2000–2012). dissertaVerlag, Hamburg (2020)
8. T. Malik, Technology in the service of development: The NADRA story, http://www.cgdev.org/publication/technology-service-development-nadra-story. Last accessed 2020/10/28
9. K. Seyfert, M. Ahmad, Options for making Pakistan's flagship national cash transfer programmeshock-responsive, https://maintainsprogramme.org/wp-content/uploads/GK- Making-BISP-shock-responsive-18062020.pdf. Last accessed 2020/10/28
10. H. Bokhari: Multi-channel electronic public service delivery mechanisms in developing countries - A case study of the eSahulat programme in Pakistan. In Proceedings of the 4th International Conference on Theory and Practice of Electronic Governance, pp. 243–248, ACM, New York (2010)
11. PTA, Annual Report 2015, https://www.pta.gov.pk/annual-reports/ptaannrep2014-15.pdf. Last accessed 2020/10/28
12. M.A. Mulki, S.A. Rizvi, Branchless banking: Branching out, https://www.dawn.com/news/1113550. Last accessed 2020/10/28
13. The Express Tribune, Pakistan's internet use increases by 15% amid coronavirus lockdown, https://tribune.com.pk/story/2190753/pakistans-internet-use-increases-15-amid-coronavirus-lockdown. Last accessed 2020/10/28
14. State Bank of Pakistan, Branchless Banking Key Statistics, https://www.sbp.org.pk/publications/acd/branchless.htm. Last accessed 2020/10/28

15. A. Hashim, Pakistan daily wagers struggle to survive in coronavirus lockdown, https://www.aljazeera.com/news/2020/3/25/pakistan-daily-wagers-struggle-to-survive-in-coronavirus-lockdown. Last accessed 2020/10/28
16. S. Nishtar, Ehsaas Emergency Cash: A digital solution to protect the vulnerable in Pakistan during the COVID-19 crisis. https://www.pass.gov.pk/Document/Downloads/ EhsaasEmergencyCashReportJuly212020.pdf. Last accessed 2020/10/28
17. F. Yousafzai, First installment of Ehsaas Emergency Fund released to poor, https://nation.com.pk/10-Apr-2020/first-installment-of-ehsaas-emergency-fund-released-to-poor. Last accessed 2020/10/28
18. M. Haider, Sending SMS to Ehsas Programme Code 8171 made free. https://www.thenews.com.pk/print/642189-sending-sms-to-ehsas-programme-code-8171-made-free. Last accessed 2020/10/28
19. Government of Pakistan, Ehsaas Emergency Cash: social protection response to Coronavirus. https://www.pass.gov.pk/Document/Downloads/Slides Explaining Ehsaas Emergency Cash.pdf. Last accessed 2020/10/28
20. The Express Tribune, PM Imran launches 'Digital Pakistan' initiative, https://tribune.com.pk/story/2112360/1-digital-pakistan-pm-imran-addresses-launch-ceremony. Last accessed 2020/10/28
21. Sehat Kahani, More than 50% of individuals in Pakistan don't have access to basic primary healthcare services!, https://sehatkahani.com/2019/05/03/sehatkahani-application-launch/, last accessed 2020/10/28.
22. The Nation, Female doctors of Sehat Kahani fight coronavirus using telemedicine!" https://nation.com.pk/31-Mar-2020/female-doctors-of-sehat-kahani-fight-coronavirus-using-telemedicine. Last accessed 2020/10/28
23. GSMA, Sehat Kahani Employing mobile technology to connect women doctors to underserved communities in Pakistan. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/05/Sehat-Kahani-Employing-mobile-technology-to-connect-women-doctors-to-underserved-communities-in-Pakistan.pdf. Last accessed 2020/10/28
24. T. Palmer, S. Ajadi, S. Hinrichsen, Using technology to fight COVID-19: A spotlight on telemedicine start-up Sehat Kahani in Pakistan. https://www.gsma.com/mobilefordevelopment/blog/using-technology-to-fight-covid-19-a-spotlight-on-telemedicine-start-up-sehat-kahani-in-pakistan. Last accessed 2020/10/28.
25. I. Baloch and A. Taddese, EdTech in Pakistan : A Rapid Scan, https://docs.edtechhub.org/lib/FIQDEKCI. Last accessed 2020/10/28
26. K. Abbasi, Teleschool goes on air today to compensate for academic loss, https://www.dawn.com/news/1548995. Last accessed 2020/10/28
27. The News, Ministry to launch SMS system for teleschool, https://www.thenews.com.pk/print/660616-ministry-to-launch-sms-system-for-teleschool. Last accessed 2020/10/28.
28. N. Naviwala, How 'Teleschool' Can Revolutionize Pakistan's Education System, United States Institute of Peace, https://www.usip.org/blog/2020/04/how-teleschool-can-revolutionize-pakistans-education-system. Last accessed 2020/10/28

VLSI Design Flow Using Vinyas Design Bot



Veena S. Chakravarthi, S. Sowndarya, and Shubham Raj

Abstract Very Large-Scale Integration (VLSI) is the process of creating integrated circuit (IC) by combining millions of transistors into a single chip. This technology is used in most applications in all domains. In this paper, we describe the patent pending work of development of intelligent machine to do VLSI design modeling from the requirements. The Vinyas Design Bot is an intelligent bot which automates the process of capturing design requirements in the form of chats, discussion notes and conversation and generates Verilog design database from it. The work involves extracting specification from the requirements by Natural Language Processing (NLP), deriving logic from specifications by convolutional neural networks (CNN) and performing optimization by artificial intelligence (AI) to generate the project database with Verilog HDL models and electronic design automation (EDA) run scripts. The functionality of Vinyas Design Bot is demonstrated by two case studies – ALU design and I2C design.

Keywords NLP · I2C protocol · ALU Design · Vinyas design bot · Verilog design · RTL design · Test bench · Simulation

1 Introduction

VLSI design process is becoming more and more complex with integration of multiple cores onto system on chip. VLSI design is always required to be first-time success due to increased cost of design and fabrication. It is necessary to automate the process to avoid most obvious manual errors and interpretation errors in particular. For VLSI circuits, from specification, the process of Verilog design and physical design to generate GDS files for fabrication is quite a matured and standard flow [1]. Design methodologies use electronic design automation (EDA) tools with most of the processes automated. Digital system design flow is shown in Fig. 1.

V. S. Chakravarthi (✉) · S. Sowndarya · S. Raj
BNM Institute Technology, Bangalore, India
e-mail: veenasc@bnmit.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_36

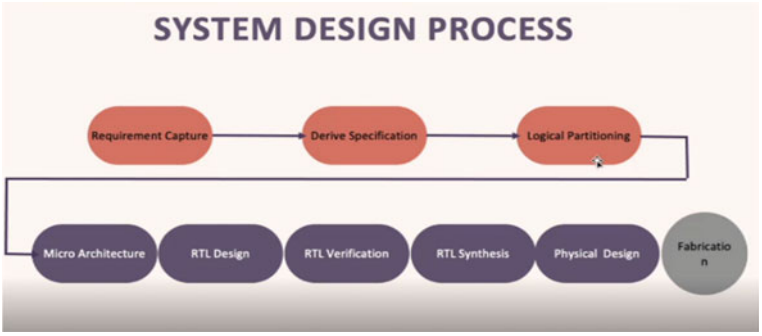


Fig. 1 Design process

Generating the design specification is mostly manual with requirements available in different forms like document, mails, oral discussions and meeting minutes. Generally, there are two important things to design a functional block and the first one is to get the requirements to be translated to specification right and the second is to verify the model for the correct behavior. The procedure in VLSI design flow starts by knowing the objective and specifying the requirements [2]. Then, different types of logic required to achieve the final outcome are separated. Then, the following steps are performed:

(1) Micro architecture: The architecture is designed by using elements having the range in micrometer.
(2) RTL [Register Transfer Level] design: RTL design abstraction models a synchronous digital circuit in terms of the flow of digital signals between hardware registers and the logical operations performed on those signals.
(3) RTL verification: RTL verification step ensures that the design is logically correct and without major timing errors.
(4) RTL synthesis: This process involves the implementation of the design in the form of logic gates by using a synthesis tool.
(5) Physical design: Physical design translates the logical description of data into the technical specifications for storing and retrieving data so as to provide adequate performance and ensure database integrity, security and recoverability.
(6) Fabrication: It is the final process of placing the design onto a wafer (silicon). These wafers undergo processes such as cutting, sizing, polishing, deposition, etching and cleaning.

The aim of the Vinyas Design Bot is to generate the VLSI design database in Verilog code from the requirements given as text document. Even without knowing the syntax of the language, anyone will be able to implement their logic in the form of code using Vinyas Design Bot.

- Build auto HDL designer using python or based platform
- Build auto-generating HDL design database using Design Bot.

- Verify the HDL design database by simulating it using standard simulator on EDA platform.
- Validate the design database by porting onto FPGA.

2 Vinyas Design Bot

Vinyas Design Bot consolidates the requirements and generates specification automatically and writes out the Verilog design files. This section explains the algorithms and flow of Vinyas Design Bot. The Vinyas Design Bot converts the design requirement in chat conversation via **dialog parser** which is text or speech to text converter. It uses **Natural Language Processing** (NLP) method to do this conversion. There are many ways of interpretation of requirements. For example, design and test teams have different ways of representing the requirements, most of them in terms of normal conversation/textual ways. However, explaining requirements for a design can create ambiguity. Thus, by automating initial part of design specifications, the hurdles of mis-interpretation of the design are reduced.

The complete process involved in VLSI designing using Design Bot is depicted in Fig. 2. The Design Bot not only helps industrial experts but also helps in the education field. In the industrial field, it helps in avoiding ambiguity during code designing process as explained in the previous section, whereas in the educational field, it acts as a guide to the students to improve their skills. It enables self-learning among students. The logic that the student wishes to implement should be framed as an English sentence. This will act as input to the bot. Further whatever the student wishes to add to the code can be communicated to the bot and it will convert those English sentences into code.

Input processing: Vinyas collects number of team members involved in the conversation and decides the team identity for each of the team member. The team members conversation is recorded, and the resulting audio file is parsed to process the conversations. Conversation is further converted into sentences. The

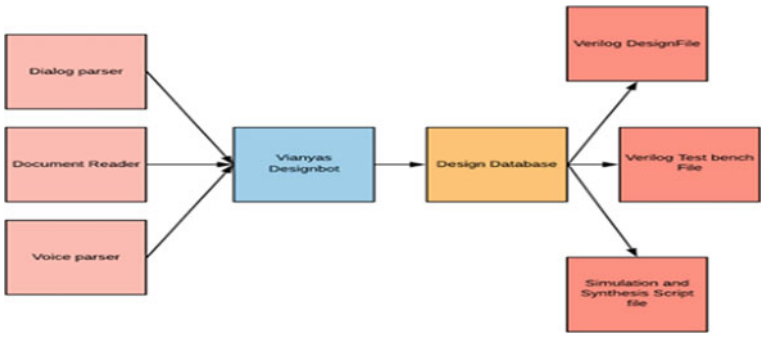


Fig. 2 Vinyas design bot block diagram

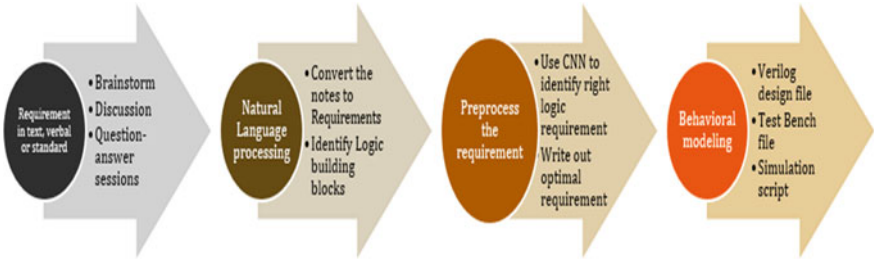


Fig. 3 Functional block of vinyas design bot

audio file is converted to text format and is now ready for parsing. The sentences are interpreted depending on the context of the conversation. Vinyas has intelligence to "understand" the sentences, including the contextual nuances of the language within them. The technology can then accurately extract information and insights contained in the complete documents and parse them meaningfully.
Logic extraction: Once the input processing is completed, different lists containing specific words for different logic are collected from the partially processed list of sentences and count of the number of times, they are repeated in the conversation is noted. This is used to extract the logic from the sentences [3].
Logic Optimization and Verilog feature extraction: Logic optimization uses machine learning algorithm which works on previously learnt logics which will be reused. It writes out Verilog design files. Output design files written out are Design and test bench models in Verilog HDL, Simulation and Synthesis EDA tool run scripts. Functional blocks of Vinyas Design Bot are shown in Fig. 3. To perform Verilog feature extraction, Textblob and NLTK libraries are imported. The chatbot starts the conversation by asking the number of speakers present. The speakers are given as input using a for loop. Then, the conversations are entered using a for loop. Finally, all conversations are printed. All the conversations are converted to a paragraph containing strings. All the full stops in the paragraph are replaced with blank spaces to avoid detection of full stop in parts of speech. Then, all the words are converted to lower case to avoid ambiguity. Converting the given string into the lower case also helps in the identification of keywords properly.

2.1 Requirement Processor

- **Extraction of parts of speech:** The TextBlob function is used to the paragraph. Then the different parts of speech are obtained using the blob.tags function [4].
- **Defining the list of keywords for logic identification:** Separate lists are created for each logic so that particular keywords are determined for logic identification.

The steps involved in the methodology are depicted in the block diagram in Fig. 3.

2.2 Requirements in Text, Verbal or Standard

- **Creation of verb list:** An empty list for verbs is created. The list of tuples in sentences is iterated to identify different types of verbs. As and when the verbs are detected, the list is appended. Then, the repeated elements in the list are removed.
- **Mapping verbs to output:** A list of strings y is created containing from y1 to y10. Based on the number of operators, the corresponding list of strings from y is extracted. These can be used as output variables.
- **Creating symbol list:** Initially, an empty list for symbols is created. Based on the decided operation, the symbol list is appended with the corresponding symbol and printed.
- **Using counters and deciding the circuit:** Initially, the counters for all circuits are initialized to 0. Then, the entire list of sentences is iterated and compared with the words in the predefined list. If there is a match, then the counter is incremented for each case and the corresponding circuits and variables are assigned.

2.3 Logic Extraction and Optimization

CNN—convolutional neural network is used for the optimization of the code [5]. A logic can be implemented in different ways. Thus, with the help of Convolution neural network optimized VLSI design database can be generated.

2.4 Behavioral Modeling

This process involves generation of Verilog code and testbench from earlier obtained logic.

- **Creation of directories:** OS, shutil and other python libraries are used to create directories in the required folders [6]. The paths are specified and the names of the directories are mentioned accordingly.
- **Creation of the testbench file inside the TB folder:** The name of the module used for this purpose is the Verilog module name appended with "_tb". The inputs are declared with the keyword "reg" and the outputs are declared with the keyword "wire". The unit under test (UUT) is instantiated and stimulus is given by applying random inputs. Then, the waveform file is given for debugging using $dumpfile and $dumpvars function. The module stops executing after a certain delay.
- A main folder called Verilog folder is created. Inside this folder, three subdivisions are created: The **Source code folder** contains the Verilog code file, the **Testbench folder** contains the Verilog test bench file and the script file. **Readme file** is the file with all details of the VLSI design database (Fig. 4).

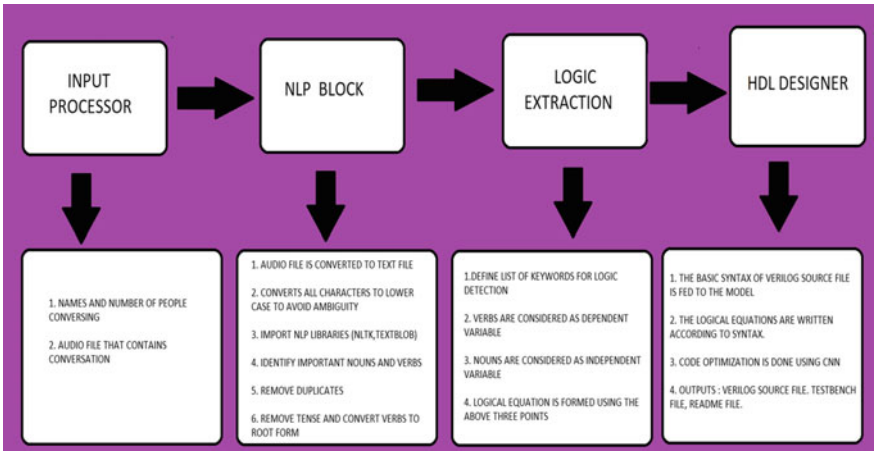


Fig. 4 Workflow of ALU design using vinyas design bot

3 Design Cases

3.1 Design Case: ALU Design Using Vinyas Design Bot

Requirements for ALU: To design an ALU, we need to identify the logical operations to be performed. This is extracted from the conversation. The variables are chosen accordingly and can be any valid identifiers. Also, an operator is a variable. Sample inputs are shown in Fig. 5.

Specification: The number of people involved in the conversation must be specified based on which the input variables are chosen. The mode of operation (chat or audio) and the path where the output files are written out be specified.

Logic derivation: The counts of certain words necessary for a particular operation determines the different types of logic present. Based on the number of operations, the corresponding output variables are chosen. Finally, branching and iteration statements are used accordingly to print the output in proper Verilog code format.

Output files: Based on the logic identified each output variable is assigned with the specific operator between the input variables. Basically, 3 output files are obtained. The first file is the Verilog file which contains the input and output variables, and it maps the output to corresponding operations of the input as shown in Fig. 6. The next file is the testbench file. This file gives stimulus to the input and checks the output. The inputs are given randomly within the specific range as shown in Fig. 8. The other output file shown in Fig. 7 is the readme file which gives the description of the files present.

```
HI! I AM HERE TO HELP YOU WITH YOUR DESIGN. TELL ME YOUR IDEA AND I WILL CONVERT IT INTO AN IMPLEMENTABLE CODE!
LET ME KNOW HOW MANY OF YOU ARE INVOLVED IN BRINGIN UP THIS CONCEPT?2
THAT'S GREAT. I WOULD LOVE TO KNOW ABOUT YOU ALL.
TELL ME YOUR NAME PLEASE A
TELL ME YOUR NAME PLEASE B
['A', 'B']
PLEASE EXPLAIN YOUR IDEA: I am planning to go for a trip.
TAGGING YOUR NAME ALONG WITH YOUR IDEA WILL BE OF GREAT HELP TO ME.  : A
PLEASE EXPLAIN YOUR IDEA: That is a nice idea
TAGGING YOUR NAME ALONG WITH YOUR IDEA WILL BE OF GREAT HELP TO ME.  : B
PLEASE EXPLAIN YOUR IDEA: We will plan the place together and go there if it is acceptable by both of us.
TAGGING YOUR NAME ALONG WITH YOUR IDEA WILL BE OF GREAT HELP TO ME.  : A
PLEASE EXPLAIN YOUR IDEA: Fine. We need to book the bus tickets.
TAGGING YOUR NAME ALONG WITH YOUR IDEA WILL BE OF GREAT HELP TO ME.  : B
PLEASE EXPLAIN YOUR IDEA: Either anyone of us have to purchase both the tickets or we have to purchase our tickets individuall
y.
TAGGING YOUR NAME ALONG WITH YOUR IDEA WILL BE OF GREAT HELP TO ME.  : A
PLEASE EXPLAIN YOUR IDEA: In case if you are not interested in this trip, then even I will not come and we shall cancel it.
TAGGING YOUR NAME ALONG WITH YOUR IDEA WILL BE OF GREAT HELP TO ME.  : B
PLEASE EXPLAIN YOUR IDEA: We should possess id cards with unique id numbers.
TAGGING YOUR NAME ALONG WITH YOUR IDEA WILL BE OF GREAT HELP TO ME.  : A
PLEASE EXPLAIN YOUR IDEA: If payment is illegal then to penalize we will be multiplying individual shares.
TAGGING YOUR NAME ALONG WITH YOUR IDEA WILL BE OF GREAT HELP TO ME.  : B
PLEASE EXPLAIN YOUR IDEA: We will spend individual shares of money and sum it up to final expenditure.
TAGGING YOUR NAME ALONG WITH YOUR IDEA WILL BE OF GREAT HELP TO ME.  : A
PLEASE EXPLAIN YOUR IDEA: DONE
TAGGING YOUR NAME ALONG WITH YOUR IDEA WILL BE OF GREAT HELP TO ME.  : B
```

Fig. 5 Sample inputs for ALU

Fig. 6 ALU verilog file

*ALUDesign - Notepad

File Edit Format View Help

```
module ALUDesign (
//inputs, outputs and internal variables declared here
input [ 7 : 0] A,
input [ 7 : 0] B ,
input [ 2 : 0] op,
output [ 7 : 0] y0 ,
output [ 7 : 0] y1 ,
output [ 7 : 0] y2 ,
output [ 7 : 0] y3 ,
output [ 8 : 0] y4 ,
output [ 15 : 0] y5
) ;
wire [ 2 : 0] op ;
reg [ 7 : 0] y0 ;
reg [ 7 : 0] y1 ;
reg [ 7 : 0] y2 ;
reg [ 7 : 0] y3 ;
reg [ 8 : 0] y4 ;
reg [ 15 : 0] y5 ;
  always @ ( op or A or B )
 begin
  case( op)
  3'b000 : y0 = A | B ;
  3'b001 : y1 = A & B ;
  3'b010 : y2 = ~ A ;
  3'b011 : y3 = A ^ B ;
  3'b100 : y4 = A + B ;
  3'b101 : y5 = A * B ;
  endcase
 end
endmodule
```

Fig. 7 Readme file



The simulation runscript file is also present. The VLSI design files are simulated using EDA playground simulator and waveforms can be obtained as shown in Fig. 9.

3.2 Design Case: I2C Design Using Vinyas Design Bot

I2C is a standard protocol for serial transmission of data between integrated circuits [7]. It has two major components. They are the master and the slave (Fig. 10).

Master device—As it goes by the name, the slave device is controlled by the master. The master generates clock which is one of the important signals to initialize and direct data transfer with the slave.

Slave device—The slave accepts and responds to the signals from the master. The slave has the ability to send data to the master and to receive data from the master.

I2C protocol includes two lines for data transmission between the devices. They are SDL (Serial Data Line) and SCL (Serial Clock Line). SCL is concerned with the clock signal and SDA directs the data signal. Serial clock line is responsible for carrying clock signal, whereas serial data lines are used for transferring data from master to slave and vice versa. Together they are used to generate various conditions like start stop, etc. Apart from sending data SDA line is also used for sending address, read/write bit and ACK/NACK bits. In I2C protocol, messages are sent in the frames of data as shown in Fig. 11. The message is a set of data as frames that include start and stop conditions, read/write bit, ACK (Acknowledge)/NACK (Negative Acknowledge) bits and the data to be transmitted.

Initially, the circuit is said to be in idle state when there is no data to be transmitted. The beginning of a data transfer is characterized by a "START" condition. The START condition is defined as a high to low transition on the SDA line while SCL is high. With the advancement in I2C technology, one can connect multiple slaves to a single master. One can also have multiple masters controlling single or multiple slaves [8]. In these cases where there are multiple masters/slaves, there will be ambiguity with respect to identification of receiver device. In order to avoid this, the master sends the slave 7 or 10 bits address frame. Each slave compares the address sent from

*ALUDesign_tb - Notepad

File Edit Format View Help

```
module ALUDesign_tb;
//inputs
    reg [ 2 : 0] op ;
    reg [ 7 : 0] A;
    reg [ 7 : 0] B;
//outputs
    wire [ 7 : 0] y0;
    wire [ 7 : 0] y1;
    wire [ 7 : 0] y2;
    wire [ 7 : 0] y3;
    wire [ 8 : 0] y4;
    wire [ 15 : 0] y5;
   //applying stimulus
initial
   begin
   // applying inputs
     A = 8'h93 ;
     B = 8'h92 ;
   op = 3'b000 ;
    #100 ;
    A= 8'hFF ;
    B= 8'hFF ;
   op = 3'b001 ;
    #100 ;
    A = 8'h00 ;
   op = 3'b010 ;
    #100 ;
    A = 8'h3 ;
    B = 8'h5 ;
   op = 3'b011 ;
    #100 ;
   op = 3'b100 ;
    #100 ;
    A = 8'h2 ;
    B = 8'h3 ;
   op = 3'b101 ;
    #100 ;
   end
//Instantiate the Unit Under Test (UUT)
ALUDesign u_ALUDesign
(
    .op(op),
    .A(A),
    .B(B),
    .y0(y0),
    .y1(y1),
    .y2(y2),
    .y3(y3),
    .y4(y4),
    .y5(y5)
);
//waveform file for debug
initial
   begin
    $dumpfile("ALUDesign_tb.vcd");
    $dumpvars(2,ALUDesign_tb);
#600 $finish;
   end
endmodule
```

Fig. 8 ALU testbench file

master to its own address and if the address matches, the further procedures for data transfer take place.

There are 2 types of data transfer operations that can take place. They are the "READ" operation and the "WRITE" operation. During write operation, data is written onto slave i.e., data is sent from the master to the slave. During read operation, data is read by the master from the slave i.e., data is sent from the slave to the master. The "read/write" bit is a single-bit data frame which is included in message signal.

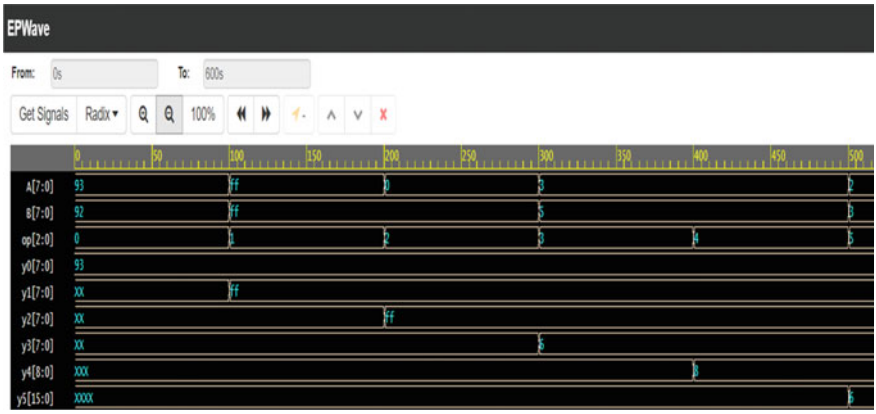


Fig. 9 ALU simulation waveform

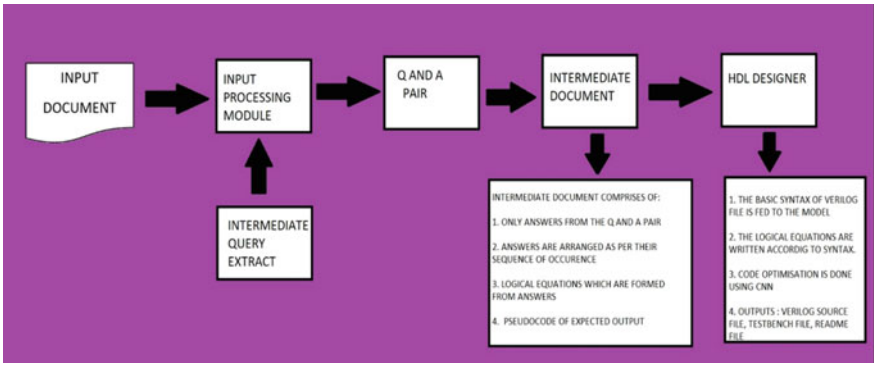


Fig. 10 Workflow of I2C design using vinyas design bot



Fig. 11 Message as a sequence of data frames

If it is a read operation, the read/write bit is pulled high. If it is a write operation, the read/write bit is made low.

Along with data, an ACK (Acknowledge) bit which is a single-bit data frame is sent from sender to receiver. Through this ACK bit the sender communicates with receiver to check if data is received successfully. The receiver puts the ACK signal high if data transfer is successful. If the data transfer is a failure, then the ACK bit is pulled low indicating NACK (Negative Acknowledgement). If ACK bit is pulled low then this data transfer process is repeated.

The end of a data transfer is characterized by a "STOP" condition The STOP condition is defined as a low to high transition on SDA line while SCL is high. The stop condition is generated by the master.

3.2.1 Requirements in Text, Verbal or Standard Document

This is the input processing stage. The input can be an email, a document, a conversation between people or any form of notes which contains information. This stage aims at splitting or simplifying the input document. By doing so it will be easier for the model to analyze each sentence and bring a logic out of it.

Importing of libraries: To perform Verilog feature extraction, Textblob and Natural Language Toolkit (NLTK) libraries are imported.

Document input: There are 2 major inputs. One is the document that contains complete information about I2C protocol. The second one is the set of questions which needs to be asked in general to explain any protocol.

Q and A pair creation: The input processing module compares the input document with the question set. It tries to find a matching answer to every question in the question set. If the model cannot find answer to a particular question, then the question is prompted to the user and the user needs to answer them manually.

As an output, it produces question with matching answer as a pair.

SAMPLE QUESTION SET: Identify the number of inputs, outputs, intermediate signals. Name those signals. For each identified signal the following questions are asked: When is the signal high? When is the signal low? When is the signal idle?

A group of interlinked sentences is identified as an event. Each event is subjected to the following questions. When is an event successful? When is an event said to be unsuccessful?

What is the expected event if previous one is successful?

3.2.2 Requirement Processor

Creation of intermediate document: The question-and-answer pair that is created in the input processing stage acts as a base for this intermediate document.

A statement is formed using each question-and-answer pair. The statements are arranged in the order of their occurrence. Using NLP libraries such as textblob and NLTK, parts of speech tagging are done to the statements. In general, in any sentence, the verbs indicate the action which the noun performs. By this we can say that the nouns are considered as independent variables and verbs are considered as dependent variables. The Vinyas Design Bot tries to map necessary nouns as input variables and hence they are considered as independent variables. In the similar way, the bot tries to map dominant verbs as output variables that are dependent on input nouns and hence verbs are called as dependent variables. The relation between nouns and

verbs is derived by comparing the words in the statement with a predefined list of keywords. The predefined list of keywords contains the root words that are used by the bot for identifying the appropriate and optimized logic from the given input.

As a next step, the logical equation is formed from every statement. Based on the tense of the sentence, the model attempts to decide if the statement can be only data which is constant at all times or if the data changes as per change of other parameters that are related to the protocol. Hence, based on the syntax and the data category, the model decides the placement of every logical equation. Hence, a pseudocode for the final output code is created. The Vinyas Design Bot optimizes the code using CNN and generates the Verilog file, Verilog testbench file and readme file through behavioral modeling.

4 Conclusion

Vinyas Design Bot functionality is explained using I2C design requirements and ALU Design and VLSI design files are generated. Vinyas Design Bot can be helpful for students, industry experts and other enthusiast learners. The usage of coding and design modeling is extensive both in the industrial and educational field. So, this will make the process of design modeling and coding much easier for industry experts and students. However, the bot should be fed with proper inputs like good quality audio file if audio is to be used as input. Spelling mistakes in the input conversations and corrupted audio files can lead to a different logic. So, the noisy audio and misspelled conversations should be taken into account while giving input.

The further enhancement on Design Bot includes testing complex design requirements, adding machine learning features like feeding design data set for training and identifying number of test cases for exhaustive simulations. This work has been filed for patent vide number: **TEMP/E-1/63385/2020-CHE**.

Acknowledgements Authors acknowledge ECE Department and BNM Institute of Technology, Bangalore for supporting this work.

References

1. M.M. Mano, M.D. Ciletti, Digital Design: with an introduction to verilog HDL 5e, Pearson, 2013
2. R. Sobot,Practical considerations in VLSI IC design flow with respect to tool limitations, in *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1558–1561 (2015).https://doi.org/10.1109/ISCAS.2015.7168944
3. G. Ramesh, J. Somasekar, K. Madhavi, G. Ramu, Best keyword set recommendations for building service-based systems. Int. J. Sci. Technol. Res. **8**(10), 2019

4. B.D. Bašić, M.P. di Buono,An analysis of early use of deep learning terms in natural language processing, in *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*, pp. 1125–1129 (2020).https://doi.org/10.23919/MIPRO48935.2020.9245375
5. S. Albawi, T.A. Mohammed, S. Al-Zawi,Understanding of a convolutional neural network, in *2017 International Conference on Engineering and Technology (ICET)*, pp. 1–6 (2017). https://doi.org/10.1109/ICEngTechnol.2017.8308186
6. Z. Dobesova,Programming language Python for data processing, in *2011 International Conference on Electrical and Control Engineering*, pp. 4866-4869https://doi.org/10.1109/ICECENG.2011.6057428
7. A.S. Warrier, A.S. Belvadi, D.R. Gawhane, T.K Babu Ravi, FPGA implementation of SPI To I2C bridge, Int. J. Eng. Res. Technol. (IJERT). **2**(11), (2013)
8. K.B. Bharath, K.V. Kumaraswamy, R.K. Swamy,Design of arbitrated I2C protocol with DO-254 compliance, in *2016 International Conference on Emerging Technological Trends (ICETT)*, pp. 1–5 (2016).https://doi.org/10.1109/ICETT.2016.787

Detection and Classification of Brain Tumor Using MRI Images



Rahul Koli, Sahil Lotya, Prasad Govekar, Karan Sachdev, and Gresha Bhatia

Abstract The brain tumor is a devastating disease, which shortens the life expectancy quite a bit in their highest grade. We aim to present a multiclass brain tumor classification algorithm using deep networks convolution neural networks with loss function as the binary cross-entropy and optimizer as Adam and ResNet50 on multiple datasets of Magnetic Resonance Images. Deep learning has earned a lot of development in the medical field in the last few years. MRI has been a constructive tool for medical research in current years and has many applications like brain tumor detection. In the detection of tumors, MRI images of the brain were classified as tumorous or non-tumorous using deep network CNN. In the classification, contrast-enhanced MR images are used to classify the images into three types of brain tumor: pituitary, glioma, and meningioma. By making use of this, we can identify and give the required medication to the patients.

Keywords Brain tumor · Deep learning · CNN · Figshare · Transfer learning

1 Introduction

The universal method for the diagnosis of tumor type is the use of MRI images. MRI is an imaging approach used by the medical field which utilizes radiology to capture pictures of the anatomy and physiological processes of the human body. However,

R. Koli (✉) · S. Lotya · P. Govekar · K. Sachdev · G. Bhatia
Computer Engineering, Vivekanand Education Society's Institute of Technology, Mumbai, India
e-mail: 2018.rahul.koli@ves.ac.in

S. Lotya
e-mail: 2018.sahil.lotya@ves.ac.in

P. Govekar
e-mail: 2018.prasad.govkear@ves.ac.in

K. Sachdev
e-mail: 2018.karan.sachdev@ves.ac.in

G. Bhatia
e-mail: gresha.bhatia@ves.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_37

it is based on the hunch of the doctor in-charge, and observation of large amount is not feasible for any human. Detection of brain tumor in early stages is subject to the experience of the neurologist. The first step in diagnosing the brain tumor is to determine if it is cancerous or not, is executed by a biopsy. Especially, for a brain tumor, it is important to have accurate identification of the tumor and to evade surgery and uncertainty [1]. So, the prime objective is to create an efficient model for brain tumor detection and classification using MRI images [2].

Three major kinds of brain tumors are pituitary, glioma, and meningioma tumors. Meningiomas emerge from the layers which protect the cerebrum and surrounding of the nervous system and pituitary tumors are mass of cells which rest inside the cranial part [3–6]. The differentiate trait is that gliomas are malignant in nature and meningiomas are benign but slow growing tumors. Even if pituitary tumors maybe benign, they can cause a lot of damage but meningiomas have sluggish growth tumors [5, 6]. Because of this, we must be completely able to differentiate between these three types of tumors and to give the appropriate medication (Fig. 1).

Brain tumor is one of the deadliest diseases requiring beforehand detection and accuracy. The diagnosis and detection are dependent on neurologists or radiologist for the estimation of MRI image which is plausible to human errors and is time-consuming. This paper presents a convolution neural network model for classification of tumor of the 3 major types: pituitary, glioma, and meningioma tumor from the MRI images.

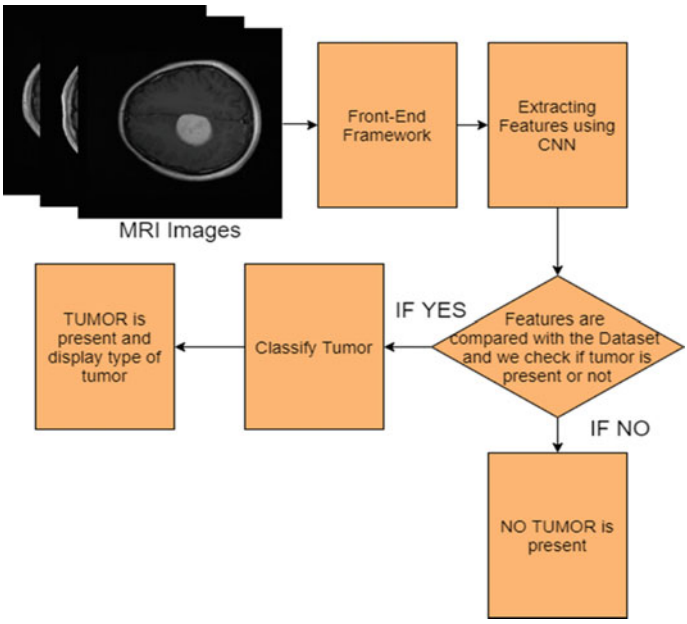


Fig. 1 Block diagram for classification of brain tumor

Table 1 Existing system versus our proposed system

Existing system	Proposed system
Some of the Existing systems which are built using Support Vector Machines are only able to detect and it is very difficult to classify using this type of model	We have used CNN which is good in working with images which is why it is easier in classifying the tumors
Some other Existing systems were built using Artificial Neural Network had low accuracy (~70%)	We have used CNN with ResNet50 as the pretrained model and achieved 96% accuracy
A biopsy is the removal of a small amount of tissue for examination under a microscope and is the only definitive way a tumor can be diagnosed. A pathologist then analyzes the sample(s). So, to eliminate the process of biopsy and have the model detecting the type of brain tumor	Our model helps in eliminating the step of performing a biopsy and determining the type of tumor

2 Lacuna in the Existing System

See Table 1.

3 Related Work

It is very important to detect the tumor in the earliest stages as it reduces the chances of casualty. Several evaluations were supervised by analysts for distinguishing the brain tumor using ML procedures. Here, let's see a succinct survey of some analysts which add to the discovery of cerebrum tumors.

Tianming Zhan et al. have effectively segmented the brain by using complex SVM and SRC classifiers. The inputs given to their model were the normalized NIfTI file which we receive after the MRI scan. To segment, they have used an MRI scan of a normal person's brain and compare it to any person with a tumor. They have implemented the fuzzy C-means clustering algorithm to delineate the tumor and give an accurate description of where the tumor might be present [7].

Shakeel P and Mohamed et al. have presented a categorization framework utilizing ML-based back-propagation neural systems to upgrade the presentation to recognize the brain tumor. The elements are extracted using fractal measurement calculation. The multifractal measurement calculation is used to select the highlighted features. The proposed model has high easy-to-use qualities in slicing the tumor pictures. The result was featuring tumor partition while the remaining part around it is masked [8].

A Jagan has suggested a model for identifying cerebrum tumors in three-dimensional MRI images. In this system, fuzzy C-means clustering algorithm is used to give a better result for classification [9].

A. S. Parihar had used CNN to detect brain tumors using different view angles like Sagittal, Coronal, and Axial from the MRI images. He had trained 3 Link-Net models, one for each view angle. His final accuracy was 0.79 or 79% [10].

Sanjay Saxena et al. have used fuzzy C-means clustering for brain tumor extraction. Basically, it consists of three steps where first step is to identify the brain tumor region by feature extraction then moving toward second step which localizes the tumor region using sliding window method and in the third step, they use C-means clustering to obtain the actual position of the tumor. They use Flair MRI Scans for their experiment [11].

Geetanjali Birare et al. have used k-means clustering and otsu thresholding for segmentation then they have extracted texture features and classified the images by gray level matrix and SVM. They obtained the accuracy of 98.51 for detecting brain tumor cells using SVM [12].

4 Material and Methods

4.1 Datasets

The Kaggle dataset [13] used in detection contains 253 brain MRI images divided into tumor and non-tumor. The tumor folder contains 155 MRI images and the non-tumor folder contains 98 MRI images. For classification, we have used the publicly available figshare dataset [14] which was presented by Cheng et al. [15]. Inside the available dataset, all the MRI images are given in matlab.mat format which consists of Patient ID, Type of tumor, 512 $\times$ 512 MRI image, coordinates for the tumor border, and binary mask image of the affected region. This consists of 3064 MRI images with 3 different brain tumor types: pituitary tumor (930 images), meningioma (708 images), and glioma (1426 images). We used the following libraries of python3: Keras, sklearn, cv2, imutils, NumPy, matplotlib.pylot.

4.2 Data Augmentation

As the amount of data available to us was limited, we augmented the data available, to increase the number of samples we had, to train the model using techniques such as cropping, padding, and horizontal flipping. This helps in increasing the data without actually adding new data to the dataset. We have rotated our dataset at angles like -45, 45, -90, 90, -120, 120, -180, 180, -270, 270, -300, 300, -330, and 330. After performing the data augmentation, we were able to increase the total number of input samples to 24,512. We have augmented the samples in such a way as to balance the dataset. We have used seventy percent data for training, fifteen percent for validation, and fifteen percent for testing.

4.3 Model Used

Firstly, we have used a CNN model to detect if any tumor is present. The CNN model is constructed using deep networks with binary cross-entropy as the loss function and optimizer as Adam (Figs. 2 and 3).

For classification, we have used the ResNet50 pretrained model. This model is imported from the PyTorch library. The architecture of ResNet50 is shown in Fig. 4.

The ResNet50 model takes the input of an MRI image in a tensor format. It then predicts to which type does the MRI Image belongs from the 3 classes (Glioma, Meningioma, Pituitary) that we are predicting. We have saved this model's parameters in a.pt file that stands for PyTorch. These models are then loaded into our Web site using Django.

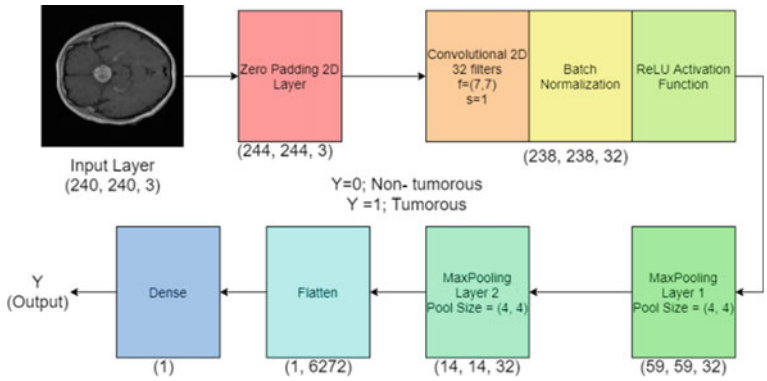


Fig. 2 Architecture of CNN model of tumor detection

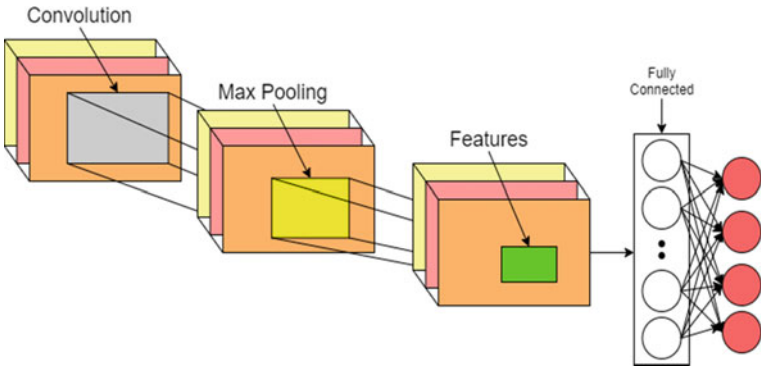


Fig. 3 ResNet architecture

Fig. 4 Performance table for the detection model

	Validation set	Test set
Accuracy	89%	90%
F1 score	0.89	0.90

5 Material and Methods

Our classification algorithm is tested on a PC with Intel Core i5-8590 CPU, 8 GB RAM. The results show how effective is our proposed deep learning-based system, for helping the radiologist/neurologist in taking a precise decision for classifying brain tumors into the three major types (Fig. 5).

Training the CNN model used for detection in the chunk of epochs $10 + 3 + 3 + 3 + 5$ we have generated an accuracy of 89.9 for the test dataset as shown in Fig. 6.

Fig. 5 Loss metrics

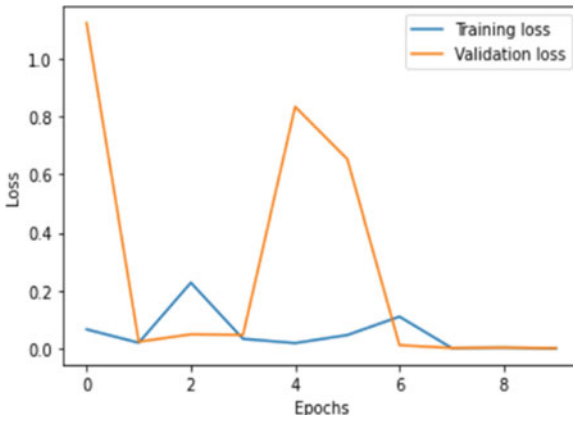
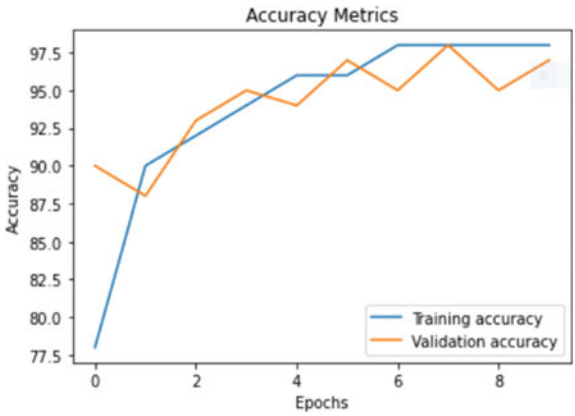


Fig. 6 Accuracy metrics



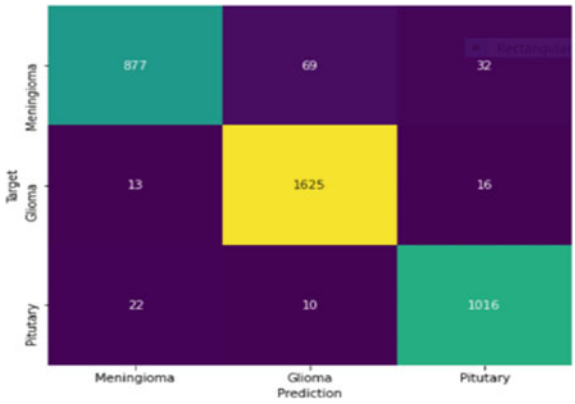


Fig. 7 Confusion matrix for the classification model

Fig. 8 Classification report

Clasification Report

	precision	recall	f1-score	support
0	0.96	0.90	0.93	978
1	0.95	0.98	0.97	1654
2	0.95	0.97	0.96	1048
accuracy			0.96	3680
macro avg	0.96	0.95	0.95	3680
weighted avg	0.96	0.96	0.96	3680

Training the classification model on 10 epochs and dropout = 0.4 as shown in Fig. 7 (Fig. 8).

The above model classifies brain tumors with training accuracy = 98, validation accuracy = 96, test accuracy = 95.60 as shown in Fig. 9.

Testing the model (Fig. 10):

6 Future Scope

Our project is detecting the brain tumor with an accuracy of 89% and our classification model classifies them into Meningioma, Glioma, Pituitary with an accuracy of 96%.

The Project can be further extended by:

- Increasing the accuracy of the detection model.
- For the detection model, the more varied datasets which can include the top as well as the side view should be used to train to increase the accuracy of the model.

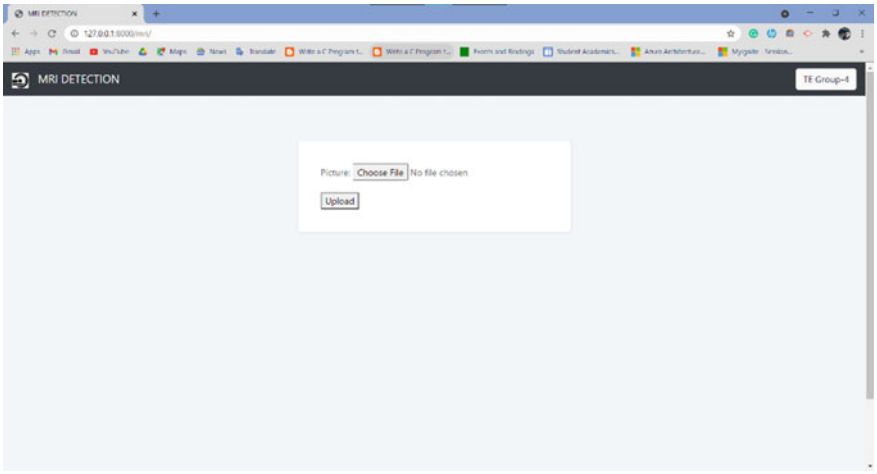


Fig. 9 Frontend of Django web site

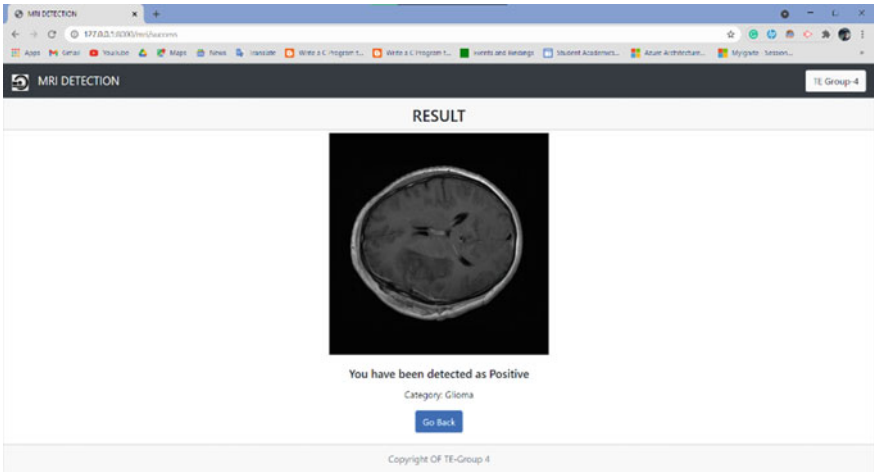


Fig. 10 Implementation using Django

- Also, a classification algorithm needs to be implemented for the classification of different grades of tumor; which would be a great aid for the doctor and patients.
- A deep analysis can be carried out from the database by verifying the trend of brain tumor over years.

7 Conclusion

Two CNN models for brain tumor detection and classification were introduced during this study. The classification was performed using Magnetic Resonance Images database which can classify into the three major tumor types. Our designed CNN is easier than pretrained networks as we can run it on any personal computer because of the algorithm on which the model runs utilizes fewer resources. Image processing plays a key role in the healthcare industry. The brain tumor is detected by using the MRI images and the appropriate treatment is given to the patient. For ResNet50 Model, we were able to classify the brain tumors with training accuracy = 98%, validation accuracy = 96.30%, test accuracy = 95.60 with 10 epochs dropout = 0.4 and for the detection of brain tumor using CNN model has an accuracy of 89.9% on the test set and F1 score of 0.89. These are the two methods using which we have done the classification and then we have deployed these models on a Web site using Django.

References

1. J. Byrne, R. Dwivedi, D. Minks, Tumours of the brain, in *Recommendations Cross-Sectional Imaging Cancer Management*, 2nd edn., ed. by T. Nicholson (Royal College of Radiologists: London, UK, 2014), pp. 1–20. Available online: https://www.rcr.ac.uk/publication/recommendations-cross-sectional-imaging-cancer-management-second-edition. Accessed on 5 November 2019
2. P. Afshar, K.N. Plataniotis, A. Mohammadi, Capsule networks for brain tumorclassification based on MRI images and coarse tumor boundaries, in *Proceedings of the ICASSP 2019–2019 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP),* Brighton, UK, 12–17 May 2019; pp. 1368–1372
3. Cancer Treatments Centers of America—Brain Cancer Types. Available online: https://www.cancercenter.com/cancer-types/brain-cancer/types. Accessed on 30 November 2019
4. American Association of Neurological Surgeons—Classification of Brain Tumours. Available online: https://www.aans.org/en/Media/Classifications-of-Brain-Tumor. Accessed on 30 November 2019
5. L.M. DeAngelis, Brain tumor. New Engl. J. Med. **344**, 114–123 (2001)
6. D.N. Louis, A. Perry, G. Reifenberger, A. Von Deimling, M. Figarella-Branger, W.K. Cavenee, H. Ohgaki, O.D. Wiestler, P. Kleihues, D.W. Ellison, The 2016 World Health Organization classification of tumor of the central nervous system: a summary. Acta Neuropathol. **131**, 803–820 (2016)
7. T. Zhan, Y. Chen, X. Hong, Z. Lu, Y. Chen, Brain tumor segmentation using deep belief networks and pathological knowledge. CNS Neurological Disorders drug targets 16 (2017). https://doi.org/10.2174/1871527316666170113101559
8. S.P. Mohamed, T. Tobely, H. Al-Feel, G. Manogaran, S, Baskar, Neural network based brain tumor detection using wireless infrared imaging sensor. IEEE Access. 1–1 (2019). https://doi.org/10.1109/ACCESS.2018.2883957
9. K. Bhima, A. Jagan, Analysis of MRI based brain tumor identification using segmentation technique, in *2016 International Conference on Communication and Signal Processing (ICCSP)*, Melmaruvathur, India, pp. 2109–2113 (2016). https://doi.org/10.1109/ICCSP.2016.7754551

10. A.S. Parihar, A study on brain tumor segmentation using convolution neural network, in *2017 International Conference on Inventive Computing and Informatics (ICICI)*, Coimbatore, India, pp. 198–201 (2017). https://doi.org/10.1109/ICICI.2017.8365336
11. S. Saxena, et al., Brain tumour segmentation in FLAIR MRI using sliding window texture feature extraction followed by fuzzy C-means clustering. IJHISI **16**(3), 1–20. Web. 25 Apr. 2021.https://doi.org/10.4018/IJHISI.20210701.oa1
12. G. Birare, V.A. Chakkarwar, Automated detection of brain tumor cells using support vector machine, in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (2018), pp. 1–4. https://doi.org/10.1109/ICCCNT.2018.8494133
13. N. Chakrabarty, *Brain MRI Images for Brain Tumor Detection*, Version 1 (2019)
14. https://doi.org/10.6084/m9.figshare.1512426.v1
15. W. Cheng, S. Huang, R. Cao, W. Yang, Z. Yang, Z. Yun, Q. Wang, Feng, Enhanced performance of brain tumor classification via tumor region augmentation and partition. PLoS ONE **10**(10), e0140381 (2015). https://doi.org/10.1371/journal.pone.0140381

Online Food Delivery (OFD) System: An Empirical Study of the Polarization of Potential Consumers and Investigating the Association Between the Determinants Molding the Polarization During COVID-19 Pandemic



Jarin Tasnim, Tanvir Alam, Samapty Saha, and Md Forhad Rabbi

Abstract While ICT is burgeoning in southeast Asia, online food delivery (OFD) picking upstream due to its concrete influence on the mob's experience. The COVID-19 pandemic caused an unprecedented impact in most commerce including OFD due to the escalation of safety aspects. On account of the explosion of the pandemic and to prevent the spread of COVID-19, socio- and economic factors arise that likely turn OFD potential user's attitudes and behavior. This report highlights a six-month-long online survey ($n = 158$) in Bangladesh that analyzes the fluctuation in OFD consumer tendency, identifying the polarization of potential purchasers during the COVID-19 and considering the safety, e-satisfaction, and e-trust. Besides, we also discussed the associations between these determinants that are responsible for polarizing the consumers into marginal groups during the pandemic in developing countries like Bangladesh and proposed some suggestions for OFD service providers based on our findings.

Keywords Human-computer interaction · Bangladesh · Online food delivery · E-trust · Safety · Consumers · Cluster · COVID-19 · Pandemic

1 Introduction

The remarkable growth of Internet and digital technology access and availability is enabling people from previously undervalued or marginalized inhabitants living in the Global South to reap the benefits provided by online retailing and e-commerce development in general. A growing body of research explicates how these distinct communities have appropriated and adopted E-commerce in a variety of novel and innovative means such as OFD System [19, 20]. According to Digital Bangla (2019),

J. Tasnim (✉) · T. Alam · S. Saha · M. F. Rabbi
Shahjalal University of Science and Technology, 3114,Sylhet, Bangladesh
e-mail: frabbi-cse@sust.edu

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_38

Bangladesh's Internet penetration stood at 41% in January 2020 [11]. In Bangladesh, retail e-commerce is growing at 72% per month [3].

Moreover, researchers studying e-commerce applications in the Global South have witnessed consumer views toward online services/retailing that are notably different from Western contexts due to their culture, mentality, situation, mindset, and heritage [1, 10]. For example, the prevalent Western paradigm holds laws for food delivery systems to guard safety, excellence, satisfaction, and diverse traits, which is not the circumstance for collectivist societies where there is no administration to guarantee food quality and promise. Besides, delivery men and the majority of the consumers are not technologically advanced and oblivious of their equities and safety. Because of the mass frequency and congested dwelling, locating dispatch spots are arduous for delivery men.

The COVID-19 pandemic not only sparked fears of an impending economic crisis and recession, but it also hit severely the online food retailing and e-commerce business and belongings [4, 12, 14]. As a consequence of the outbreak, social distancing, self-isolation, travel restrictions, and unemployment lead to a drastic transformation in inhabitant's position, mindset, and financial disposition. The social and cultural ambiances that shape the Global South colonist's perspective toward OFD and the challenges that result from the COVID-19 pandemic are currently not well-known.

Identifying the parameters behind customer e-satisfaction, experience and behavioral intention in Western contexts has been the topic of research for decades [1, 21]. But the notion of customer trait in Western contexts cannot solely be applied as is to alliances in the Global South. Particularly during crisis states like the COVID-19 pandemic, customer behavior and traits are unexplored. Our research fills this cleft in the literature with an inquiry conducted with inhabitants in Dhaka, Bangladesh that (1) generates a nuanced perception safety, hygiene, trust, ease and timeliness expectancy, social influence form consumer satisfaction, behavior, attitude, and practices throughout COVID-19 pandemic and (2) analyzes the challenges and tensions that emerge in OFD sector while COVID-19 pandemic.

2 Related Work

Although OFD are well-known practices affirmed by the restaurant sector universally, scholastic attention in measuring issues associated with OFD is yet nurturing [18]. The most frequent inquiry approach strives to monitor such systems from the customer's perspective. For illustration, in a qualitative study on technology acceptance model (TAM) conducted on university pupils on Turkey that endeavored to determine the perspectives could drive customer's attitudes. The modeled Trust, Innovativeness, and External Influences are the main factors that influence the Internet user's attitudes[1].

Researchers proposed to discover the principal viewpoints that could cause Brazilian shopper's appropriation of OFD and further intimated the significance of content, usability, and functionality on the acceptance of such arrangements [15]. They have

also acknowledged different approaches pertaining to the foremost motorists of the user approval of OFD [21].

Cho et al. [7] discovered that recognized utility and patrons opinion toward such novel systems are broadly molded by the level of trust, product verity, and design. Their experimental research in China and those notable deviations in the customer's perception of such apps were discerned between single-person families and multi-person families.

All former research that experimented with consumer attitude and intention was administered in outline when the COVID-19 pandemic did not hit hard on folk's survival on the globe. The COVID-19 pandemic has had extensive outcomes beyond the scope of the disease itself and forces to quarantine it, including political, cultural, and social implications [2, 13, 16].

A survey study on COVID-19 shows the hostile conclusion of the pandemic on e-commerce applications in Malaysia [9]. An empirical insight from Taiwan confirms that an additional verified case of COVID-19 boosted purchases of online food shopping service trades by 5.7% and the figure of shopper's by 4.9% [5]. Xuwen Gao, Xinjie Shi discover out from contemporary research that the part of confirmed COVID-19 cases progresses the possibility of consumers buying food online[8]. Erudite debates western people are more aware and deliberate than the marginalized people about their food intake. Although delimit factors that have highly pervasive domination on modeling consumer behavior and attitude in the flourished territory, it is not accepted in a developing country. Several articles show the online behavior of consumers varies based on cultural difference [6, 17].

3 Methodology

For discovering insights regarding the perception of service among the native individuals in Bangladesh, we followed quantitative approach. We have constituted a set of questionnaires. There we conveyed several means to dissect diverse aspects of common people associated with the usage of OFD applications. The acknowledgments to the questionnaire reveal the current scenario of the users in terms of their perspective toward OFD usage. The set of questionnaire includes interrogations concerning the followings issues presented in Table 1 .

After receiving the response from the questionnaire, we preprocessed the dataset by handling missing data and employing suitable encoding techniques with the intent to apply statistical means to explore insights. To recognize the separation of OFD users based on perspective and features, we performed clustering. Via cluster analysis, we had spotted polarization of the consumer group based on our dataset, but the correlation between features that possibly mold polarization is yet unexplored. With an aim to examine these associations, we conveyed Chi-Squared hypothesis testing between prominent pairs of features to verify whether dependency exists between the particular pair of feature or not.

Table 1 Information extracted from participants of the survey

Type of questions	Features
Personal information	Locality, Financial condition, Living status, Gender, Age, Salary range
Perspective information	Reliability in services, Trust on quality during the pandemic, Reuse intention, Faced issue during COVID-19, OFD response on issue, Rating system benefited or not, Feels comfortable with address location describing, Observed difference before and after the pandemic, Noticed safety measure, Ensure timeliness, Encouragement behind using OFD applications
Usage of OFD	Frequency of ordering food, Preferred payment method, Preferred time of order, Preferred type of app

4 Data Analysis

The insights have assisted us to recognize the real condition between consumers and providers of OFD systems in Bangladesh during the pandemic. In this segment, we have presented the verdicts of our experiments.

Out of 278 questionnaires, 158 questionnaires were returned, suggesting a 56.7% response rate. The sample data were accumulated from individuals between March to May of 2021 when COVID-19 was at its peak. We have discussed some prominent feature which played a vital role in same genre research in the past studies. As multiple reasons may influence a consumer to lean on OFD applications, that is why we set up a multiple choice question and the outcome is described in Fig. 1. We see a significant portion of people are not sure about their trust issue on OFD application tells us finding out their reason behind insecurity is important to understand the challenges during COVID-19 (Fig. 2).

Using cash on delivery for payment purpose while using OFD imposes a high risk of spreading COVID-19. Despite this, a major portion of consumers(Fig. 3) prefers cash on delivery than other online payment options(using Credit card or Mobile financial service(MFS). Its probable reason could be a limited portion of users in Bangladesh are privileged and at the same time comfortable with credit cards which is used as a payment method with almost all the existing OFD applications (FoodPanda, Shohoz Food, Evaly Food). We observed that some OFD providers (Food Panda) do not have the functionality to pay using the most prevalent MFS systems.

The analysis of the survey data has been performed in two ways: (1) Cluster analysis and (2) Feature correlation analysis.

Cluster analysis: To discover whether the consumers of OFD systems are polarized or not, we performed cluster analysis based on the features.

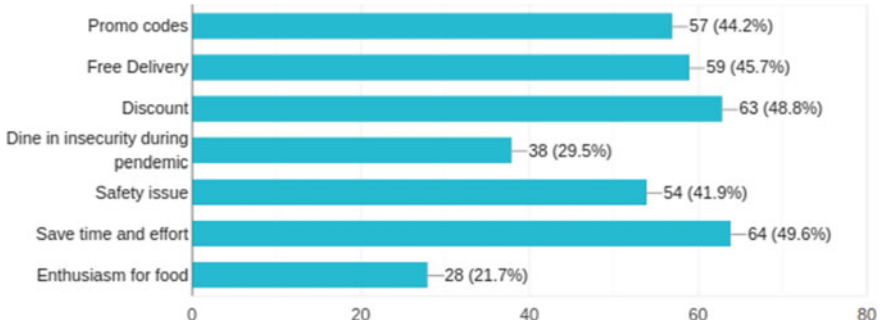


Fig. 1 Encouragement toward using OFD

Fig. 2 E-Trust (Reliability in services)

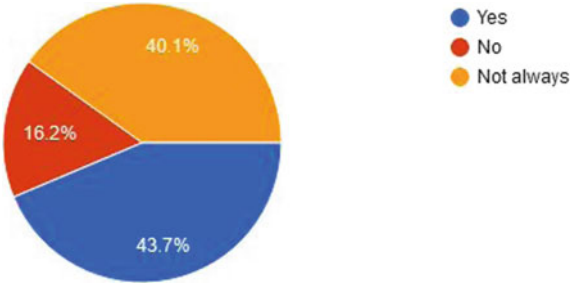
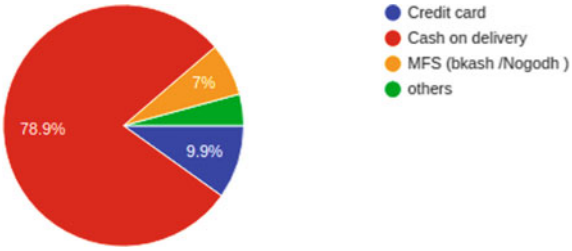
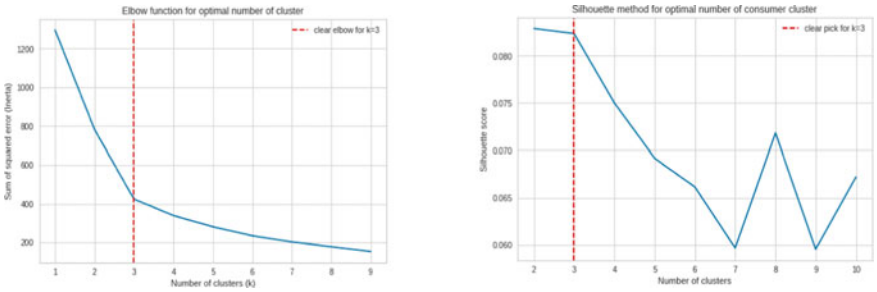


Fig. 3 Preferred payment schemes of User



We dealt with messy data in the following approaches:

- Replace Null Values of a feature with it's mean value in the data frame.
- As most of the features of collected unsupervised data are categorical by characteristics, encoding and scaling techniques are employed to shape the categorical data into numeric values to apply clustering algorithms in the dataset. For ordinal categorical features (salary range, age group, order frequency), we implemented Label encoding; whereas for nominal categorical features (Gender, Location, living status e.t.c), we applied one-hot encoding. The major drawback of one-hot encoding is, for high cardinality, the number of features grows very high resulting in the curse of dimensionality. Due to this, we typically apply one-hot encoding followed by PCA for dimensionality reduction. We find that the judicious combination of one-hot plus PCA can hardly be beaten by other encoding schemes.



(a)Elbow function (fine elbow for k=3) (b)Silhoutte method (pick at k=3)

Fig. 4 marginalized consumer cluster obtained by K-means clustering

Through this process, the dimensionality of the features was reduced into two principal components PC1 and PC2 on which we applied k-means clustering.

We witnessed particular features that could not let data points to be classified into definite groups because certain features affected data points of all clusters on identical significance. That is why in case of including these features lead to a large number of squared error between data points and cluster centroid. To circumvent this problem, we eliminate three features (Preferred app, Ensure timeliness, Preferred time for order) via trial and error. While determining the association between features molding potential online customer behavior, we ignored these features. After reducing the squared error, we are able to group dataset into cluster (For example, $k = 1, 2, 3$, etc.)

To find the optimal number of marginal consumer groups, Elbow function and Silhouette approach are followed, and their outcomes are depicted in (Fig. 4). There is a clear elbow detected in Elbow function (Fig. 4a) indicating three marginal groups of consumers, and from silhouette method evaluation (Fig. 4b), we found a clear pick for $k = 3$ which validate the outcome of elbow function. By clustering, we recognized that the consumer of OFD users is polarized into three marginal groups during the COVID-19 pandemic. The three clusters are visualized in (Fig. 5).

Feature correlation analysis:

Understanding the association between multiple features that lead to an exquisite division of online food consumers into marginalized groups could reveal a notable recognition of practical insight and concealed patterns and will also lead to improvements in decision-making. Earlier in line to acknowledge the valuable insight and abstruse pattern of the dataset, we conducted clustering and only considered those feature that acts a vector enables the entire dataset to be clustered optimally. But the association and inter-dependency linking the feature that could lead to plausible shaping of OFD consumer behavior and attitude are yet unknown.

In order to discover the associations, the feature correlation analysis is directed by developing hypothesis based on prominent features to determine whether there is relationship.

Null hypothesis is rejected for pair of features having P-value$< = 0.05$ and is considered correlated. The p-values and the primary association between the most

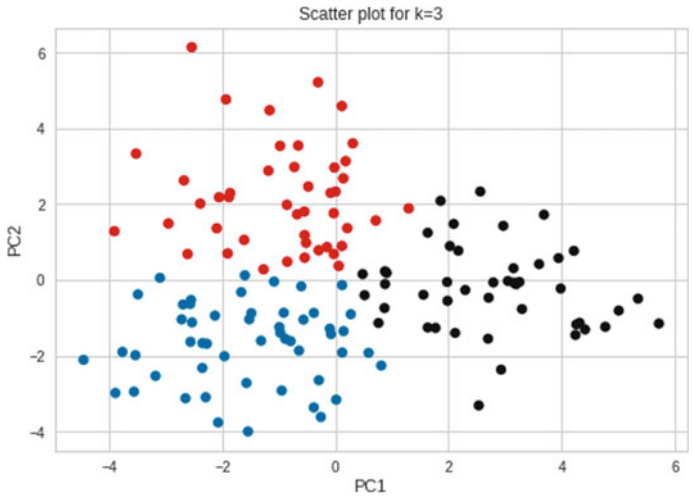


Fig. 5 Polarization of OFD users into three clusters

notable pairs of attributes found in this analysis are presented in Table 2. Here, for example, from the table, we recognize that dwellings from urban areas who have easy access to OFD are more incline to order food online, and also, they are much comfortable in ordering food online even during COVID-19 pandemic.

5 Conclusion and Future Work

The study has endeavored to contribute comprehension regarding the viewpoints and aspects that could mold Bangladeshi consumer's satisfaction and reuse intention toward OFD systems during the crisis moment of the COVID-19 pandemic. Based on findings, OFD service providers can improve their services and user experience during the COVID-19 pandemic, which will help them to gain consumers' faith. In future, we wish to work on the following aspects:

– Designing prototype from HCI perspective that OFD applications should adopt to regain or maintain consumer trust using OFD considering the pandemic situation.
– We encourage further participatory work analyzing how the dimensions of each feature are correlated and associated with each other and their impact on clustering.

Although we had some limitations due to the ongoing pandemic situation, we cannot conduct any qualitative interview as people are not in the metal state to participate it because, whether they or their family members are affected by COVID-19 situations. We believe if we are able to conduct qualitative interview, we can get more clear picture.

Table 2 Feature correlation analysis

Feature 1	Features 2	P-value	Null hypothesis	Result
Locality	Order frequency	0.0047	Rejected	People staying in the Urban area are more inclined to use OFD than sub-urban area.
Locality	Reuse intention	0.000543	Rejected	City people are more inclined to reuse OFD system
E-trust	Reuse intention	0.00094	Rejected	Consumers who find OFD reliable are interested in reusing it
Locality	E-trust	0.000543	Rejected	Urban people feels more reliable in ordering food online than Suburban people
AGE	Financial condition affect	0.00421	Rejected	Effect on financial status during COVID-19 varies based on age groups.
OFD response on issue	Reuse intention	0.00376	Rejected	People who have a smooth experience of using OFD are tend it utilize it again.

References

1. S.M. Alagoz, H. Hekimoglu, A study on tam: analysis of customer attitudes in online food ordering system. Proc.-Soc. Behavioral Sci. **62**, 1138–1143 (2012)
2. S.R. Baker, N. Bloom, S.J. Davis, K.J. Kost, M.C. Sammon, T. Viratyosin, *The Unprecedented Stock Market Impact of Covid-19* (Tech. rep, National Bureau of Economic Research, 2020)
3. BizDataInsight: Rising of online food delivery business (2019 (accessed May 19,2019)). https://bizdatainsight.com/2019/05/27/rising-of-online-food-delivery-business/

4. J.J. Cavallo, H.P. Forman, The economic impact of the covid-19 pandemic on radiology practices. Radiology, 201495 (2020)
5. H.H. Chang, C. Meyerhoefer, *Covid-19 and the Demand for Online Food Shopping Services: Empirical Evidence from Taiwan*. Tech. rep, National Bureau of Economic Research (2020)
6. P.Y. Chau, M. Cole, A.P. Massey, M. Montoya-Weiss, R.M. O'Keefe, Cultural differences in the online behavior of consumers. Commun. ACM **45**(10), 138–143 (2002)
7. M. Cho, M.A. Bonn, J.J. Li, Differences in perceptions about food delivery apps between single-person and multi-person households. Int. J. Hospitality Manage. **77**, 108–116 (2019)
8. X. Gao, X. Shi, H. Guo, Y. Liu, To buy or not buy food online: the impact of the covid-19 epidemic on the adoption of e-commerce in china. PloS one **15**(8), e0237900 (2020)
9. M.W. Hasanat, A. Hoque, F.A. Shikha, M. Anwar, A.B.A. Hamid, H.H. Tat, The impact of coronavirus (covid-19) on e-business in Malaysia. Asian J. Multidisc. Stud. **3**(1), 85–90 (2020)
10. J.J. Lee, S. Lee, The differences of Asian and western consumer's attitudes towards brand extensions by information types: attribute-related vs. non-attribute-related information. Int. Rev. Manage. Marketing **7**, 281–290 (2017)
11. S.Y.T. Lee, C.W.D. Phang, Leveraging social media for electronic commerce in Asia: research areas and opportunities. Electronic Commerce Res. Appl. **14**(3), 145–149 (2015)
12. N.V. Loayza, *Costs and Trade-offs in the Fight Against the Covid-19 Pandemic: A Developing Country Perspective* (2020)
13. medicalnewstoday: COVID-19 global impact: How the coronavirus is affecting the world (2020). https://www.medicalnewstoday.com/articles/covid-19-global-impact-how-the-coronavirus-is-affecting-the-world
14. M. Nicola, Z. Alsafi, C. Sohrabi, A. Kerwan, A. Al-Jabir, C. Iosifidis, M. Agha, R. Agha, The socio-economic implications of the coronavirus and covid-19 pandemic: a review. Int. J. Surgery (2020)
15. G. Pigatto, J.G.C.F. Machado, A. dos Santos Negreti, L.M. Machado, Have you chosen your request? analysis of online food delivery companies in brazil. Br. Food J. (2017)
16. K. Søreide, J. Hallet, J.B. Matthews, A.A. Schnitzbauer, P.D. Line, P. Lai, J. Otero, D. Callegaro, S.G. Warner, N.N. Baxter, et al., Immediate and long-term impact of the covid-19 pandemic on delivery of surgical services. Br. J. Surgery (2020)
17. C. Tirelli, M.P. Martínez-Ruiz, R. Gómez-Ladrón-De-Guevara, Major influences on buying decision processes by international university students. differences by continent of origin. Appetite **71**, 104–112 (2013)
18. Y.S. Wang, T.H. Tseng, W.T. Wang, Y.W. Shih, P.Y. Chan, Developing and validating a mobile catering app success model. Int. J. Hospitality Manage. **77**, 19–30 (2019)
19. R.H. Weber, Digital trade and e-commerce: challenges and opportunities of the Asia-pacific regionalism. Asian J. WTO Int. Health L Pol'y **10**, 321 (2015)
20. C.M. Wood, Marketing and e-commerce as tools of development in the asia-pacific region: a dual path. Int. Marketing Rev. (2004)
21. V.C.S. Yeo, S.K. Goh, S. Rezaei, Consumer experiences, attitude and behavioral intention toward online food delivery (ofd) services. J. Retailing Consumer Services **35**, 150–162 (2017)

Accident Hotspot Detection by DB-Scan Clustering



Pooja Shinde, Gauri Kudalkar, Shruti Pawar, Harshita Tiwari, and Hitendra Khairnar

Abstract "Road Accident Alert System" is being created keeping in mind the large number of road accidents and related casualties that occur every day in Bengaluru, India. Knowing the conditions under which these accidents happen and where they happen is a very powerful information that can be used to take action to avoid them. Our main objective is to identify the accident hotspots in the city with the help of thorough and discrete data given about the various road accidents taking place in the city. Our app will alert the user regarding the accident hotspots while using the Web app for navigating from source to destination. The proposed idea precisely focuses on the accident-prone zones in Bengaluru. Using the dataset available, the blackspots are identified and clustered to form accident zones within the city. This paper will focus on the implementation of clustering algorithm to generate the list of blackspots, the technical requirements and voice alerts given to the user.

Keywords Road accidents · Clustering · Data mining · Accident zones · Hotspot zones · DB-scan · REST architecture

1 Introduction

Bengaluru, India, stood third in the number of road accidents that took place amongst various cities in the country in 2019. The IT capital of India reported 4,684 accidents and 768 deaths last year, an increase of 1.6% and 12%, respectively, over 4,129 accidents and 686 deaths the year before, according to the data issued by the Ministry of Road Transport and Highways.

Most of the deaths could have been avoided if the details of accident-prone zones were informed and reported at the earliest. Our motive is to build a Web application which displays the accident prominent zones and alerts the user when they arrive near

P. Shinde (✉) · G. Kudalkar · S. Pawar · H. Tiwari · H. Khairnar
Cummins College of Engineering for Women, Pune, India

H. Khairnar
e-mail: hitendra.khairnar@cumminscollege.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_39

them, thereby making the navigation safer for the users travelling across Bengaluru city.

This paper describes the technologies, the requirements, the implementation method to generate accident zones, the overview of the clustering algorithm we have implemented and also the voice alert feature along with result and conclusion.

2 Technology and Requirements

2.1 Technologies Used

For backend development purpose, Spring Boot framework has been utilized to adhere industrial standard for code. The primary coding language used is Java with REST framework. Hence, a client–server frame work exists, where the client sends HTTPs request to the server using Web browser. The backend takes support from MS-SQL database to store accident-related data.

For the frontend development (client-side development), we are using React JS library along with Ajax—Asynchronous JavaScript and XML, which though not a technology by itself, is a new way to utilize a number of existing technologies altogether, including HTML CSS, JavaScript, DOM, XML, XSLT, and most importantly the XMLHttpRequest object [1].

2.2 Requirements

Hardware Requirements. Since the client application is a Web application, the basic availability of PC or mobile with a compatible Web browser, speaker or audio access and wireless Internet connection satisfies the needs of this application.

Software Requirements. Interface between the application and third-party libraries for geolocation access. Adding dependencies via SpringBoot and setting up MS-SQL database. Configuring this connection acts as the communication interface between the application and the database server.

3 Implementation

3.1 Execution Plan

When HTML CSS, JavaScript, DOM, XML, XSLT, and most importantly the XMLHttpRequest object technologies are combined in the Ajax model, Web applications are able to deliver fast, incremental updates to the user interface without

needing to reload the entire browser page. This makes the application faster and more responsive to user actions [2].

JSON is used more than XML in AJAX because of its advantages like being lighter. Both JSON and XML are used for packaging information in the Ajax model. Thus, Ajax is a tool set which acts as client-side Web development technologies.

REST (Representational state transfer) software architecture [3] is implemented which uses subset of HTTP. The advantages of using REST architecture are it provides on demand service and takes care of scalability of the application. It also provides flexibility and portability to user allowing the user to use any client device to connect to backend server.

With REST architecture, the client through frontend service sends a "get" request to the backend server to get a blackspot list. The blackspots are the location spots where accidents occur more frequently and thus are to be critically observed to avoid or reduce accidents considerably.

The backend server is responsible for generating list of blackspots. To generate blackspot, the backend framework uses a list of accident locations. This list of accident location is clustered using clustering algorithms like a DBSCAN (Density-based spatial clustering algorithm) [4], and these clusters are considered to form into a blackspot or accident-zone.

The history of accident locations stored in the MS-SQL database, filtered based on time and weather, is used as an input to this algorithm. At output, multiple blackspots are discovered. These blackspots are then sent as a response to the get request from frontend client.

The Fig. 1 describes the activity at backend server in sequence.

After getting the list of blackspots as a response from the backend server, they are displayed on the map in the client application using marker class [5] (Fig. 2).

The voice alerts are generated in the client application using React-H5-Audio-Player package [7] when the user comes near the accident zone (200 m before arriving in the accident zone). We use geolocation tracking here to continuously keep the track of user's location while they are travelling.

3.2 Clustering

For clustering, we are using DBSCAN, density-based spatial clustering algorithm [4]. The advantage of this is that in DBSCAN, unlike K-means, we need not specify the number of clusters we want to form; rather, based on the scenario, DBSCAN adjusts the number of clusters. Hence, number of blackspots need not be restricted rather depends on accident locations.

Noise factor or the outliers are taken care by the algorithm while clustering. This ensures accuracy of blackspots. The shape for cluster is not fixed and decided based on situation. This ensures that it reflects the real nature of the blackspot regions which are not restricted by shape, and their shape may vary from region to region.

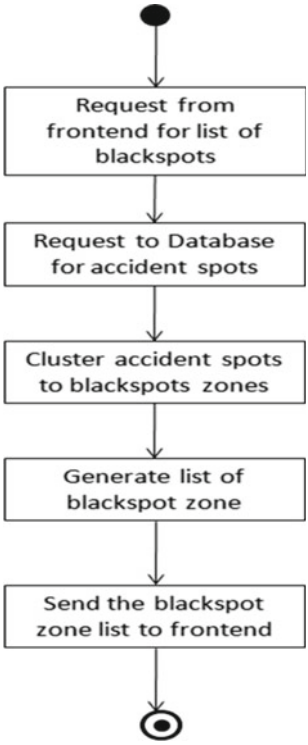


Fig. 1 Activity diagram

$$\text{hav}(\Theta) = \text{hav}(\varphi_2 - \varphi_1) + \cos(\varphi_1)\cos(\varphi_2)\,\text{hav}(\lambda_2 - \lambda_1)$$

where

- φ_1, φ_2 are the latitude of point 1 and latitude of point 2 (in radians),
- λ_1, λ_2 are the longitude of point 1 and longitude of point 2 (in radians).

Fig. 2 Haversine equation formula [6]

For implementing the algorithm, we are using Haversine metric as shown in Fig. 2. The Haversine formula is most prominently used in navigation-related calculations as in our case. We use the above equation to get the distance value between two geolocation coordinates more accurately considering the earth's spherical nature, thereby increasing our algorithm's performance. This brings the project model more near to accurate measurements [6].

3.3 Implemented Algorithm

```
public List<Cluster> getClusters() {
  for(location point: this.points){
      if(this.visited.get(points.indexOf(point))!=null){
        continue;
      }
      List<Integer> neighbors = getNeighbors(point);
      if(neighbors.size() >= this.min_points) {
      Cluster c = new Cluster(this.clusters.size());
      buildCluster(point,c,neighbors);
      this.clusters.add(c);
      }
      else this.visited.put(points.indexOf(point),true);
    }
    return this.clusters;
}
```

4 Result

The result of the DBSCAN clustering algorithm implemented is a list of clusters as a JSON object. Each cluster has a cluster ID, viz. clusterId and list of geolocation coordinates of the accident spots included in that cluster to form zones. These zones formed based on location, time and weather conditions, are displayed on the map in the client application using markers.

User gets voice alerts while travelling when he comes near an accident zone (200 m before), informing him about the reason and precaution to avoid any accident while driving in that accident zone. The number of clusters formed won't be limited and can increase as we add more data in the database, it will also make the locations of the clusters more accurate and will increase the overall efficiency of the result with the help of the algorithm.

5 Conclusion

The application generates accident zones and alerts the user regarding the areas or geolocations where user must drive more safely in the city considering past experiences of that location by others. This will increase road safety and potentially reduce the number of road accidents occurring within the city. Providing the service as a

Web application will help the user run the service anytime anywhere on demand and on any device without downloading.

The service is trustworthy to all the users as nobody other than the traffic management authorities can feed the data to the system and the authentication and authorization of a responsible person will be taken care by the system.

The app will not be able to function without a stable internet connection. It also requires regular updates on data from traffic and other concerned authorities to maintain its overall efficiency and give latest details to the users.

References

1. X. Zhang, Y. Zhang, J. Wu, Research and analysis of Ajax technology effect on information system operating efficiency, in *Research and Practical Issues of Enterprise Information Systems II, IFIP—The International Federation for Information Processing*, vol. 254, ed. by L.D. Xu, A.M. Tjoa, S.S. Chaudhry (Springer, Boston, MA, 2008), pp. 641–649
2. J.J. Garrett, *Ajax: A New Approach to Web Applications, Adaptive Path* (2005). http://www.adaptivepath.com/publications/essays/archivcs/000385.pbp. Last accessed 2021/03/28
3. R. Richards, Representational State Transfer (REST), in *Pro PHP XML and Web Services*. Apress, Berkeley, CA (2006), pp. 633–672
4. M. Ester, H.P. Kriegel, J. Sander, X. Xu, A density-based algorithm for discovering clusters in large spatial database with noise, in *Proceeding of KDD*. AAAI, Portland (1996), pp. 226–231
5. Google Maps Platform Web Documentation for JavasScript Map API - Marker class. https://developers.google.com/maps/documentation/javascript/reference/marker. Last accessed 2021/04/18
6. E. Winarno, W. Hadikurniawati, R.N. Rosso, Location based service for presence system using haversine method, in *2017 International Conference on Innovative and Creative Information Technology (ICITech)*. IEEE, Salatiga, Indonesia (2017), pp. 1–4
7. React-H5-Audio-Player official Documentation. https://www.npmjs.com/package/react-h5-audio-player. Last accessed 2021/04/21

AI Powered Language Teaching Bot Using Dialogflow



Chingmuankim and Rajni Jindal

Abstract Oftentimes, we as humans want an instant answer and reply to the many questions in our heads, and it is not always possible to get answers for our queries at one go. However, with the advancement in the field of artificial intelligence, we can overcome these challenges with the help of a chatbot. This chatbot is a software influenced by an AI that gives an automatic response to the user. In this paper, the authors have utilized a tool called Dialogflow for implementation of a chatbot that can simulate a language translator for Paite. Dialogflow has a pre-trained machine learning-based model that allows us to feed in our data for automatic response. The proposed application is to give translation in Paite for the input words and sentences. The Chatbot serves as a Paite language teaching bot in this application. This application is beneficial for both the end user and the developer as the user gets his/her desired response, and the developer saves his/her time giving response to the many queries received daily. Furthermore, we will discuss in detail about the workflow and the methodology behind implementation of this work.

Keywords Chatbot · Artificial intelligence · Machine learning · NLP

1 Introduction

An AI powered language teaching bot is an intelligent bot that can understand the intent of the input given by the user which correspondingly provide a meaningful response to the queries and request. AI powered bots are smarter than the normal chatbots as it uses natural language processing and machine learning. It is basically a simulation of features of human being such as trainability, dependability and scalability.

Features of a Chatbot

Chingmuankim (✉) · R. Jindal
Delhi Technological University, New Delhi, India
e-mail: chingmuankim_phd2k19@dtu.ac.in

R. Jindal
e-mail: rajnijindal@dce.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_40

Trainability: This intelligent bots can be trained to perform the task which we want to do. It can improve overtime and learn from its experiences through every interaction it had and eventually become smarter and efficient than the normal chatbots.
Dependability: It is dependable as it can be used anytime and anywhere unless there is network issue.
Scalability: It is adaptable to the demands of the users by expanding its resources in terms of size and others such as its vocabulary and dictionary.

All the above-mentioned features can be found in Dialogflow. Dialogflow is a Google Cloud platform powered by an AI that allows developers to create chatbots as per the user's requirements. It is a state-based data model that allows the users to trigger intents as many times they require, define transitions and can manage queries beyond the training data. One interesting thing about this tool is that it is a cross-platform tool and can also be integrated with various social networking applications such as Facebook messenger, Telegram, Line, Twitter, Viber, Skype and many other. It has the capability to understand natural language.

2 Literature Review

Chatbot is a technology that can simulate conversation between the agent and the users without the intervention of human beings [1] by making use of a natural language through various platforms such as websites, mobile applications, messengers, etc. Chatbots are trained to give meaningful responses to the users by pre-feeding data which are most likely expected to be asked by the end users. Chatbots without the presence of NLP is just a processing and exchange of text without any meaningful conversation. However, with the help of NLP, it is possible to extract the intent of the users' queries, thus making it more intelligent. Various researchers has conducted their study in the field of NLP using chatbots. Some of these will be discussed in the following:

Patel et al. [2] created a web-based UNIBOT that provides various information about students and college-related information. The proposed work is created using PHP using the concept of AI and ML. Students can pose queries related to information regarding the university. But how about understanding the user's intent and not just responding to the queries?

Reyes et al. [3] discussed about the methodologies used for developing a virtual assistant that can help students learn on their own. These process involves knowledge abstraction, response generation and the flow of conversation and decision trees. This virtual assistant gives answers to the queries asked by multiple students at the same time. Such kind of virtual assistants are useful where there is scarcity of teachers in universities and improve the performance of students. In this work, data have been collected from internet on discussion forums and interaction with students, assignment work and frequently asked questions on the topic which the teacher

knows. They have created the data using two spreadsheets, one having details of the syllabus of the subject and important concepts while the other contains questions and answers taken from the internet.

Kowsher et al. [4] developed a Bengali chatbot which is also known as Doly that is used for education purpose. They have used machine learning search algorithms to discover list of matching results from the corpus. Naïve Bayesian algorithm is used for generation of the right answer. In the later part, they have compared their chatbot with neural conversational machine (NCM) and Cleverbot. NCM is an end-to-end model which requires previous sentences or pre-defined rules to predict the next sentence. While Doly is a retrieval-based system that works by feeding in random questions to the NCM and gives response to the queries.

Purohit et al. [5] build a chatbot which is a deep learning-based dialogue system on a sarcastic, non-sarcastic, emotional and humorous data. In this work, they have trained a seq-to-seq model on 3000 question–answer-based dataset and experimented these human-like traits data with an end-to-end dialogue system. Long short-term memory (LSTM) is used as an encoder model for mapping the word-level sequence of input sentences to state vectors. The target sequence of sentences is decoded by the second LSTM model one token at a time. Greedy Search algorithm is used for predicting the next utterance.

On reviewing these papers, a few gaps have been discovered in [2, 3] on the technique employed.

Patel et al. [2] found that the chatbot lacks intelligence, in the sense that it does not have the ability to understand the intent of the user's request, i.e. it lacks NLP.

Reyes et al. [3]. Chatbot lacks features like embedding link of the recorded video lectures of the faculty, so the student can understand better. Moreover, the bot could also have a feature that could capture the student's attendance and store at one place so that it will be easy for the faculty to access.

Besides all this, it is also found that understanding user's intent requires mapping between queries and its ambiguous answers. Such type of issues can be enhanced by applying NLP techniques to the data. In this work, one of the NLP technique called named entity recognition is applied to enhance the smartness of the bot.

3 Methodology

The development of this chatbot involves three phases. These are:

3.1 Design Phase

In the design phase, we decide on what to build, taking into account the reaction on the end product we want to have on our chatbot. We define the personality [6] and expression [7, 8] of the chatbot we desire to have based on our requirements.

Table 1 Sub-modules of intent and its task

S.no.	Sub-modules	Task
1	Training	Feeding of data
2	Response	Adding words and phrases correspondingly to the training data for each intent
3	Parameters	Extracted values from the training phrases These parameters are assigned entity type that can be used to perform logic or generate responses
4	Contexts	These helps us understand the intent of the phrases input by the end user

By personality and expression, we mean to say whether the chatbot should simply respond to the user's request, act smartly by giving suggestions to users, perform-based task etc.

3.2 Development Phase

In these phase, we create our chatbot by feeding the data into the console. These phase further consists of creation of two modules. These are the two core areas of the application of NLP technique applied to this work. These two modules are:

3.2.1 Intent

In these, we can train our system by adding words and phrases which the end user is likely to ask the agent and add responses to it accordingly (Table 1).

3.2.2 Entities

This module is used to extract useful facts from what the end user typed such as nouns, quantifiers, numbers, dates, who, what, where, and when. It is used here as a named entity recognition technique that extracts information from the queries of the end users and are being used by the developer to give a smart reply.

3.2.3 Deployment Phase

In this phase, we chose the platform for deploying the chatbot for use.

4 Algorithm

This chatbot follows a hybrid-based approach which is a combination of a rule-based and machine learning-based approach, one for the purpose of matching and the later for selecting the best result. In rule-based approach, the agent matches the sentence correspondingly to the input by the user and extract parameters if it has been specified in the training phrase.

For example: If the agent asks for user's credentials such as name, age and gender, the agent will start to match the input or response given by the user; if found matching, it will extract the parameters as specified.

While in machine learning-based approach, the agent learns from the occurrences of the pattern of the training phrases and the language models that has been provided to the console of the Dialogflow. It is also responsible for understanding the expressions of the end users, performing matching with the intents and extract structured data. Based on these structured data, it creates model for making decisions about which intent should be matched to the expressions of the end users.

For example: If the training phrases has been specified with a parameter such as last name, noun, pronoun and adjectives, the agent will be able to learn and identify these parameters automatically as more number of phrases are fed to the training data, without the need to manually specify it all the time. With lots of training phrases and responses fed into Dialogflow which are having the same intent, ML model will decide which intent will be the best match to the end users expressions. This will be done by the machine itself.

5 Data Preparation

For initiating the conversation, we have created a module name "Greetings" which includes the basic introduction of every conversation. The entire hierarchy of the tree structure is listed in Fig. 1. Data are prepared accordingly for each module.

6 Output

Figure 2 shows the output of the tested data. It can be concluded from the figure that when the user queries for the translation of a numerical number "one", named entity recognition technique is applied to extract information by specifying it is a number to the entity module. By doing so, developer do not require to re-type the digit "one" for every response.

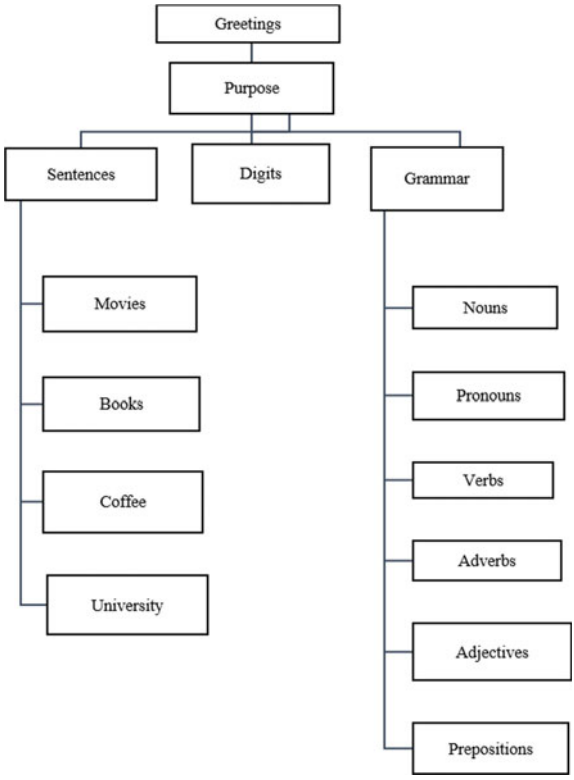


Fig. 1 Hierarchy of the tree structure

7 Conclusion and Future Work

The presence of NLP technique has a positive impact on the chatbot by improving its performance, enhancing personality of the bot which makes it an intelligent bot. Moreover, making it more user-friendly and flexible to be used by the end users. Besides language translator, the tool can also be used in various fields. One such is in the field of education [3]. NLP can also be applied to automatically check open-ended questions and assign marks without the intervention of the faculty. Sentimental analysis can also be performed on the sentences input by the user.

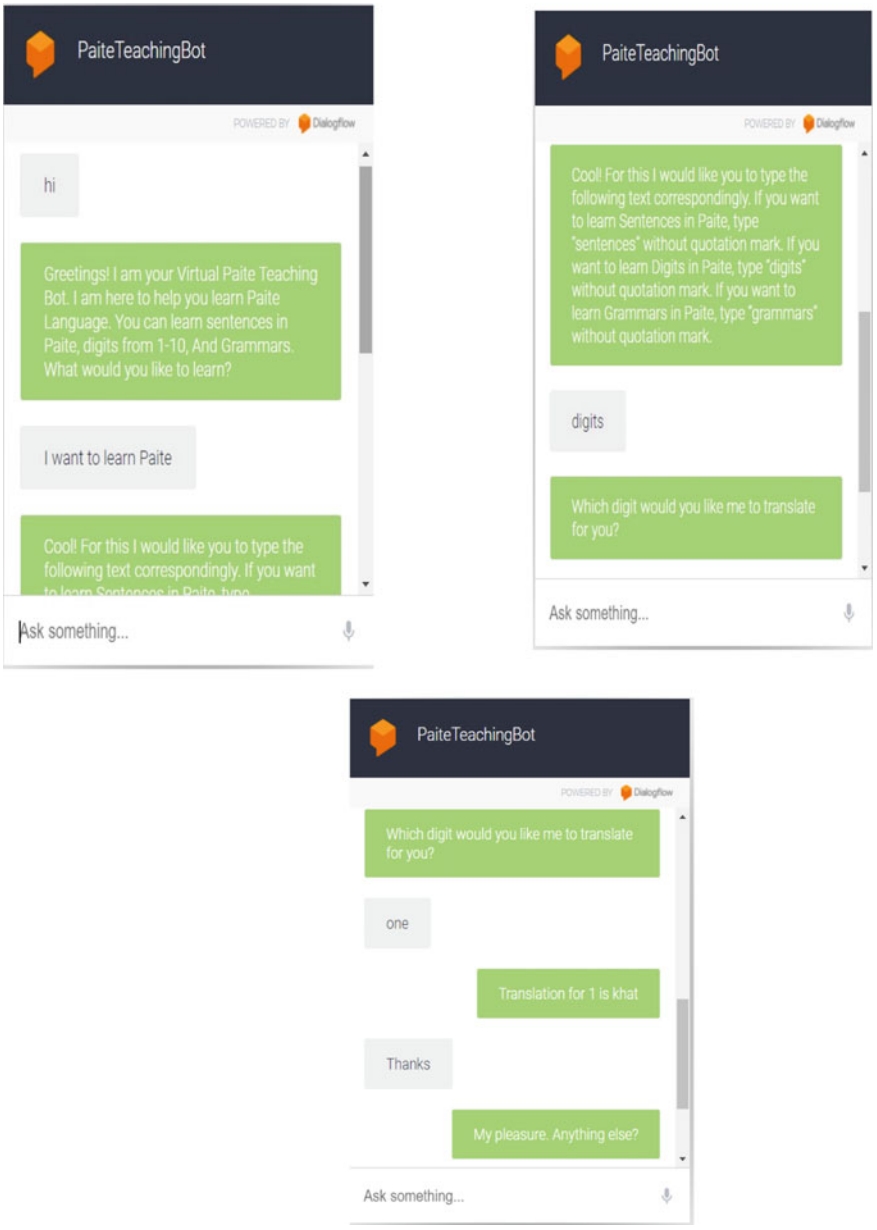

PaiteTeachingBot
POWERED BY Dialogflow
hi
Greetings! I am your Virtual Paite Teaching Bot. I am here to help you learn Paite Language. You can learn sentences in Paite, digits from 1-10, And Grammars. What would you like to learn?
I want to learn Paite
Cool! For this I would like you to type the following text correspondingly. If you want
Ask something...
PaiteTeachingBot
POWERED BY Dialogflow
Cool! For this I would like you to type the following text correspondingly. If you want to learn Sentences in Paite, type "sentences" without quotation mark. If you want to learn Digits in Paite, type "digits" without quotation mark. If you want to learn Grammars in Paite, type "grammars" without quotation mark.
digits
Which digit would you like me to translate for you?
Ask something...
PaiteTeachingBot
POWERED BY Dialogflow
Which digit would you like me to translate for you?
one
Translation for 1 is khat
Thanks
My pleasure. Anything else?
Ask something...

Fig. 2 Output

References

1. N. Albayrak, A. Ozdemir, E. Zeydan, An overview of artificial intelligence based chatbots and an example chatbot application | Yapay Zeka Tabanli Rehber Robotlara Genel Bir Bakis ve Örnek Bir Rehber Robot Uygulamasi. 26th IEEE Signal Process Commun. Appl. Conf. SIU **2018**, 1–4 (2018)
2. N.P. Patel, D.R. Parikh, D.A. Patel, R.R. Patel, AI and web-based human-like interactive University Chatbot (UNIBOT), in *2019 3rd Int. Conf. Electron. Commun. Aerosp. Technol.*, pp. 148–150 (2019). https://doi.org/10.1109/iceca.2019.8822176
3. R. Reyes, D. Garza, L. Garrido, V. De la Cueva, J. Ramirez, Methodology for the implementation of virtual assistants for education using Google Dialogflow, in *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11835 LNAI, no. October, pp. 440–451 (2019). https://doi.org/10.1007/978-3-030-33749-0_35
4. M. Kowsher, F.S. Tithi, M. Ashraful Alam, M.N. Huda, M. Md Moheuddin, M.G. Rosul, Doly: Bengali Chatbot for Bengali Education, in *1st Int. Conf. Adv. Sci. Eng. Robot. Technol. 2019, ICASERT 2019*, vol. 2019, no. Icasert, pp. 1–6 (2019). https://doi.org/10.1109/ICASERT.2019.8934592
5. J. Purohit, A. Bagwe, R. Mehta, O. Mangaonkar, E. George, Natural language processing based jaro-the interviewing chatbot, in *Proc. 3rd Int. Conf. Comput. Methodol. Commun. ICCMC 2019*, no. Iccmc, pp. 134–136 (2019). https://doi.org/10.1109/ICCMC.2019.8819708
6. S. Ilíc, R. Nakano, I. Hajnal, Designing Dialogue Sy*stems: A Mean, Grumpy, Sarcastic Chatbot in the Browser*. arXiv (2019)
7. K.A.L.R. Carranza, J. Manalili, N.T. Bugtai, R.G. Baldovino, Expression tracking with OpenCV deep learning for a development of emotionally aware Chatbots, in *2019 7th Int. Conf. Robot Intell. Technol. Appl. RiTA 2019*, pp. 160–163 (2019). https://doi.org/10.1109/RITAPP.2019.8932852
8. C.H. Kao, C.C. Chen, Y.T. Tsai, Model of multi-turn dialogue in emotional Chatbot, in *Proc. - 2019 Int. Conf. Technol. Appl. Artif. Intell. TAAI 2019*, pp. 1–5 (2019). https://doi.org/10.1109/TAAI48200.2019.8959855

Analyses of Feature Selection and Classification Techniques for Diabetes Prediction



Sina Patel, Vijayshri Khedkar, and Sonali Kothari Tidke

Abstract Diabetes is a metabolic disease that severely affects the human body causing high sugar levels in the blood. Machine learning has been used for predicting various diseases. Researchers across the globe are motivated to experiment with different methods to predict diabetes at an early stage. Different classifiers are used for predicting diabetes, yet some classifiers are barely analyzed. Predicting diabetes at an early stage with easy to measure factors will help patients and healthcare workers to tackle the consequences of diabetes at starting stage and save lives. Also, feature selection plays an important role in building any machine learning model, and it becomes even more major aspect when dealing with medical data. In this paper, various techniques for feature selection and prediction of diabetes are reviewed.

Keywords Diabetes · Machine learning · Prediction · Feature selection · Classification

1 Introduction

The number of people suffering from chronic diseases is vast worldwide. However, the main reason of concern is the people affected by diabetes disease and its related complexities among these people. There are different factors that characterize diabetes mellitus as a chronic disease. These factors include a long healing cycle, many severities, and persistent diseases. Predominantly, types of diabetes fall under three categories: type-1, type-2, and gestational. The first type of patient's body generally does not produce enough insulin. This type is assumed to occur due to genetics. Some medical indications of this disease are more thirst and repeated urination, high blood sugar levels, etc. However, this type cannot be prevented. In

S. Patel (✉) · V. Khedkar · S. K. Tidke
Symbiosis International (Deemed University), Symbiosis Institute of Technology, Pune, India

V. Khedkar
e-mail: vijayshri.khedkar@sitpune.edu.in

S. K. Tidke
e-mail: sonali.tidke@sitpune.edu.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_41

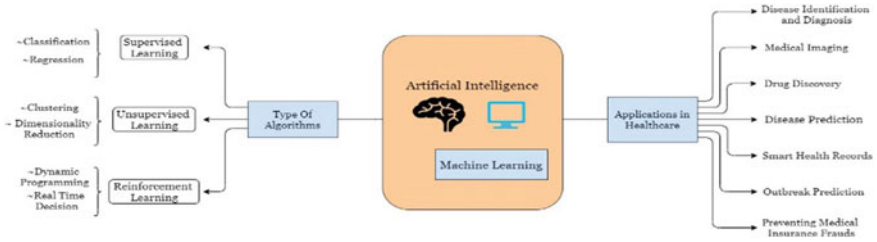


Fig. 1 Machine learning and healthcare domain

the second type of this disease, insulin is produced in the body but unable to use it. In old people, this disease mainly occurs due to obesity, high blood pressure, lifestyle, and other maladies. This can be prevented if detected at an early stage. The third type occurs during pregnancy when the body cannot produce enough insulin. Signs of this type are excessive thirst, not clear vision, and slow healing wounds. Due to the advancements in the information of medicine, medical sectors with the enormous amount of complex patient data are eager for extracting valuable information from this data to aid in the growth of these sectors [1]. The application of machine learning and other artificial intelligence systems for the study of clinical data to aid in diagnosis and therapy is an indicator of smart medicine with the most real-world importance. The improved standard of living of people and the western-influenced dieting habits have considerably increased the incidence, mortality, and morbidity of diabetes and impacted our health seriously.

The role of machine learning as a tool in clinical databases is quite important. This method provides a set of comparatively improved resources for enhancing the sensitivity and/or specificity in the prediction and diagnosis of diseases [2]. In medical science research, machine learning has emerged as one of the main prioritized topics due to the serious social impression of the specific illness. Figure 1 shows various applications of machine learning in healthcare domain. Hence, machine learning methods in diabetes mellitus are undoubtedly a big matter of concern in estimation, diagnosis, control, and other associated clinical administration factors. The maximized scale and complexity of medical data has made the prediction of diabetes mellitus a critical and complex research issue [3].

In the field of medical science, accuracy is always a major issue; with different algorithms, we can obtain different accuracies on the same dataset. So, it is very important to analyze which algorithm provides the best outcome for better prediction. Identifying the most influential risk factors which ultimately increase the prediction accuracy is a heavy task when there are multiple features in a dataset. Selecting all features or irrelevant features often leads to complex systems, decreased accuracy, and consumes more time. Therefore, feature selection is an important step in building a model for predicting diabetes. Feature selection is process to identify most relevant features that contribute the most to the outcome.

This paper reviews current methods for feature selection and prediction of diabetes using machine learning.

2 Diabetes Prediction Techniques

There are mainly two approaches identified for predicting diabetes:

2.1 Machine Learning-Based Techniques

Xu et al. [4] devised a random forest (RF)-based diabetes prediction model for predicting T2DM. The key objective of this work was to analyze the impact of some existing signs on diabetes as well as to discover rules on original data. This technique could considerably reduce disease risk through as curtaining a strong and comprehensible model for T2DM from a clinical database. RF classifier made use of many decision trees for sample training, and integrated all trees; weight for generating conclusive outcomes. In the conclusion, the RF algorithm reduced the overfitting issue of the single decision tree to a great extent.

Zhu et al. [5] recommended a new model based on data mining to diagnose and predict diabetes disease in early stage. k-means was a simple clustering algorithm. This algorithm could be utilized for different types of data. This algorithm was very responsive to original locations of cluster center. This algorithm either provided an enough and competently clustered dataset for the logistic regression model, or lesser data due to the inaccurate clustering of the real dataset. The tested outcomes depicted that PCA algorithm made improvements in the k-means approach. This k-means algorithm showed 2.5% improvement in accuracy rate while logistic regression showed 1.98% more accuracy rate.

Syed et al. [6] presented an algorithm that had taken the benefit of partitioning based on tree. The adaptive SVM approach was utilized to perform the classification. The preprocessing was carried out under sampling SMOTE that was capable to prune the data. The outcomes demonstrated that the presented algorithm were more effective as compared to the conventional solution to process diabetic data and discover effective classification from it.

Husain and Khan [7] investigated the performance of ensemble learning of various machine learning paradigms. Author utilized NHANES dataset which is a form of survey data and concluded that ensemble technique gives better performance. The main aim of the paper was to predict diabetes at early stage. The performance of proposed approach was 0.75 AUC.

Maniruzzaman et al. [8] suggested the use of logistic regression as feature selection technique. Author combined this approach with random forest as classification algorithm. The main aim was to identify the risk factors associated with diabetes using logistic regression and identify the best performing protocol. NHANES dataset was used with NB, DT, AB, and random forest classifier. Results shows random forest yield good accuracy.

Priya et al. [9] conducted a research work to analyze the diabetic patients' datasets along with predicting the diabetes mellitus disease in the initial stage. This work

made use of naïve Bayes classifier model for diabetes prediction. The information from medical databases with different features was gathered to arrange information in the diabetes dataset of patients. The recommended scheme based on naïve Bayes classifier generated predictive results of diabetes by accepting different input features such as blood pressure, sugar level, etc. Predictions based on all these factors were highly accurate.

Sneha and Gangil [10] used decision tree, naïve Bayesian, support vector machine, random forest, and K-nearest neighbor for predicting diabetes in early stage on data collected from UCI with attributes usually requiring lab tests. The main aim was to select correct attribute. Author proposed a multistep correlation-based feature selection approach which improved the performance to a certain extent. RF and DT out performed in terms of specificity. However, SVM gave better accuracy of nearly 77%.

Deo and Panigrahi [11] used NHANES dataset for predicting diabetes by extracting features like: age, ethnicity, gender, BMI, blood pressure, lab cholesterol, nutrition intake, calorie consumption, fitness, smoking, and drinking habits. Moreover, linear SVM and bagged trees were compared giving 88.5% and 87% accuracy. However, after removing outliers and missing values, the dataset was very small which cannot be validated in real-time situations.

Daghistani and Alshammari [12] compared logistic regression (LR) and random forest (RF) on data extracted from MNGHA database which mainly consisted of features derived from lab test. Dataset consist of 66,325 records; however, there were many missing values and attributes with missing values larger than 40% were dropped and rest were replaced by mean or mode. Comparatively RF resulted in better accuracy than LR.

Li et al. [13] analyzes important features of diabetes through data mining. Author used RFE and chi-squared as feature selection technique and experimented the data prediction with a combination of XGboost and linear regression suggesting that linear regression did not significantly contributed in improving the performance. However, combining both did not yield good performance as compared to employing XGboost alone. Also, work shows that efficiently choosing features through different techniques and data preprocessing leads to better accuracy.

Nibareke and Laassiri [14] optimized and compared linear regression, naïve Bayes and decision tree for predicting diabetes. However, accuracy of all algorithms was almost similar, but in terms of score and error, decision tree is a good choice.

Chatrati et al. [15] proposed a smart health monitoring system that utilizes inputs like blood pressure from devices and predicts whether patient is diabetic or not. Author used only two attributes which are blood pressure and glucose for prediction and suggested that main feature for estimating is diastolic blood pressure. Also, SVM gave best accuracy of 75% in proposed framework. Also, author concluded that hypertension is big challenge to healthcare system.

Hasan et al. [16] suggested that preprocessing techniques such as: outlier treatment, feature selection, efficiently handling missing values is an efficient way for achieving good results. Different algorithms were experimented for predicting

diabetes. Combining AdaBoost and XGboost gave good effect on performance. Moreover, ensemble learning reduces error and improves the accuracy of classifiers.

2.2 Deep Learning-Based Techniques

Woldemichael and Menaria [17] recommended the use of data mining algorithms for diabetes mellitus prediction. This applied back propagation (BP) algorithm for predicting the chances of diabetes in a person. To improve the performance of predictive mode, this work applied fivefold cross-validation method and used learning rate of high value. The tests were conducted on PIMA Indian dataset. The BP algorithm used in this work provided accuracy, sensitivity, and specificity of 83.11%, 86.53%, and 76%, respectively, in diabetes prediction.

Mirshahvalad and Zanjani [18] investigated that the ML approaches were utilized as the computer-aided systems for predicting that whether the patient was probably suffered from diabetes or not. There were three diverse publicly available datasets utilized for testing the suggested technique and comparing it with the perceptron algorithm. The outcomes represented that suggested algorithm performed better in comparison with the perceptron algorithm on average AUC basis.

Jahangir et al. [19] implemented computerized multilayer perceptron (Auto MLP) for creating a diabetes prediction model. This approach was united with an outlier detection scheme called enhanced class outlier detection with the aid of distance-based algorithmic approach. This system optimized used parameters mechanically in the course of training without the need of human intervention. This system performed outlier detection in the data preprocessing stage. The devised system reported most appropriate outcomes in terms of accuracy which was counted as 88.7%.

Zhou et al. [20] suggested using deep learning for diabetes prediction. The experiments were performed using deep cognition AI on deep learning studio. The deep learning gave better accuracy on PIMA dataset as compared to state-of-the-art method. However, training this type of model requires good performance hardware when dealing with large datasets.

Thaiyalnayaki [21] suggested use of deep learning perceptron and SVM for diabetes classification. PIMA dataset was utilized for this purpose. Tenfold cross validation was employed giving accuracy of 77.474%. Author concluded that accuracy can be increased by using different fusion of features and advanced neural networks.

3 Discussion

Various machine learning methods have been suggested for predicting diabetes. There are several steps from collecting the data, preprocessing it, selecting optimal features and classifying it at the end. Efficiently cleaning data and handling missing values

could lead to better accuracy. Techniques like SMOTE have been used for handling unbalanced data. There various attributes through which diabetes can be predicted at early stage: BMI, obesity, blurred vision, insulin, blood pressure, etc. Optimally selecting these features for predicting diabetes is also an important task. Principal component analyses or correlation between attributes are mainly used for identifying dependency between features. After that, various classification algorithms are employed for classifying the correct class. Support vector machine, logistic regression, decision trees, K-nearest neighbors are some common algorithms which have been researched for predicting diabetes mellitus. SVM is used by various authors and on different datasets. It can be seen that SVM gives optimal results even when used on different datasets. Therefore, it can be concluded that SVM is a better performer in terms of accuracy and bring generality to the models. However, optimal selection of features that result in better accuracy as well as selecting features which do not require advance lab tests by utilizing different approaches is the way forward. Feature selection techniques are yet to explore in the field of diabetes prediction. Also, there is a need for recent dataset which is large enough to predict diabetes under varied situations. The training time complexity of SVM and RF is $O(n^2)$ and $O(n*\log(n)*d)$, respectively, where n is number of points in training set and d is dimensionality of the data (Table 1).

4 Conclusion

In this work, it is concluded that data mining technology adopts different classification models for diabetes prediction, such as SVM, naïve Bayes, decision tree, KNN, RF, etc. SVM and RF are two methods which are widely used for diabetes prediction. However, SVM generalizes the model since it shows optimal results when applied to different dataset. Time complexity of an algorithm depends on number of training points and dimensionality. The more features, the more complexity; therefore, feature selection is important part to reduce training time. Random forest is an important ensemble learning algorithm based on bagging. It is an ensemble classification model composed of many decision trees. Also, trying ensemble and deep learning approach can result in better accuracy. Accurately predicting of diabetes with early signs attributes and without advanced lab tests is an efficient way for estimating diabetes in early stage. Efficiently selecting and identifying features affecting diabetes and trying unused or different approach classifier to improve accuracy is way forward. Finding optimal combination of various feature selection techniques can be explored further.

Table 1 Comparison table of various studies

Author	Missing values	Class imbalance	Feature selection	Classification technique	Performance	Dataset
[4]	Dropped			Random Forest Support Vector Machine	84.13% 69%	Private
[10]				Naive Bayes K-Nearest Neighbor C4.5	67.50% 70.10% 75.14%	Private
[5]	Means		Correlation	Logistic regression	95.42%	PIMA
[6]			PCA + K-means	Logistic regression	97%	PIMA
[19]				Perceptronf-Boosting	0.72 ADC	NHANES
[14]			Recursive Feature Elimination Chi-squared	XGboost XGboost -i-Logistic Regression	79.60% 77.90%	PIMA
[22]		SMOTE Interquartile Range algorithm	_	C4.5	89.50%	PIMA
			PCA	AdaBoost	94.10%	
[17]	Mean		Independent component analysis Correlation	XGboost	94.60%	PIMA
[13]	Mean and Mode			Random Forest Logistic Regression Support Vector Machine Random Forest	88% 70.30% 77.73% 75.39%	Private: MNGHA
[11]			Correlation	Naive Bayes Decision Tree K-Nearest Neighbor	73.48% 73.18% 63.04%	UC1 diabetes
[18]	Mean		Chi-squared	fiack Propagation J48	83.11% 78.26%	PIMA
[12]	Dropped	SMOTE(under sampling)	Principal Component Analysis	Bagged trees Support Vector Machine	88.43% 90.81%	NHANES
[16]				Ensemble	0.75 AUC	NHANES
[9]	Dropped		Logistic Regression	Random Forest	94.20%	NHANES

References

1. D. Bala Bisandu, et al., *Diabetes Prediction Using Data Mining Techniques* (2019). Accessed: Oct. 21, 2020 (Online). Available: www.rsisinternational.org
2. L.H.S. De Silva, N. Pathirage, T.M.K.K. Jinasena, *Diabetic Prediction System Using Data*

Mining (2016). Accessed: Oct. 21, 2020 (Online). Available: http://ir.kdu.ac.lk/handle/345/1250
3. P.B. Patel, P.P. Shah, H.D. Patel, *Analyze Data Mining Algorithms for Prediction of Diabetes*, © 2017 IJEDR, vol. 5, 2017, Accessed: Oct. 21, 2020 (Online). Available: www.ijedr.org
4. W. Xu, J. Zhang, Q. Zhang, X. Wei, Risk prediction of type II diabetes based on random forest model, in *Proceedings of the 3rd IEEE International Conference on Advances in Electrical and Electronics, Information, Communication and Bio-Informatics, AEEICB 2017*, Jul. 2017, pp. 382–386. https://doi.org/10.1109/AEEICB.2017.7972337
5. C. Zhu, C.U. Idemudia, W. Feng, Improved logistic regression model for diabetes prediction by integrating PCA and K-means techniques. Informatics Med. Unlocked **17**, 100179 (2019). https://doi.org/10.1016/j.imu.2019.100179
6. R. Syed, R.K. Gupta, N. Pathik, An advance tree adaptive data classification for the diabetes disease prediction, in *2018 International Conference on Recent Innovations in Electrical, Electronics and Communication Engineering, ICRIEECE 2018*, Jul. 2018, pp. 1793–1798. https://doi.org/10.1109/ICRIEECE44171.2018.9009180
7. A. Husain, M.H. Khan, Early diabetes prediction using voting based ensemble learning. Commun. Comput. Information Sci. **905**, 95–103 (2018). https://doi.org/10.1007/978-981-13-1810-8_10
8. M. Maniruzzaman, M.J. Rahman, B. Ahammed, M.M. Abedin, Classification and prediction of diabetes disease using machine learning paradigm. Heal. Inf. Sci. Syst. **8**(1), 1–14 (2020). https://doi.org/10.1007/s13755-019-0095-z
9. K.L. Priya, M.S. Charan Reddy Kypa, M.M. Sudhan Reddy, G.R. Mohan Reddy, A novel approach to predict diabetes by using Naive Bayes classifier, in *Proceedings of the 4th International Conference on Trends in Electronics and Informatics, ICOEI 2020*, Jun. 2020, pp. 603–607. https://doi.org/10.1109/ICOEI48184.2020.9142959
10. N. Sneha, T. Gangil, Analysis of diabetes mellitus for early prediction using optimal features selection. J. Big Data **6**(1), 13 (2019). https://doi.org/10.1186/s40537-019-0175-6
11. R. Deo, S. Panigrahi, Performance assessment of machine learning based models for diabetes prediction, in *2019 IEEE Healthcare Innovations and Point of Care Technologies, HI-POCT 2019*, Nov. 2019, pp. 147–150. https://doi.org/10.1109/HI-POCT45284.2019.8962811
12. T. Daghistani, R. Alshammari, Comparison of statistical logistic regression and randomforest machine learning techniques in predicting diabetes. J. Adv. Inf. Technol. **11**(2), 78–83 (2020). https://doi.org/10.12720/jait.11.2.78-83
13. M. Li, X. Fu, D. Li, Diabetes prediction based on XGBoost algorithm, in *IOP Conference Series: Materials Science and Engineering*, Mar. 2020, vol. 768, no. 7, p. 072093. https://doi.org/10.1088/1757-899X/768/7/072093
14. T. Nibareke, J. Laassiri, Using Big Data-machine learning models for diabetes prediction and flight delays analytics. J. Big Data **7**(1), 78 (2020). https://doi.org/10.1186/s40537-020-00355-0
15. S.P. Chatrati, et al., Smart home health monitoring system for predicting type 2 diabetes and hypertension. J. King Saud Univ. - Comput. Inf. Sci. (2020) https://doi.org/10.1016/j.jksuci.2020.01.010
16. M.K. Hasan, M.A. Alam, D. Das, E. Hossain, M. Hasan, Diabetes prediction using ensembling of different machine learning classifiers. IEEE Access **8**, 76516–76531 (2020). https://doi.org/10.1109/ACCESS.2020.2989857
17. F.G. Woldemichael, S. Menaria, Prediction of diabetes using data mining techniques, in *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018*, Nov. 2018, pp. 414–418. https://doi.org/10.1109/ICOEI.2018.8553959
18. R. Mirshahvalad, N.A. Zanjani, Diabetes prediction using ensemble perceptron algorithm, in *Proceedings - 9th International Conference on Computational Intelligence and Communication Networks, CICN 2017*, Mar. 2018, vol. 2018-January, pp. 190–194. https://doi.org/10.1109/CICN.2017.8319383
19. M. Jahangir, H. Afzal, M. Ahmed, K. Khurshid, R. Nawaz, An expert system for diabetes prediction using auto tuned multi-layer perceptron, in *2017 Intelligent Systems Conference,*

IntelliSys 2017, Mar. 2018, vol. 2018-January, pp. 722–728. https://doi.org/10.1109/IntelliSys.2017.8324209
20. H. Zhou, R. Myrzashova, R. Zheng, Diabetes prediction model based on an enhanced deep neural network. Eurasip J. Wirel. Commun. Netw. **2020**(1), 148 (2020). https://doi.org/10.1186/s13638-020-01765-7
21. K. Thaiyalnayaki, O. Research, Classification of diabetes using deep learning and SVM techniques the dataset of 768 samples are from Pima Diabetes, National Institute of Diabetes and Digestive and Kidney Diseases. Int. J. Cur. Res. Rev. **13** (2021). https://doi.org/10.31782/IJCRR.2021.13127
22. N. Nnamoko, I. Korkontzelos, Efficient treatment of outliers and class imbalance for diabetes prediction. Artif. Intell. Med. **104**, 101815 (2020)

Analysis of Marketing Mix and Website Performance on E-marketplace of Agricultural Products



Reni Diah Kusumawati, Teddy Oswari, Tristyanti Yusnitasari, and Himanshu Dutt

Abstract The pandemic period is an opportunity and threat to be able to meet national food needs. Restrictions on outdoor activities change consumer behavior in meeting their daily food needs, like food purchases that were done at brick and mortar saw a shift to online. Technological developments support the fulfillment of food needs with the availability of an e-marketplace offering a variety of agricultural products. This study discusses consumer purchase decisions on e-marketplaces for agricultural food products. Population in this study is consumers who have used e-marketplace to purchase agricultural products. The results showed that the elements of marketing mix and e-marketplace performance simultaneously effect on consumer purchasing decisions. Collectively, this impact is 43.6% meaning that marketing mix and e-marketplace Web site hold high impact on purchase decisions of agricultural products. Additionally, by the use of e-marketplaces by paying attention to the element of marketing mix, farmers can cut the length of distribution chain, thereby increasing their income.

Keywords Agricultural products · E-marketplace · Marketing mix · Purchase decision · Web sites performance

R. D. Kusumawati (✉) · T. Oswari · T. Yusnitasari
Gunadarma University, Jakarta, Indonesia
e-mail: reni_dk@staff.gunadarma.ac.id

T. Oswari
e-mail: toswari@staff.gunadarma.ac.id

T. Yusnitasari
e-mail: tyusnita@staff.gunadarma.ac.id

H. Dutt
Visiting Faculty, Jamia Millia Islamia (Central University), New Delhi, India
e-mail: himanshudutt@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_42

1 Introduction

Long distribution chain from farmers to consumers for selling their agricultural products results in significant price differences due to middleman involved. This chain involves farmers, small traders, wholesalers, main markets, brokers, traditional markets, and vegetable traders. This happens not only in Indonesia but also in several other developing countries. Another problem faced by farmers is the difficulty of promoting agricultural products and attracting consumers to make purchases directly from farmers [9].

The pandemic started in early 2020 severely affected the economic growth across the World. This decline however did not occur significantly in the agricultural sector compared to manufacturing and services. This is because people have consumption needs from the agricultural sector, especially well-habituated countries like Indonesia and India, where agriculture consumption is comparatively high. The agricultural sector contributes 15.46% to the gross domestic product (GDP) and is the second largest sector in contributing after the information and communication sector in Indonesia. Almost similar contribution is India's agricultural sector contribution to its GDP. The pandemic saw this consumption only going up as people piled up stocks due to lockdown restrictions. The policies implemented by the government during the pandemic period had put restrictions on operating hours for shops and the movement of the people. This has resulted in changes in the consumer behavior forcing both—shops and consumers—to shift to online or the e-marketplace.

Changes in consumer behavior along with technological developments force farmers to adopt innovation in farming and use of technology to process. For consumers, changes in behavior are marked by the rise of e-marketplaces that is seen as convenient and time-saving choice to meet their daily needs [13, 14]. This shift is causing agriproduct sellers to use digital platforms as a solution to target more consumers directly and maximize their income. The rapid growth of the e-marketplace along with the growth in the number of Internet users comes as a great opportunity to agriculturists to reach out to more consumers.

Using the e-marketplace properly by paying attention to the elements of the marketing mix will help the agricultural sector to reach a wider market share. E-marketplaces can cut distribution chains that are too long, so that prices for agricultural products do not experience significant changes from farmers to consumers. E-marketplaces provide benefits for consumers where agricultural products can reach consumers directly without going through long distribution channels, besides that e-marketplaces also provide benefits for farmers where agricultural products can be widely known by consumers, so that the number of buyers will increase and result in increase in farmer income.

The growth in the number of Internet users in the world continues to grow every year. This growth also occurs in Indonesia, so that it can provide great opportunities for business actors, especially in the agricultural sector, to be able to promote agricultural products to consumers. Utilization of the Internet is expected to cut the length of the trade chain for agricultural products. The methods of marketing agricultural

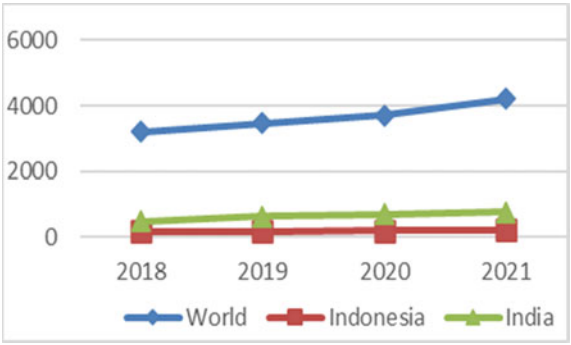


Fig. 1 Internet user growth

products that have been successfully carried out in India can also be adopted to be applied in Indonesia, due to the characteristics of Indonesia which are almost similar to India, where the agricultural sector makes a large contribution to the country. The growth of Internet users is presented in Fig. 1.

2 Literature Review

The development of information and communication technology followed by the growth in the number of Internet users around the world can assist business actors, especially farmers in introducing their products to consumers without being limited by distance and time, so that buyers of agricultural products do not only come from locally but also nationally or internationally [10]. It is very important for business actors to pay attention to things that can attract consumers to buy the products offered. Understanding business actors toward consumer behavior is a major concern because this will greatly help business actors in understanding how consumers think and then choosing products, and brands they like from the various alternatives offered [11]. Consumer decisions in buying product are typically influenced by environmental, social, cultural, personal, and psychological factors [6].

Marketing mix elements need to be considered by business actors to influence consumer behavior in deciding to make purchases, so that the company can compete with its competitors. Matter of concern to these business actors can be in the form of determining prices that are in accordance with good product quality, attractive promotions, choosing the right distribution channels so that products can reach consumers in their intact condition, good service, ease of transactions, and convenience. These factors are major considerations for consumers in determining whether to purchase or not [2, 7].

Digital has changed consumer behavior landscape, which was previously done conventionally, now many consumers purchase products by online [5]. The appearance of e-commerce Web sites is important for business actors to be able to attract consumers to visit and make purchases [12]. Using Web sites to market agricultural

products may still be difficult for small farmers but using Web sites already available can garner benefits, because today's consumers have made a lot of purchases online [8]. It is important for business actors to pay attention to the appearance of a Web site that is attractive to consumers so that consumers are interested in visiting the Web site and making purchases.

The completeness of the e-marketplace Web site like availability of frequently asked questions (FAQ) facilities, complete information about the various products available on the Web site, and ease in finding the products that consumers desire holds the key for attracting consumers and purchases on the Web site. In addition, consumers will like Web sites that provide speed in accessing, updates on product availability, and speed of response given to consumers when consumers ask questions or raise complaints [1, 9].

The use of e-marketplaces in the agricultural sector provides many benefits, such as time savings, reduced costs, and a wider reach [3]. E-marketplaces help facilitate consumers to search for products, order products, pay for it using modes of transactions with security, and get secure product delivery [4]. The e-marketplace for agricultural products aims to develop an innovative online market concept in line with changes in consumer behavior, so that it can offer a shorter path so that products can reach consumers faster at relatively cheaper prices [3].

3 Research Method

This research is a quantitative descriptive study that uses survey method. Data is collected through questionnaire method. Survey items on questionnaire represented consumer perceptions about the marketing mix variables and impact of performance of e-marketplaces on the purchasing decisions for agricultural products sold through e-marketplaces. The population in this study is consumers who have purchased agricultural products through the e-marketplace, selected using random sampling techniques. The questionnaire in this study was made using Google Forms and then distributed online to the respondents.

The questionnaire is divided into two parts: the first part contained demographic information about consumers and the second part contained consumer statements related to the research variables. Likert-type scale is used to measure the perceptions, opinions, and attitudes of research respondents toward the phenomenon being studied [15], and the rating scale ranged between 1 and 5.

4 Result and Discussion

The hypothesis taken was whether there is any effect of marketing mix variables and the performance of the e-marketplace Web site on the agricultural product purchase decisions for consumers. If yes, to what extent then?

Table 1 Simultaneous test result

ANOVA[a]						
Model		Sum of squares	df	Mean square	*F*	Sig
1	Regression	356.35	10	35.635	6.886	0.000[b]
	Residual	460.56	89	5.175		
	Total	816.91	99			

[a]Dependent variable: Purchase decision
[b]Predictors: (constant), Web site convenience, product, Web site feature, process, Web site content, promotion, people, price, place, physical evidence

Simultaneous test results (F test) for marketing mix variables (product, price, promotion, distribution, service, physical evidence, process), e-marketplace Web site performance (Web site features, Web site content, Web site convenience), and decisions purchase of agricultural products on the e-marketplace as presented in Table 1.

Table 1 shows that the sig. *F* is less than 0.05, which indicates that simultaneously the marketing mix variables (product, price, promotion, distribution, service, physical evidence, process) and the performance of the e-marketplace Web site (Web site features, Web site content, Web site convenience) affect the purchasing decisions of agricultural products in the e-marketplace.

Partial test results for marketing mix variables (product, price, promotion, distribution, service, physical evidence, process) and e-marketplace Web site performance (Web site features, Web site content, Web site convenience) on agricultural product purchasing decisions on e-marketplace are presented in Table 2.

If the significance value is smaller than the alpha (α) value 0.05, it can be said that the variables have effect on the decision to purchase agricultural products on the e-marketplace Web sites. Therefore, only promotion and physical evidence have an effect on purchasing decisions for agricultural products, while product, prices, distribution, services, processes, Web site features, Web site content, and Web site convenience have no effect on the purchasing decisions.

This indicates that the promotion and evidence of existence of an e-marketplace are most important requirement for consumers to make purchase decision.

The results showed that product variables had no effect on purchasing decisions for agricultural products in the e-marketplace. This may happen because most agricultural products do not have high product differentiation, so consumers are well aware of the product they want. On pricing, the consumers seem not to be focused much. This may be because customer do not find much variance in pricing and out of his loyalty to a particular e-marketplace Web site.

Same with the distribution since all e-marketplace offer home delivery and expected to send product fresh so it does not affect the purchase decision. Besides all e-marketplaces provide almost the same services such as facilities for communicating with sellers, availability of information about products being sold, and availability of shipping services, so no strong differentiation here as well. Process do not have

Table 2 Partial test result

Coefficients[a]						
Model		Unstandardized coefficients		Standardized coefficients	*t*	Sig
		B	Std. error	Beta		
1	(Constant)	8.297	3.435		2.415	0.018
	Product	−0.256	0.138	−0.219	−1.857	0.067
	Price	−0.215	0.167	−0.169	−1.282	0.203
	Promotion	0.514	0.178	0.381	2.885	0.005
	Place	0.176	0.184	0.130	0.959	0.340
	People	0.036	0.199	0.026	0.183	0.856
	Physical evidence	0.697	0.193	0.529	3.615	0.000
	Process	−0.150	0.177	−0.112	−0.848	0.399
	Web site feature	−0.238	0.178	−0.118	−1.337	0.185
	Web site content	0.287	0.203	0.142	1.416	0.160
	Web site convenience	−0.174	0.215	−0.086	−0.809	0.421

[a]Dependent variable: Purchase decision

because consumers believe that each e-marketplace provides an easy process for consumers in terms of user experience and number of screens from product listing to checking out.

It is also found that consumers do not get influenced by the features, content, and convenience of the e-marketplace. It is so because each e-marketplace is promoting to attract its consumers to buy. However, the ease of finding information about products and ease of transacting definitely provide benefits for the e-marketplace [4].

Table 3 quantifies the effect of marketing mix, e-marketplace Web site performance, and agricultural product purchasing decisions on e-marketplaces.

The *R* square value of 0.436 shows the contribution of the marketing mix variable (product, price, promotion, distribution, service, physical evidence, process), the

Table 3 Coefficient of determination

Model summary[b]				
Model	R	R square	Adjusted R square	Std. error of the estimate
1	0.660[a]	0.436	0.373	2.275

[a]Predictors: (constant), Web site convenience, product, Web site feature, process, Web site content, promotion, people, price, place, physical evidence
[b]Dependent variable: Purchase decision

performance of the e-marketplace Web site (Web site features, Web site content, Web site convenience) on purchasing decisions for agricultural products in the e-marketplace is as much as 43.6% while the rest is influenced by other variables not included in this research model.

5 Conclusion

Results show marketing mix (promotion, physical evidence) had an effect on purchasing decisions for agricultural products on the e-marketplace whereas the performance of the e-marketplace Web site (Web site features, Web site content, Web site convenience) had no effect on product purchase decisions. Contribution of marketing mix variables (product, price, promotion, distribution, service, physical evidence, process) and e-marketplace Web site performance (Web site features, Web site content, Web site convenience) to purchase decisions is 43.6%, while the rest is influenced by other variables not included in the model. The results of this study are expected in the future to provide an overview for consumers who want to purchase agricultural products, and things that need to be considered so as not to harm consumers in purchasing agricultural products on the e-marketplace. The use of e-marketplaces as a form of technological development in marketing agricultural products will cut the length of the distribution chain, so that products can reach consumers quickly, and farmers' income can increase.

Managerial Implications

This research will be useful for farmers and new entrepreneurs involved in selling agricultural products through e-marketplaces. This study will also provide information to the agricultural sector to understand the internal and external factors that make consumers decide to buy agricultural products. The results of this study will help consumers to appreciate farmers who have helped meet food needs with agricultural products. For academics, the results of this study will help to understand the theory of consumer behavior applied to agribusiness in relation to the marketing mix and the performance of the e-marketplace Web site.

Research Limitations

The objects used in this study are still very small when compared to consumers who consume agricultural products in Indonesia. The data will be more representative if more respondents are used as samples in this study. The topic of consumer perceptions tends to involve consumers' emotions; therefore, the data obtained can be biased in revealing the real thoughts of respondents. However, this does not mean that the data used in this study are invalid, because in some cases it is not possible to be perfect in obtaining data.

Research Development Plan

In further research, the researcher wants to add other factors such as convenience, trust, experience, actual use, loyalty that will influence consumer behavior of agricultural products. Thus, researchers hope to improve the research and make it more objective and comprehensive.

Acknowledgements The authors would like to thank to Gunadarma University for all the support in this research. To Ristekdikti who has provided research grants. To friends and colleagues for input and support, to agricultural industry for their time in giving information related to this study. To respondents for fulfill the questionnaire used in this research.

References

1. E.P. Becerra, V. Badrinarayanan, C.H. Kim, Influence of thinking tendencies on online transaction of hybrid retailers. J. Bus. Res. **66**(3), 336–344 (2013)
2. A. Dodor, exploring marketing mix for building a viable agro business. Br. J. Educ. Soc. Behav. Sci. **6**(2), 78–86 (2015)
3. S.E.K. Gally, L. Fenyvesi, A new agricultural electronic marketplace, the way forward for the procurement of inputs. EAAE Congress **2014**, 1–6 (2014)
4. J. Juswadi, P. Sumarna, N.S. Mulyati, Digital marketing strategy of Indonesian agricultural products, in *International Conference on Agriculture, Social Sciences, Education, Technology and Health (ICCASETH 2019)*, vol. 429 (2019), pp. 105–110
5. Kominers, S. Duke, A. Teytelboym, V.P. Crawford, An invitation to market design. Oxford Rev. Econ. Policy **33**(4), 541–571 (2017). https://doi.org/10.1093/oxrep/grx063
6. Kotler, P. dan Gary Armstrong. *Principles of Marketing*, 12th Edn., Prentice Hall, Inc. A Pearson Education Company, Upper Saddle River, New Jersey (2016)
7. R.D. Kusumawati, T. Oswari, T. Yusnitasari, H. Dutt, analysis of marketing mix strategies for sales of agricultural products on e-marketplace in indonesia. Int. J. Econ. Manage. Stud. **8**(2), 118–112 (2021)
8. N. Newman, L.F. Bergquist, N. Immorlica, K.L. Brown, B. Lucier, C. McIntosh, Designing and involving an electronic agricultural marketplace in Uganda, in *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*, Article No. 14 (2018), pp. 1–11
9. H. Nugroho, R. Hendriyanto, K. Tisamawi, Application for marketplace agricultural product. Int. J. Appl. Information Technol. **2**(2), 58–67 (2018)
10. Pujianto, S. Novari, Marketplace dan e-commerce bagi petani guna peningkatan penjualan hasil pertanian. Seminar Nasional Teknologi Informasi, Bisnis, dan Desain (2016)
11. R. Ariyani, T. Yusnitasari, T. Oswari, R.D. Kusumawati, S. Mittal, Consumer Behaviour analysis in online music purchases in Indonesia by implementing 7p's marketing strategy using quality function deployment (QFD). Am. J. Eng. Technol. Manage. **4**(3), 57–65 (2019)
12. R.H. Wuisan, Analisis penggunaan e-commerce agribisnis pada pemasaran bawang merah dan cabai merah (studi kasus platform e-commerce sikumis dan limakilo). Thesis. Institut Pertanian Bogor, Indonesia (2017)
13. S. Shahriari, M. Shahriari, S. Gheiji, e-marketplace and it impacts on global trend and market. Int. J. Res. Granthaalayah **3**(4), 49–55 (2015)
14. R. Shahjee, the impact of electronic commerce on business organization. Scholarly Res. J. Interdiciplinary Stud. **4**(27), 3130–3140 (2016)
15. Sugiyono, Metode Penelitian Evaluasi (Pendekatan Kuantitatif, Kualitatif dan Kombinasi). Bandung, Alfabeta (2018)

A Machine Learning Approach for Gait Based Human Authentication in Smart Cities



Arindam Singh and Rajendra Kumar Dwivedi

Abstract Internet of things (IoT) is helping us to develop smart cities. Smart cities need security. Human authentication through surveillance is one of the important issues. Several machine learning algorithms can be used to identify a person on basis of their movements and gestures. In this paper, we devised a supervised machine learning technique for the classification of images. We tested our method on the CASIA-B data set which is available in the public domain. It consists of 124 subjects. We found our method outperforming the existing schemes, viz support vector machine (SVM), k-nearest neighbor (kNN), neural network (NN), convolutional neural network (CNN), fuzzy set theory and discrete Fourier transform.

Keywords Human authentication · Gait recognition system · Machine learning · Deep learning · Supervised learning · Unsupervised learning

1 Introduction

As can be seen in today's world of rising security demands in response to rising crime trends, science analysis on human identity has been widely applied to security and safety issues. Since humans have brains, they can quickly recognize an individual based on their movements. Is the computer capable of performing this mission as well? Yes, in this smart age, we have a variety of strategies for teaching machines to perform a variety of tasks. Biometric technology, which is dependent on human estimates, can identify individuals from afar even though their faces are obscured, covered, not apparent, or not noticeable to cameras in low-light situations Biological characteristics, called biometrics, are measured and analyzed to determine a person's identity. A biometric is a particular dividing factor used for identification. To date, culture seems to be ruled by identification schemes that use one or more of these biometrics [1, 2]. The first published guide for analyzing the way of awakening was made by Aristotle (384–322 BCE). He came from Athens, Greece, and he presented several hypotheses on human and animal movement [3]. Eduard and

A. Singh (✉) · R. K. Dwivedi
Department of IT and CA, MMMUT, Gorakhpur, Uttar Pradesh, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_43

Willhelm collaborated on many works, including the 1836 publication of Mechanik der Gehwerkzeuge (Mechanics of the Human Walking Apparatus) [4]. Otto Fischer (1861–1917), a German mathematician, was the first to do a three-dimensional gait analysis. Professor of Anatomy Willhelm Braune (1831–1892), with whom he had previously worked in measuring the inertial dimensions of the human body, will remain synonymous with his name. Engineer Larry Lamoreux used goniometers to measure three-dimensional hip joint kinematics as well as one-dimensional knee and ankle angles on a metal exoskeletal frame [3]. Fortunately, this was the beginning of the computer revolution, which made for ever-faster data processing and ever-greater output opportunities [3].

2 Literature Review

Human mobility was first researched in the medical sector [5, 6] when physicians looked at how people walked to see if they had any health issues. So someone assumes that a person's gait should be used as a natural feature to identify them. In this part, we looked at a few different methods for distinguishing people based on their movements. The following are some of the studies:

Song [7] suggested GaitNet, a method based on two convolutional neural networks, one for gait segmentation and the other for classification. With a single frame, the model of human silhouette release and gait recognition was developed, and they were trained end-to-end. For defining a human being by partial gait loop, Babaee [8] used a completely convolutional neural network (deep learning). Chantapakul [9] discusses how to use 3 Kinects and String Grammar Fuzzy-Possibilistic C-Medians to classify people. Kinects are recording both sides view as well as front view and a person take a walk-in 3.35 m defined path. Batchuluun [10] suggested a method for identifying people by using thermal cameras to capture the front and back photos of the object. Body activity is used to identify the object, and a convolutional neural network is used to isolate the attribute and classify it. Sharma [11] describes new gait energy image-based feature called a sigmoid feature (GII-BPSF). This method makes use of fuzzy set theory and the image-sigmoid function of gait knowledge. Deng [12] describes a new approach for human recognition called gait dynamics graph (GDG). For human identity, Wang [13] suggested a method based on an Acoustic sensor system and a deep neural network.

Bhargavas [14] creates a project that uses the Kinect sensor and the SVM algorithm to identify an individual. The skeleton signal, which is a color image with skeleton points, is extracted by the Kinect sensor. For human recognition, Bajwa [15] used a support vector machine algorithm with K-nearest neighbors (KNN) and neural network (NN). Dubois [16] developed the method which uses depth images and gait sequence for the identification of human beings. The Hidden Markov Models (HMMs) are used for detecting gait sequence that is recognizing the activity performed by persons. Chen [17] identifies a human identity approach focused on silhouette correlation analysis. The image series is used for background modeling

and image subtraction, and then the binary silhouette image is used for image correlation. For human identity, Munsell [18] proposed a new approach based on motion and anthropometric biometrics. The Kinect sensors generate depth images that can be used to identify people. From Kinect recordings, the motion classifier may distinguish running and walking action. Sudha [19] describes a new hybrid holistic approach for detecting unwanted people in monitoring areas. The process is divided into two phases: preparation and testing. In the training phase, context modeling and foreground extraction are used to produce binary silhouettes, which are then used to remove features.

Major findings of the survey

Table 1 presents a comparative study of the existing schemes. According to our study, numerous machine learning algorithms have varying degrees of success in distinguishing humans. As we can see from this survey, approaches that use neural networks for detection have higher precision than those that do not.

3 Proposed Work

Human identification can be done variously and gives a different accuracy of identification. Our method is having two phases of training and testing. The training and testing phases have comprised of the steps as shown in Fig. 2.

Our method includes several steps as shown in Fig. 1. These steps are explained as below:

- Input videos or images are taken from video cameras located at different locations.
- Preprocessing steps are shown in algorithm 1. Here Gaussian blur function is widely used for reducing the image noise. It provides more clarity to the images that give the smooth image for the segmentation process.
- Reducing features using principal component—It helps to make our method more efficient by decreasing the computational time and by achieving high accuracy. PCA is used to transform multidimensional datasets into 2-dimensional and 3-dimensional. The working of PCA is shown in algorithm 2.
- Feature Extraction is a technique for reducing the number of features in a dataset by creating new ones from existing ones (and then discarding the old features). step-size, dimension of a human silhouette, angle Joints are the features we extracted from the silhouette images.
  - Measurements of height and width are taken as the length and width of the silhouette. And then, to produce the most important and elegant skeleton function points, we converge and simplify essential points [21] algorithm 3 is showing the whole skeletonization process.
  - After the skeletonization of the body, we apply Houge transform [20] on the skeleton for extracting the joint angle. Head, Neck, Torso, Right hip and Thigh, Left hip and Thigh, Lower Right Leg, Lower Left Leg body parts we extract

Table 1 Comparative study of learning-based identification techniques

Approach	Techniques	Authors	Year	Limitations	Findings
Single	SVM	Bhargavas [14]	2017	Small dataset	93% recognition rate
		Sudha [19]	2011	The study is limited to side view	Identification rate 97.91
	KNN	Chantapakul [9]	2018	Less subject and accuracy	73.33% accuracy
	CNN	Babaee [8]	2019	Limited to side view	Accuracy 96.1%
		Son g[7]	2019	Accuracy can be improve	78% accuracy
		Batchuluun [10]	2018	Study limited to front and back view	97.4% classification rate
	Hidden Markov Models	Dubois [16]	2015	Works for indoor	75% accuracy
	Discrete Fourier transform	Chen [17]	2014	Area of a correlated image only	90% of accuracy
	Fuzzy set theory	Sharma [11]	2018	The result can be improve	Identification rate 93.21%
Hybrid	Classifiers	Munsell [18]	2012	Low recognition rate	Identification rate 90%
	Acoustic sensor system and DNN	Wang [13]	2017	Distance Limit in capturing the subject	97% Accuracy
	SVM with KNN and NN	Bajwa [15]	2016	Complex because of more than one classification technique	98.7% accuracy
	Nonlinear dynamics analysis approach and the direct matching method	Deng [12]	2018	Limited view	Average accuracy is around 95%, 99%, (A-90%, B-91%), (A-89%, B-89%), (A-98% B-99%), respectively

from the skeleton. The development of a joint angle from the most likely straight line detected using the Hough transform, where is the joint angle determined using: $90 + \theta = \varnothing$

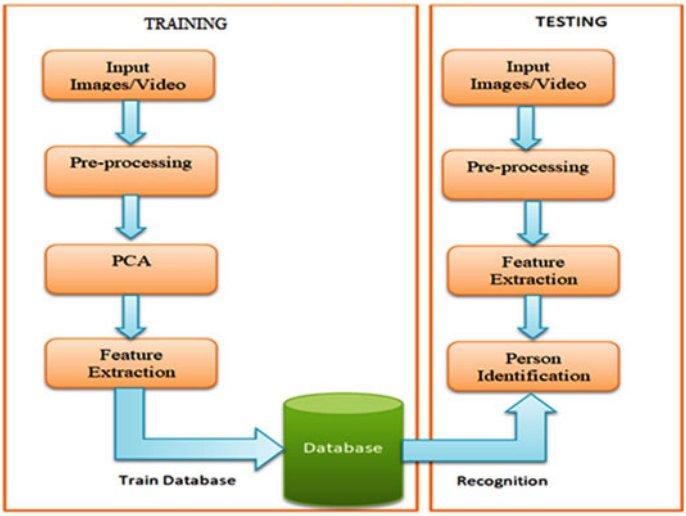


Fig. 1 Proposed approach

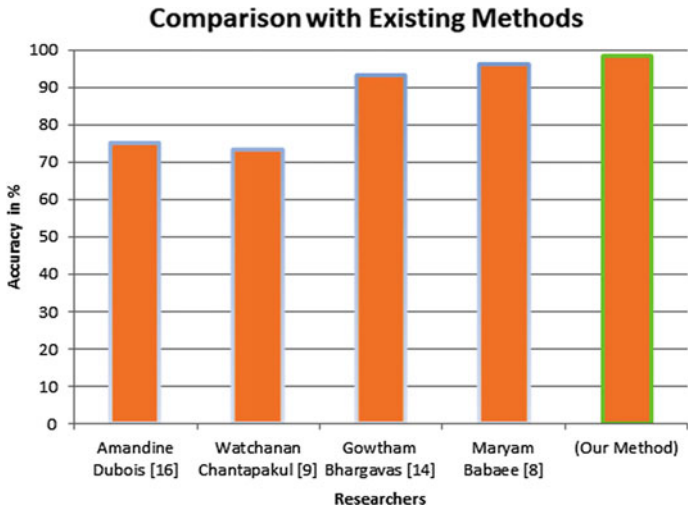


Fig. 2 Comparison of accuracy of the proposed method with the existing schemes

- Classification is done by using SVM (Support Vector Machine) is a supervised machine learning algorithm that can be used to solve classification and regression problems.

There are three algorithms in our proposed scheme. Algorithm 1 is for preprocessing, Algorithm 2 is for reducing features with principal component analysis, and Algorithm 3 is for skeletonization. These algorithms are presented as below:

Algorithm 1: Pre-Processing

Input: Gait cycle frames
Output: Silhouette Extraction
Begin
1. Resize the frames into in specific size
2. Remove the noise from the frame by applying the Gaussian blur function
3. Apply segmentation on the image
    a. Extract the foreground
    b. Remove the background
4. Generate Silhouette of each frame

End

Algorithm 1 is devised for preprocessing in which we resize the frames, remove the noise and apply segmentation on the images.

Algorithm 2: Reducing Features with Principle Component Analysis

Input: Original Features
Output: Reduced Features
Begin
1. Standardisation of data
    a. $z = \frac{value - mean}{standard\ Deviation}$
2. Compute convergence matrix
3. Find out Eigenvalues and Eigenvector of convergence matrix
4. Place Eigenvalues in descending order
5. Select x eigenvector having greatest eigenvalue
    a. Where x < number of features
6. Construct the matrix z from the x selected Eigenvectors
    a. The final dataset has only x-dimensions.
7. $Final\ dataset = FeatureVector^T * Standardized\ orignal\ dataset^T$

End

Algorithm 2 deals with the reduction of features using the principle component analysis method.

Algorithm 3: Skeletonization

Input: Silhouette image

Output: Estimation of joint position

Begin

1. Finding out the gradient distance transform
   a. $|\nabla DT| = \sqrt{(\frac{\partial DT}{\partial x})^2 + (\frac{\partial DT}{\partial y})^2}$
2. Extract the local maximum point and critical point
   a. For calculating LMP: $DT(p) \geq DT(q)$ for $\forall q \in Q$
      i. Where Q is a set of 8 connected neighbor of p
      ii. p is a local maximum point
   b. For calculating Critical point
      i. CP = LMP(∇DT) is a min of its connected neighbor
3. Skeleton feature point detection
   a. Feature point of Skelton connection
   b. Joints estimation
      i. (Head, Neck, Sholders, Elbow, Wrist, Waist, Knee, Ankle)

End

Algorithm 3 is used for skeletonization which provides estimated joint positions of the silhouette image.

4 Results and Discussions

The software used for the implementation is Anaconda Spyder 3.3.6. It provides a python development environment. The proposed approach is implemented on dataset CASIA-B available in the public domain. We used this dataset for testing our proposed scheme.

An N x N matrix is used to evaluate the accuracy of a classification model, where N is the number of target groups. This matrix is known as the confusion matrix. Dataset is divided into training and testing sets. 88 subjects are used for training and 36 is left for testing where we found that 87 subject out 88 is predicted correct and 1 predicted wrong while out of 36, one is wrongly predicted that was not available in the database as shown in Table 2.

We used accuracy as the performance metric to evaluate our scheme with the existing schemes. We have tested this method on CASIA-B which is having 124 subjects where we got an accuracy of 98.38%. The formula of accuracy is given below:

Table 2 Outcomes

TP	FP
87	1
FN	TN
1	35

$$\text{Accuracy} = (\text{TP} + \text{TN})/(\text{TP} + \text{FP} + \text{TN} + \text{FN})$$

Our method is compared with some of the existing methods which are using a single method for classification. It is shown in Fig. 2. Here, we found that our method gives 98.38% accuracy that is the best of all.

5 Conclusion and Future Scope

This paper shows the studies on different machine learning algorithms such as SVM, kNN, CNN, NN, fuzzy set theory and discrete Fourier transform that are used for human detection from their movements. The method that we proposed is an efficient method that outperforms the existing schemes in terms of accuracy. The accuracy of our scheme is observed as 98.38%. This method is easy to implement in smart cities for authenticating the person in a particular area. The limitation of this system the gait of the person should be visible by the camera so that it gives clear gait frames. We implemented our scheme in python on dataset CASIA-B available in the public domain. In the future, we can test our scheme for various other datasets on various performance metrics.

References

1. L. Hong, A. Jain, Integrating faces and fingerprints for personal identification. IEEE Trans. Pattern Anal. Mach. Intell. **20**, 1295–1307 (1998)
2. K. Chang, K. Bowyer, S. Sarkar, B. Victor, Comparison and combination of ear and face images in appearance-based biometrics. IEEE Trans. Pattern Anal. Mach. Intell. **25**, 1160–1165 (2003)
3. R. Baker, *The History of Gait Analysis Before the Advent of Modern Computers.* Elsevier Gait & Posture, vol. 26, issue 3, September, pp.331–342 (2007)
4. W. Weber, E. Weber, *Mechanics of the Human Walking Apparatus.* Translated by Maquet P, Furlong R. Springer, Berlin (1991)
5. A.K. Jain, R. Bolle, S. Pankanti, *Biometrics: Personal Identification in Networked Society.* Kluwer Academic Publishers (1999)
6. D.J. Blanke, P.A. Hageman, Comparison of gait of young men and elderly men. Phys. Ther. **69**(2), 144–148 (1989)
7. C. Songa, Y. Huanga, Y. Huanga, N. Jia, L. Wang, *GaitNet: An End-to-End Network for Gait Based Human Identification.* Elsevier, Pattern Recognition 96 (2019)
8. M. Babaee, L. Li, G. Rigoll, Person identification from partial gait cycle using fully convolutional neural network. Neurocomputing (2019)

9. W. Chantapakul, S. Auephanwiriyakul, N. Theera-Umpon, N. Khunlertgit, Person Identification from Full-Body Movement Using String Grammar Fuzzy-Possibilistic C-Medians. IEEE Conference, ICCSCE (2018)
10. G. Batchuluun, R. Ali Naqvi, W. Kim, K.R. Park, Body-movement-based human identification using convolutional neural network, in *Expert Systems With Applications* (2018)
11. H. Sharma, J. Grover, Human identification based on gait recognition for multiple view angles. Springer Int. J. Intelligent Robot. Appl. (2018)
12. M. Denga, C. Wang, T. Zheng, Individual identification using a gait dynamics graph. Pattern Recogn. **83**, 287–298 (2018)
13. Y. Wang, Y. Chen, M.Z.A. Bhuiyan, Y. Han, S. Zhao, J. Li, Gait-based Human identification using acoustic sensor and deep neural network. Future Generation Comput. Syst. (2017)
14. M. Gowtham Bhargavas, K. Harshavardhan, G.C. Mohan, A. Nikhil Sharma, C. Prathap, Human identification using gait recognition, in *IEEE International Conference on Communication and Signal Processing* (2017), pp. 1510–1513
15. T.K. Bajwa, S. Garg, K. Saurabh, GAIT analysis for identification by using SVM with K-NN and NN techniques, in *IEEE, Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (2016)
16. A. Dubois, J.-P. Bresciani, Person identification from gait analysis with a depth camera at home, in *37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* (2015)
17. J. Chen, Gait correlation analysis based human identification. Sci. World J. **168275**, 8. Hindawi Publishing Corporation (2014)
18. B.C. Munsell, A. Temlyakov, C. Qu, S. Wang, person identification using full-body motion and anthropometric biometrics from kinect videos, in *European Conference on Computer Vision* (2012)
19. L.R. Sudha, R. Bhavani, Biometric authorization system using gait biometry. Int. J. Comput. Sci. Eng. Appl. (2011)
20. H. Ng, W.H. Tan, H. L. Tong, J. Abdullah, R. Komiya, Extraction and classification of human gait features, in *Visual Informatics: Bridging Research and Practice* ed. by H. Badioze Zaman, P. Robinson, M. Petrou, P. Olivier, H. Schröder, T.K. Shih. IVIC 2009 (2009)
21. J. Ding, Y. Wang, L. Yu,Extraction of human body skeleton based on silhouette images, in *2010 Second International Workshop on Education Technology and Computer Science*, Wuhan, China (2010), pp. 71–74

Blockchain for Fool-Proof E-Voting Systems



Janardan Krishna Yadav, Srinivas Jangirala, Deepika Chandra Verma, Shashi Kant Srivastava, and Shehzad Ashraf Chaudhry

Abstract Blockchain-enabled e-voting system (BEV) is the need of the hour for many organizations and for democracies. With allegations being raised on validity of the voting system and mass protests, e.g., in the USA as well as the allegations of some hired tech companies interfering in elections of different countries, it is indispensable to have a reliable voting system to know the opinion of the voters. As paper ballot has its own issues of processing, safety and ease of e-voting is the way forward. Blockchain-based e-voting system can fix the loopholes that lead to voting frauds by first providing a unique ID to the voter and the eligible voters can cast a ballot anonymously at his comfort using a PC or smartphone. Second, the BEV's encrypted key and tamper-proof personal IDs can help to ensure the validity of the submitted vote, if any discrepancy happens it can be easily identified by the modified blockchain. The blockchain-enabled e-voting system relies on the encrypted data transfer and storage on distributed ledger that can be confirmed from any node of the blockchain. The voter ID cards are issued to the eligible voters, this ID card contains encrypted files that identify the owner and allows him/her to carry out a number of online transactions; say, for example, for a single time voting a single "coin" can be uploaded to the wallet of the user account that can be used to cast their vote only once. The voters are allowed to change their vote as many times they wish for a particular duration, say three days till the voting closes. Once the user confirms the vote by using

J. K. Yadav (✉) · S. Jangirala · D. C. Verma
Jindal Global Business School, O. P. Jindal Global University, Haryana 131001, India
e-mail: jkyadav@jgu.edu.in

S. Jangirala
e-mail: sjangirala@jgu.edu.in

D. C. Verma
e-mail: dcverma@jgu.edu.in

S. K. Srivastava
Indian Institute of Management-Sirmaur, Paonta Sahib, Himachal Pradesh 173025, India
e-mail: shashikant.srivastava@iimsirmaur.ac.in

S. A. Chaudhry
Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_44

the verification PIN or credentials, it is verified for authenticity. In the next stage, the identified authentic votes are transferred to the counting server and accounted for as advised by the voter. A non-blockchain e-voting system may leave many points where the frauds can happen for example under reporting of votes received, selecting a few responses that favor some candidate, corrupting the data, or erasing the data rendering the voting exercise invalid, etc. Blockchain proposes the possible solutions to each of these problems of the existing e-voting systems in practice. The BEV can provide the solution to the challenges any voting system in any level of organization may face, e.g., no coercion of the voters, anonymity of the voter, proof of a valid vote, correct counting and accounting of votes, avoiding single entity control on vote tallying and election result announcement, weeding out ineligible voters. All these issues will be discussed in detail in the chapter. This chapter often uses blockchain currency analogy to keep the reader interested and makes it easier for the reader who is not familiar with the blockchain technology or is familiar only with the bitcoins and focuses on major issues like voter access and voter fraud. Some used cases are also provided to illustrate the benefits and challenges in implementing the blockchain-based e-voting system industry that has remained at the forefront when it comes to technology adaptation and it seems the case for adaptation of blockchain technology. Blockchain technology has appeared as a landmark revolution in data encryption and storage. The distributed ledger system allows the hashes to be available with multiple nodes any time and tampering and modification create a new hash hence makes it easy to confirm the authenticity of the data files and track the node where the changes happened. Blockchain technology promises a great future for digital data security for digital transactions be it informational or monetary. Industries that deal with information exchange between multiple stakeholders like aviation industry have found multiple applications of blockchain technology, and the adaptations in the industry are advancing but still there is a long way to go. In this chapter, we discuss various transaction situations in the aviation industry where the blockchain technology can be of use or have already been put to practice.

Keywords Blockchain-enabled e-voting · Electoral fraud · Efficiency · Ballot anonymity · Data security · Permissioned distributed ledger

1 Introduction

Voting allows for the expression of democracy. Modern history is lined with the instances of efforts to improve the processes, mechanisms, and participation in electoral voting in an efficient and transparent fashion (ref). This is because electoral integrity signifies the nature of democracy by reflecting on the accountability and transparency of the system at one hand and improves the voter confidence re-enforcing democracy (ref). The voting mechanism suffers from two main issues—low turnout of the voters to cast votes and fraudulent behavior in voting (ref). Fraudulent

behavior in voting implies vote buying,[1] ballot box stuffing, coercing voters, booth capturing, votes cast by dead or illegal voters in addition to violations of electoral laws [2]. The spread of information and communication technology (ICT) was seen as a possible solution to both problems by enabling accessibility and transparency through adaption of the Internet technologies [3] that ranged from using a machine in a polling booth to electronic voting machines to Web cast votes. It was assumed that electronic voting (e-voting) would enable the elderly, the disabled, and in many instances, women cast their vote easily thus improving the voter turnout. It was also assumed that the e-voting would ease the operation and counting to get quicker results. In fact, e-voting has been found to be more efficient than paper voting as it ensures accurate, bias-free, convenient voting with quick results [4].

Voting through electronic means was first conducted in the USA in the year 2000 which was followed by similar e-voting in France, the UK, Spain, Ireland, Estonia, Portugal, the Netherlands, Paraguay, Finland, Austria, Germany, and Norway between 2001 and 2011. Despite these successes, it was only in 2007 that Estonia became the first country to allow remote e-voting in its parliamentary elections [4].

Despite advantages, e-voting is not fool-proof. This is proven by the latest instances in voting frauds across the world.[2] Further, operating e-voting is fraught with security issues [7] that demonstrate that e-voting may lead to challenges related to data integrity, reliability, transparency, ballot secrecy, system breakdown and data loss, misadoption due to uneducated voters, and higher costs due to storage of equipment and maintenance of data security [4].

Blockchain, that has recently emerged as a distributed ledger that is nearly fail-safe [8] can prove to be a possible solution to all the above issues. A blockchain is a data structure that maintains all transactions in near-real time. As a distributed decentralized ledger, it keeps the full and ever-increasing records protected from manipulation or tampering. "Blockchain allows every user to connect to the network, send new transactions to it, verify transactions and create new blocks. Each block is assigned a cryptographic hash (which may also be treated as a fingerprint of the block) that remains valid as long as the data in the block is not altered. If any changes are made in the block, the cryptographic hash would change immediately indicating the change in the data which may be due to a malicious activity. Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across various domains" [9]. In addition, blockchain technology increases the efficiency of conducting elections even when the number of voters increases phenomenally with only marginal increases in the cost once the private blockchain operated by the said election officials has been established making it a very sustainable system [10].

[1] Reports of vote buying were prevalent during the 2018 Venezuelan presidential election [1].

[2] Ukraine's central election system was hacked in 2014. It was also claimed that Russians had accessed the internal computers of VR Systems for eight states of USA in October 2016 around the time of Presidential elections [5, 6].

Electronic voting (e-voting) is a budding use case of blockchain through which the researchers aim to exploit the inherent benefits of blockchain, namely system integrity, anonymity of voter and non-repudiation to make the electoral processes accountable, transparent, and secure. Blockchain technology enables creation of voter-pool with unique addresses like e-wallets in cryptocurrencies. These unique IDs can adequately represent the eligible voter and the registered candidates. Further, either each voter is allotted a single voting token corresponding to their unique ID or weightage can be assigned to each voter depending upon the nature of the requirements set by the election administrator of the country and the type of seat.[3] Addresses booked and matched to the identified candidates can be similarly used to transfer voting token from voters based on their choice. This voting transaction is akin to the transaction of goods (services) and cryptocurrency from buyer to seller in a cryptocurrency blockchain. The voters could be assigned a limited time period or number of transactions to finalize their vote which once finalized can be added to the block of approved transactions. The officials of the election administration would be assigned addressed and powers to act as miner nodes approving finalized choices and adding the approved transaction to the block enabling near-real-time verified record update and maintenance that is almost immutable due to consensus protocol acknowledged by all miners and enforced by private blockchain created and run by legitimate election administrators [12].

In this chapter, we review the process of blockchain-enabled e-voting. Following this review, we examine some use cases of blockchain's application in the voting process and then the challenges involved in accepting BEV. We conclude the chapter with a discussion of possible improvements in the design of blockchain applications for e-voting in light of possible security, legal, and application issues.

2 A Review of Blockchain-Enabled Electronic Voting Systems

"Electronic voting uses electronic devices to record *and(or)* count votes" [10]. These systems are considered more efficient than paper ballots, in operation and storage that may range from voting-kiosks stationed at election offices to computers and even mobile devices [13]. Therefore, an efficient e-voting system should cover all phases of voting—registration of voters and candidates, authentication (verification), voting, and tallying. If done efficiently, nearly all issues of fraudulent practices in voting can be removed through e-voting.

In the registration phase of e-voting, the mechanism used should correctly register all eligible citizens of a country as voters. This process involves weeding out of voting

[3] Presidential elections in India happen through an electoral college. The members of the electoral colleges are Member of the Parliament (MPs) and Members of Legislative Assemblies (MLAs) of states and union territories. The vote of each MP and MLA is assigned weightage based on the population related weights for the states and union territories directly or indirectly [11].

by dead, immigrant, ineligible, and not turned up voters' IDs to be used to influence the election results which is conducted under verification of voters. Another part of the verification is when votes are being cast. Each vote must be encrypted and verifiable so that it is ensured that only eligible voters have cast their votes and through their own IDs. The anonymity and accuracy of the votes must be guaranteed. This happens only be the cast votes cannot be tampered with. Finally, the e-voting systems should allow for easy storage and efficient and correct counting of all verified cast votes [14]. Therefore, an efficient voting system should demonstrate the features listed in Table 1.

Examining the existing e-voting mechanisms, what we find that in comparison to paper ballot, electronic voting machines and Web-based voting, blockchain-enabled e-voting (BEV) is more efficient as it also the mechanism of voting that has the highest efficiency on most parameters listed in column (2) of Table 1 (please see the last row of the right-most column). While the data privacy issues may be questionable and uncertain for public blockchain, if the electoral administrative create a private and permissioned blockchain, it can overcome this issue. Further, on criteria like storage cost or scaling up of the system, allowing only eligible voters to be registered and to cast their vote, and allowing eligible members of the election administration to verify and authenticate, BEV is much more efficient than the other e-voting mechanisms too. BEV is also superior to other e-voting systems in maintaining correct records, efficiency, and counting of votes.

Blockchain-enabled voting systems have been proposed by researchers working on varied application of the blockchain [10, 12, 15]. Figure 1 illustrates a blockchain-based e-voting system that focuses on all processes of voting—registration, verification, voting, storage, and tallying. Unlike other systems, the blockchain-enabled e-voting system checks all requirements of an efficient e-voting system. In the design of a real voting system, permissioned blockchain structure with independent control node can be used to create a safer environment [10].

The literature talks about varied versions of BEV systems. Nodes may be designed in a permissionless public ledger or on a permissioned network (ref). In one version, the consensus mechanisms and process transactions can be set up by a neutral third party with independent nodes that can audit/verify once data finishes up getting stored on the ledger. Another version may be operated wholly by the electoral administrators.

Permissionless settings simulate environments well suited to a smaller number of users adopting a public blockchain due to increased level of complexity in mining a block and the average block creation time. On the other hand, permissioned blockchain simulates e-voting environments for larger number of voters required for most electorates across countries. Thus, the two types of ledgers may be chosen based on the trade-off between transaction block size and transaction processing speed.

The representation of BEV provided in 1 shows the various voting processes and their integration with the blockchain. The voting process commences with the registration of voters and candidates as unique hashes akin to e-wallets. Then, each voter address is assigned a token representing a single or a weighted vote to avoid

Table 1 Desired features of an efficient voting system

Voting process (1)	Feature (2)	Paper ballot (3)	EV machine (4)	Web-based voting (5)	Blockchain-enabled voting (BEV) (6)
Registration	1. Only eligible voters and candidates should be registered	✗	✗	✓	✓✓
Verification	2. Only eligible members of the election administration should be allotted verification power	✓	✓	✓	✓✓
Verification	3. Only eligible voters should be able to cast their vote	✗	✗	✗	?
Voting	4. The identity of voters should not get revealed	✓	✓	?	?
Voting	5. Voters should be able to cast their vote only once	✗	✗	✗	?
Voting	6. The receipt for voting should not display any information on the voter's choice	✓	✓	✓	✓
Voting	7. Voters must not be able to discuss and influence each others' choice in real time	✓	✓	✗	✗
Storage	8. Storage cost or scaling up of the system to include a much larger number of voters should raise the cost of the operation only marginally	✗	✗	✓	✓✓

(continued)

Table 1 (continued)

Voting process (1)	Feature (2)	Paper ballot (3)	EV machine (4)	Web-based voting (5)	Blockchain-enabled voting (BEV) (6)
Storage	9. The records should be stored in a fail-safe manner without a possibility of breakdown	✗	✗	✗	✓
Storage	10. Each vote should be recorded correctly and the record should be immutable	✗	✗	✗	✓✓
Tallying	11. Votes should be counted easily	✗	✓	✓✓	✓✓
Total score		***4/11***	***5/11***	***5/11***	***7/11***

Meaning of notations: ✗ implies inefficiency of a voting mechanism with respect to the stated feature in the corresponding row.
? implies uncertainty in classifying the efficiency of a voting mechanism with respect to the stated feature in the corresponding row.
✓ implies efficiency of a voting mechanism with respect to the stated feature in the corresponding row.
✓✓ imply very high efficiency of a voting mechanism with respect to the stated feature in the corresponding row.
The total scores are compiled by tallying the number of features for which the voting mechanism is efficient. This is 7 for BEV out of a total of 11 features.
Source Authors' own.

multiple voting from a single hash (refer to feature 5 in Table 1). The voters casting their vote to their chosen candidate leads to a transfer of their respective allotted token to the account of the candidate which is similar to transfer of cryptocurrency by the buyer to the seller to complete a transaction. Each transaction would be verified and added to the block which eventually gets connected to the new block as transactions grow forming a chain of cryptographically connected blocks composed of various transactions (refer to feature 3 in Table 1). This process is immutable and therefore not even a single record can be changed (refer to feature 10 in Table 1). The records from blockchain can be very efficiency tracked and tallied (refer to feature 11 in Table 1) to produce the result of the voting as soon as the last transaction within the allotted time is made.

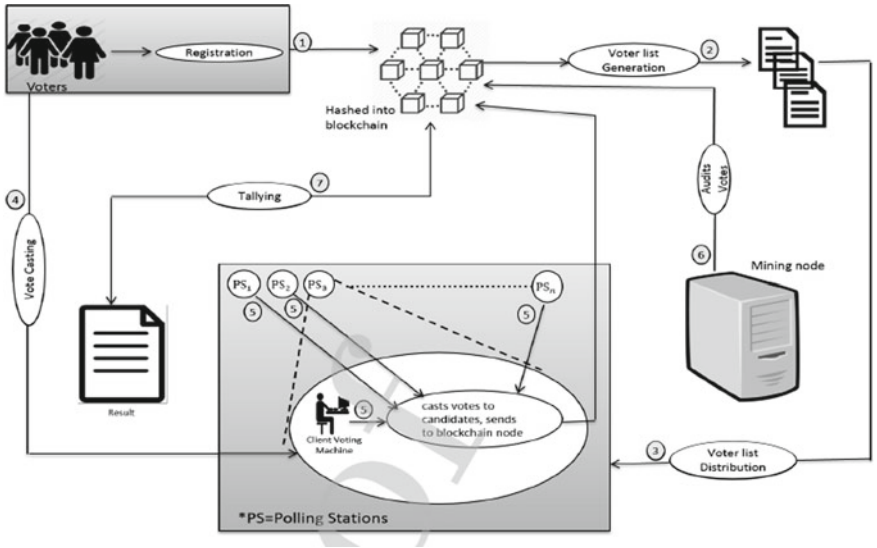


Fig. 1 A representation of a blockchain-enabled e-voting system [10]

3 Use Cases of Blockchain-Enabled e-Voting System

While blockchain technology has been around since 2008 (ref) with varied applications and use cases (ref), there are very few applications of the blockchain-enabled e-voting (BEV) system.

A small-scale instance of e-voting through blockchain was when South Korean province of Gyeonggi-do used a BEV system to collect votes on community projects in 2017 where 9000 residents participated in the voting process. The votes, results, and other relevant data were stored in a blockchain that did not involve any central authority in the voting process [15].

Sierra Leone was the first country to conduct elections through BEV system in March 2018. This BEV was designed and executed by the Swiss start-up Agora for two districts of Sierra Leone. This BEV system was partially manual where after the voting, a team of accredited observers entered the data of 400,000 ballots into the designed BEV which was an immutable distributed ledger, offering instant access to the election results ensuring trust and transparency among the electorate [16].

In another instance, Moscow commenced a BEV pilot project in June 2019 that was a joint venture of the Moscow City Election Commission and Moscow Department of Information Technology (DIT). This system was to be tested at the end of June 2019 to vote on controversial constitutional amendments [17] but issues were found with it[4] [18]. Finally, BEV system was used in elections of September 2020 but

[4] Russian officials were using a variant of the ElGamal encryption where the encryption key sizes were too small to be secure and encryption could be compromised within minutes.

remained centralized [17]. The BEV system was developed under telecommunications giant Rostelecom and was used in September 2020 for remote voting during by elections for seats in the national parliament in Kurskaya oblast and Yaroslavskaya oblast despite Central Election Commission identifying the need for improvements in the BEV [19] as the BEV system was only considered as another form of voting to enhance transparency in elections and reducing intermediaries [16].

4 Challenges

Despite blockchains are inherently designed at providing security, accuracy, and immutability features that are necessary ingredients for an efficient e-voting system, as is evident from the description of the application of BEV in real elections, several major issues need to be addressed before their widespread usage. These challenges can be categorized into three types—adoption-related issues, security-related issues, and legitimacy-related issues.

Adoption-related issues

1. Blockchains' complexity: The blockchain is a complex system to use especially when it comes to mining. Further, very few people know and operate on blockchain because it is still in its early stages of adoption (ref). The poor adoption of the technology would lower the chances of mainstream acceptability of BEV. Another deterrent in its poor adoption is low broadband access and equally poor digital user skills [15]. In 2016, when the Democracy Earth Foundation tried to use a blockchain in a peace plebiscite to ratify the agreement to terminate the conflict between the Colombian government and FARC guerrillas, the foundation's main challenge in the deployment was the technology's poor adoption.
2. Design issues: The real-time design and encryption of the BEV need to be complex enough to avoid hacking which did not happen in the 2019 trial of BEV in Russia.
3. Scalability issues: There are not enough observations to determine the scalability of BEVs. Also, the nature of the ledger and the trade-off in favor of efficiency may reduce the scalability of BEVs. Further, blockchains require much energy to perform transaction validation. Thus, using BEVs for national e-voting may not yet be economical.

Security-related issues

1. Authentication vulnerability: Despite each individual being assigned an electronic ID and a PIN, in absence of adequate monitoring and control, a hacker could vote for multiple people if happened to know the PIN for each corresponding electronic ID [15].
2. Possibility of a Sybil attack: A hacker can create a large number of nodes in an attempt to disrupt the network operation by hijacking or dropping messages in a

Sybil attack. Even consensus protocols are prone to Sybil attacks. These attacks may not only compromise the data stored in the blocks but also the anonymity of the voter.

Legitimacy-related issues

1. Transparency: "The BEV process is transparent, decentralized, and bottom-up. BEV may not perform well in a society whose culture and values exhibit low compatibility with these values" [15].
2. Traditional voting systems function under state authority: BEVs, however, may shift the power away from central actors in case the BEVs are designed by non-state owned third parties instead of the electoral administrators and other government agencies. Thus, the BEVs may face resistance from such political leaders who benefit from the status quo [15].
3. Remote voting: Remote elections provide no guarantee on the privacy of voting as does a polling booth. Real-time manipulation of a voter's vote by family, friend, or a coercer can influence one's vote. Further, people could identify themselves as another person compromising the validity of the system.
4. Voter privacy: The paper ballot voting system ensures the voters' privacy. To ensure voter privacy, the system design should ensure the inability to trace back the voters from the individual votes. While reverse tracking of hashes is not possible, leakage of the voter IDs and PINs can compromise voter anonymity [16].

5 Conclusion

In this chapter, we have critically appraised the process of blockchain-enabled e-voting. While examining the relative merits of blockchain-enabled e-voting (BEV) system against other voting systems, theoretically, BEVs are the most efficient. However, reflecting on some use cases of BEVs in South Korea, Sierra Leone, and Russia, we find that on ground, BEV's application on a large scale is fraught with challenges.

While practical application of BEVs suffers from adoption, security, and legitimacy issues, it is not going to remain so for a very long time. With increased bandwidth and digital user skills improving in COVID times (ref), the perceived complexity of the BEV design will get reduced. Further, the incident in Russia in 2019 indicates a poor choice of encryption and as more researchers work on blockchain and cryptography, the likelihood of weaker encryptions goes down (ref). The issue of scalability through permissioned private ledgers supported by biometric facilities would reduce authentication vulnerability [15]. And it may very well be that the permissioned ledger may soon be time efficient as well (just like the solution of the double spend problem got resolved), reducing the possibility of Sybil attacks to a larger extent. Further, if BEVs are not set up as remote voting, the issues of privacy, influencing of votes, etc., will not arise. However, this will reduce the expected efficiency of the BEV system on the whole.

In fact, India's Election Commission is collaborating with IIT Madras to design a two-way BEV system which would be enabled with biometric devices and a web camera. The voters will need to cast their votes at predesignated polling booths. The registration process would identify voters and authorize them through a multilayered system using biometrics and web cameras. A blockchain-enabled personalized e-ballot paper, in the form of a smart contract, will be produced. As soon as the vote will be cast, that is, the smart contract executed, the ballot would be secured through hash encryptions notifying the participant nodes (candidates and voters) of the number of votes cast to each candidate. The encrypted votes in the form of smart contract would be revalidated precounting to ensure that the system was not decrypted nor tampered with [20].

Increased adoption of blockchain technology would stimulate transparency which would provide it with legitimacy. Further, it does not necessarily imply that the BEVs need to be designed and run by the authorized parties instilling its legitimacy in different political economies.

"Blockchain technology is currently in a nascent state. There have not been enough distributed ledger technology and blockchain-based applications to sufficiently evaluate whether this technology is superior to current voting systems" [15] in reality on a scale that would make such designs get adopted by countries to conduct full-fledged elections. However, political violence and fraudulent electoral practices ranging from the poorest to the riches countries in the world create a case for further investigations on strengthening the mechanism and adoption of BEVs that are capable of ensuring secure and transparent elections that reduce electoral corruption.

References

1. N. Casey, J.H. Davis, *As Trump Adds Sanctions on Venezuela, Its Neighbors Reject Election Result* (May 2018). Retrieved from https://www.nytimes.com/2018/05/21/world/americas/venezuela-nicolas-maduro-sanctions.html
2. F. Lehoucq, Electoral fraud: causes, types, and consequences. Ann. Rev. Political Sci. **6**(1), 233–256 (2003)
3. J. Göbel, H.P. Keeler, A.E. Krzesinski, P.G. Taylor, Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay. Performance Eval. **104**, 23–41 (2016)
4. J.B. Esteve, B. Goldsmith, J. Turner, *International Experience with E-Voting*. Available online: https://www.parliament.uk/documents/speaker/digital-democracy/IFESIVreport.pdf. Accessed on 15 July 2020
5. M. Clayton, *Ukraine Election Narrowly Avoided 'Wanton Destruction' From Hackers* (June 2014). Retrieved from https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers
6. M. Cole, R. Esposito, S. Biddle, S. Grim, *Russian Hacking Effort Days Before 2016 Election* (June 2017). Retrieved from https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/
7. P.Y. Ryan, S. Schneider, V. Teague, End-to-end verifiability in voting systems, from theory to practice. IEEE Security Privacy **13**(3), 59–62 (2015)
8. S. Jangirala, A.K. Das, A.V. Vasilakos, Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment. IEEE Trans. Industrial Informatics **16**(11), 7081–7093 (2019)

9. K.M. Khan, J. Arshad, M.M. Khan, Investigating performance constraints for blockchain based secure e-voting system. Future Generation Comput. Syst. **105**, 13–26 (2020)
10. R. Taş, Ö.Ö. Tanrıöver, A systematic review of challenges and opportunities of blockchain for E-voting. Symmetry **12**(8), 1328 (2020)
11. V. Srivastava, The president of India-election and office. Indian J. Political Sci. **39**(2), 250–269 (1978)
12. F.Þ.Hjálmarsson, G.K. Hreiðarsson, M. Hamdaqa, G. Hjálmtýsson, Blockchain-based e-voting system, in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE (2018, July), pp. 983–986
13. H.N. Oo, A.M. Aung, A survey of different electronic voting systems. Int. J. Sci. Eng. Technol. Res. **3**(16), 3460–3464 (2014)
14. R. Jardí-Cedó, J. Pujol-Ahulló, J. Castella-Roca, A. Viejo, Study on poll-site voting and verification systems. Comput. Security **31**(8), 989–1010 (2012)
15. N. Kshetri, J. Voas, Blockchain-enabled E-voting. IEEE Softw. **35**(4), 95–99 (2018)
16. T.K. Sharma, (n.d.)., *Top Countries that Conducted Elections on the Blockchain.* Blockchain Council. Retrieved from https://www.blockchain-council.org/blockchain/top-countries-that-conducted-elections-on-the-blockchain/
17. A. Baydakova, *Russia's New Blockchain Elections Remain Centralized* (August 2020). Retrieved from https://www.coindesk.com/russia-vote-blockchain
18. C. Cimpanu, *Moscow's Blockchain Voting System Cracked a Month Before Election* (August 2019). Retrieved from https://www.zdnet.com/article/moscows-blockchain-voting-system-cracked-a-month-before-election/
19. A. Baydakova, *Russia's New Blockchain Voting System Isn't Ready, but It'll Be Used This Month Anyway* (September 2020). Retrieved from https://www.coindesk.com/russia-blockchain-voting-waves
20. N.A., *EC with IIT-Madras to Explore Blockchain Technology for Voting*. Economic Times (February 2020). Retrieved from https://government.economictimes.indiatimes.com/news/digital-india/ec-with-iit-madras-to-explore-blockchain-technology-for-voting/74161191

UAV System Using Convolutional Neural Network (1. Angle Prediction Model)



Abhishek Muttath, Aditya Veer, Muskan Pandey, Mayuresh Gawai, and Vaishal Wangikar

Abstract This paper presents a novel approach on development of autonomous-based navigation system with the visual from camera interface and without depending on global positioning system. This system consists of several parameters which lead to development of complex operation to be performed. Angle prediction is used as to steer the UAV to its original path. By remote sensor and camera, the data get feed on the system path by few iteration of overall dataset. This system realizes on deep convolutional neural network (CNN) combined with the steering path with inclusion the degree of freedom like yaw, roll, and pitch. The system is then able to get calculated by the generated dataset helped form Udacity simulator. By this simulator, we get the prediction of the direction of the way points. Then, the model gets trained on the behalf of this content, and finally, run on the simulation model on gazebo to check the error loss in the performance of them. The model is suitable for development in autonomous-drone navigation system that exhibits similar location such as environmental and desertification areas.

Keywords Autonomous · Steering path · Prediction · Simulation · Gazebo

A. Muttath (✉) · A. Veer · M. Pandey · M. Gawai · V. Wangikar
School of Computer Engineering and Technology, MIT Academy of Engineering, Pune, India
e-mail: apmuttath@mitaoe.ac.in

A. Veer
e-mail: asveer@mitaoe.ac.in

M. Pandey
e-mail: mpandey@mitaoe.ac.in

M. Gawai
e-mail: mvgawai@mitaoe.ac.in

V. Wangikar
e-mail: vcwangikar@comp.mitaoe.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_45

1 Introduction

Unmanned aerial vehicle (UAV) also known as aerial drones which is low cost and versatility is used in many application such as for traffic monitoring, parcel delivery, military surveillance, and getting geological data through it of a region. The later was then implemented with the onboard sensors such as global positioning system and inertial measurement units to autonomously navigate the drone along predefined paths. With the closed-loop sequence of the IMU and GPS, it enables the drone to travel along certain paths with certain parameters, and relevance of the overall GPS-based system is having the weakness that it could not calculate the value under the close environment, and missing of the satellite control over it would lead to certain devastating effect of the system. Along with this, the system is not able to rely self-dependency path of prediction, there are no means of algorithm to travel without the GPS of the system, and even in tighter areas, the system would not be able to hold a constant lock (drift) over a place which would be difficult to work with it. To overcome this issue, we have placed a solution by implementing the raw system of mounting monocular camera on the front place of drone. Onboard processing is present to calculate the matrix of image and pass through set of input layer by overlapped by the camera. The deep convolutional neural network is used to calculate the overall images captured by the system and then compute it through set of trained examples. The output of this system helps to denote the turning angles required in order to follow the path. Overall, the system could get the steering commands through this interface without the GPS intervention during autonomous drone navigation. We checked with some other outputs to their related work in Sect. 2, describe the details of our system in Sect. 3, and the collection of data in Sect. 4. Section 5 presents about experiments and results, whereas Sect. 6 gives the conclusion for the paper and its future work in a particular directions.

2 Related Work

CNNs are one of the neural network techniques which have achieved a remarkable progress in the development of the image classification system, like in visual image recognition competition (ILSVRC) [1], and since then, it is being used in different computer vision task such as in detection [2, 3], localization, and segmentation which is the growth toward the development of performance in computer vision algorithms. From a few decays, the overall development in the CNNs has been used in the development of the autonomous navigation system such as vehicles, robots, and aerial drones, combined with the reinforcement learning with the model predictive control system to train a deep neural network. The overall prediction is used to deal with the image classification of the entity to get the numerical output which would further be beneficial in dealing with it. One of the system which has implemented deals with detection of the object in four field direction not by the sensor but by

the camera using Dagger algorithm which was implemented to avoid the trees while working under its environment [3]. Certain amount of system is then compiled by the help of CNN which is used in whether detection, face classification, and many more. The important factor which uses to also deal with the UAV development of the project is basically under the drone system, which specifically deals with the autonomous driving toolkits [4]. This system has many sequential development of the parts that are present toward autonomous development of drones. Overall, the system could be implemented with the help of this toolkit which consists of many types of complex values which could directly be used for the implementation of the system [2]. In this work, we focus that the system of the drone must accomplish the task without having any problem facing by any of the sensor and should smartly shift to its network of image where other sensors tend to fail. By the help of CNN, it is possible to accomplish certain onboard processing which would help to hold the desire path with inclusive of GPS and other system which would help to make the system more sustainable throughout the peak moment of it [3].

3 Proposed Approach

3.1 Methodology

As in Fig.1, it represents the model diagram of the overall system. First of all, the system of aerial drone used to capture the video and divide it into photo buffer. Three

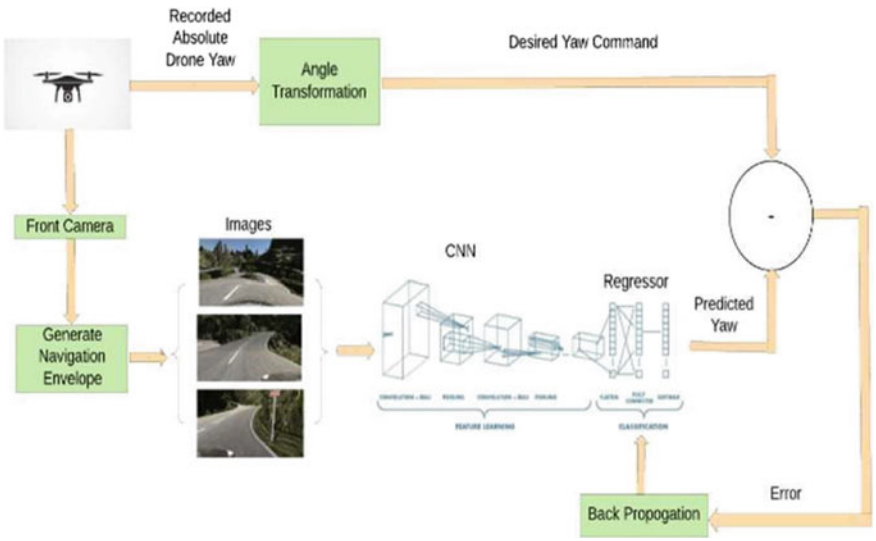


Fig. 1 System architecture

Table 1 Information used on the paths (dataset)

Path ID	Environment	No. of trained images	Distance (m)	Sum of angle change (rad)
1	Open	4320	149.90	5.00
2	Open	12,380	245.39	4.48
3	terrain	12,086	267.22	4.23
4	terrain	8648	412.16	6.63

cameras in front of the system used to capture it, then the data are compared to the trained model, and further, it is used to predict the angle as compared to the image even tough the dataset could be universal, it will be able to track down many of its data which would easily lead to optimum path detection.

This model is then passed through CNN network chain which then reduces the pixel size of the image (Conv2D). In our method, in order to flatten the curve, we use the five steps to reduce the image size in up to 64 pixel which would lead to calculation of max pooling relevant to its easiest method. Later, the system output is compared to its loss function which then reduces the distance between the predicted output and actual one.

The overall command is to steer the drone in its direction by changing the yaw and roll commands. This axis used to change the direction of the aerial drone and helped to lead its desired position.

The point should also be noted that the CNN layer must be frozen during its extraction of features when development toward its unique simulation (Table 1).

The mean squared error is one of the techniques which is used in loss function which used to calculate the predicted yaw direction and actual yaw direction.

$$\text{MSE} = \frac{1}{n} \sum_{i} (y_i - p_i)^2$$

The value of true yaw is calculated as the angle between the next waypoint and the drone heading. The point by which the drone deviates from its next waypoint position is calculated by this formula to calculate its error. Loss function is used to help the other network to easily correlate between the entire visual input and its deviation angle. During runtime simulation, the path gets divided into independent checkpoints. This checkpoint is then recognized as the segment which later on gets overlapped with the model for training the entire navigation path.

3.2 Control Surface Interface

The calculation of the system is taken place on the basis of the angle required to tilt the drone with the respect to the visual that is present during its runtime environment. The data used to fetch over the system visuals are then used in CNN network which

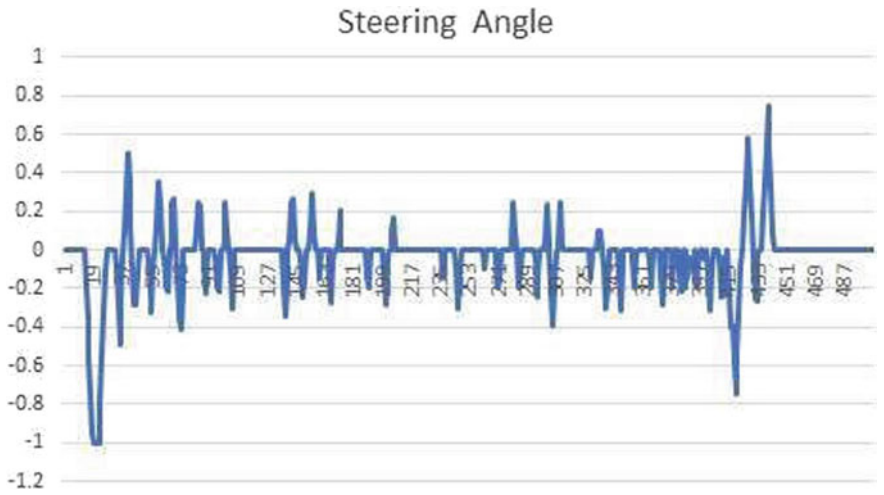


Fig. 2 Steering angle prediction

will then override the command that is given by the other sensors to perform certain task like following the path or to avoid certain obstacle. Taking the consideration of simulator-generated optimal paths or those acquired during the development of real flights makes the model vulnerable to minor drifts and less adoptable to differences in starting point (heading). For instance, if during testing, the drone drifts off, then due to this, there will be a slight visual feedback that would affect during its training point which would lead in additional drifting (Figs. 2 and 3).

4 Dataset

To generate the dataset which consists of the left image, right image, center image, and steering angle, we have used Udacity simulation software in order to generate a virtual images and angle done by consultation of human intervention. Training dataset contains 7280 frames with corresponding label including steering angle (yaw and roll) value. The image generated by this system is 640x480 which is then downscaled to 320 × 160. For better accuracy, the image is being stored in their respective directory, and content is accessed through their relative column value (Fig. 4).

5 Results and Conclusion

The final outcome of the system is to get the direction prediction in such a way that the system could easily deal with the direction, and in any failure of the system,

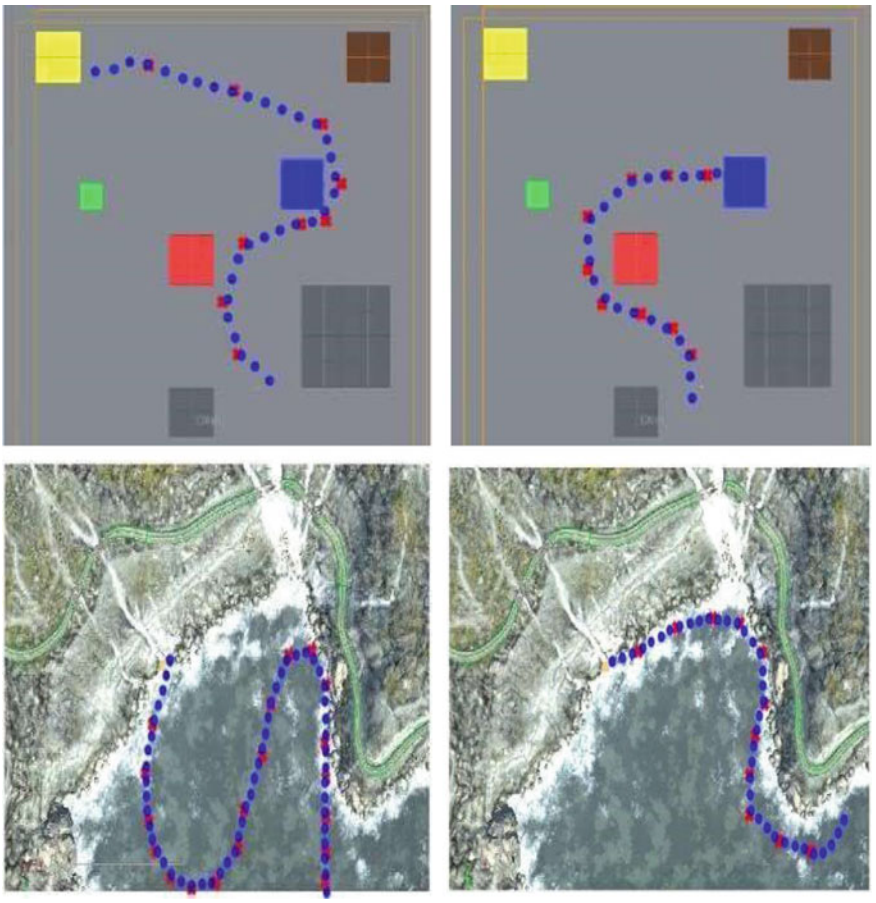


Fig. 3 Directional path by avoiding system through camera

the overall serial drone could easily solve the problem and move further in the path without any obligations.

The path of input data is processed and filtered out from the dataset creator with the help of Udacity simulation software. The parameters of this are stored then in terms of a data folder consisting of images and steering .CSV file. All over, the dependencies are then run under the model file, and this file is then trained out with 20,000 iteration in each epoch giving it a complete smooth render development which is then converted in machine understandable language.

This program creates a model name which later is used in model testing. Then, by this model, the driving data are used to get the output on the simulation. The accuracy of this model is around 86 percent, and it is universal and could work on any road dataset because of which while testing on different simulation, it was able to read out the value in a correct form.

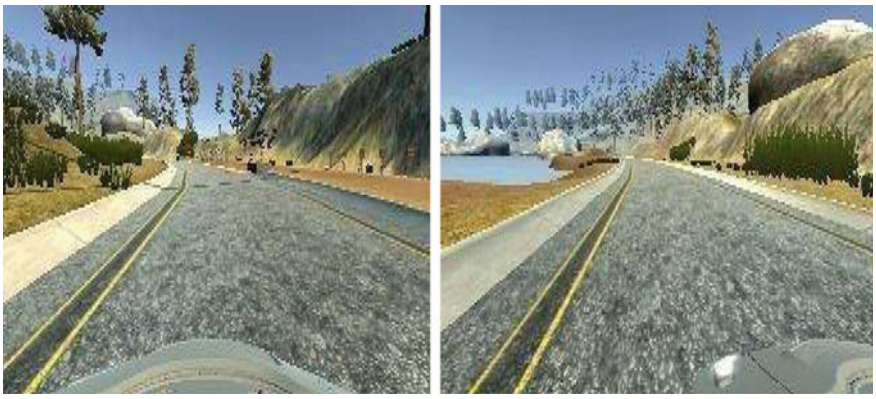


Fig. 4 Figure of left and right images captured during the runtime simulation and stored the angle value in dataset

Overall, the CNN neural network gave us the prediction through which the direction changes of aerial system could be controlled on the basis of camera rather completely relying on other sensors. This system could easily highlight the data with the combination of GPS which would lead to good performance benchmark.

In examining the final letter outcome, our predictive model on convolutional neural network (CNN) could easily establish the connection between the transfer learning models in the system. This result is eventually produced from our models without any external smoothing function. From this system, we are able to show the transfer learning on the model in the autonomous field. During this system, the CNN was limited with its computational resources, but still, it provided a good architecture. In the future work, the CNN model architecture could be expanded by deeper layers to get more accurate result, and the development phase would lead to clear understanding and implementation of the project. This project would be able to enhance the future scope of UAV system under their autonomous requirements (Fig. 5).



Fig. 5 Final simulation while running the on-time rendering system

References

1. J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, L. Fei-Fei. Imagenet: a large-scale hierarchical image database, in *IEEE Conference on Computer Vision and Pattern Recognition*. CVPR 2009. IEEE, (2009), pp.248–255 [10]
2. J. Redmon, S. Divvala, R. Girshick, A. Farhadi, You only look once: unified, real-time object detection, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (2016), pp. 779–788 [11]
3. J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, L. Fei-Fei. Imagenet: a large-scale hierarchical image database, in *IEEE Conference on Computer Vision and Pattern Recognition*, CVPR 2009 (2009), pp. 248–255
4. A. Loquercio, A.I. Maqueda, C.R. del-Blanco, D. Scaramuzza, *DRONET: Learning to Fly by Driving IEEE* (2017)

Blockchain for Aviation Industry: Applications and Used Cases



Janardan Krishna Yadav, Deepika Chandra Verma, Srinivas Jangirala, Shashi Kant Srivastava, and Muhammad Naveed Aman

Abstract The aviation industry has remained at the forefront when it comes to technology adaptation and it seems the case for adaptation of blockchain technology. Blockchain technology has appeared as a landmark revolution in data encryption and storage. The distributed ledger system allows the hashes to be available with multiple nodes any time and tampering or modification creates a new hash hence makes it easy to confirm the authenticity of the data files and track the node where the changes happened. Blockchain technology promises a great future for digital data security for digital transactions be it informational or monetary. Industries that deal with information exchange between multiple stakeholders like aviation industry have found multiple applications of blockchain technology, the adaptations in the industry are advancing but still, there is a long way to go. In this chapter, we discuss various transaction situations in the aviation industry where the blockchain technology can be of use or have already been put to practice.

Keywords Blockchain · Smart Contracts in Aviation Industry · Blockchain-based Aviation Supply Chain · Data Security

J. K. Yadav (✉) · D. C. Verma · S. Jangirala
Jindal Global Business School, O. P. Jindal Global University, Haryana 131001, India
e-mail: jkyadav@jgu.edu.in

D. C. Verma
e-mail: dcverma@jgu.edu.in

S. Jangirala
e-mail: sjangirala@jgu.edu.in

S. K. Srivastava
Indian Institute of Management-Sirmaur, Paonta Sahib, Himachal Pradesh 173025, India
e-mail: shashikant.srivastava@iimsirmaur.ac.in

M. N. Aman
School of Computing, National University of Singapore, 13 Computing Drive, Singapore, Singapore
e-mail: naveed@comp.nus.edu.sg

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_46

1 Introduction

Aviation or air transport industry is has seen a rapid growth in the past few decades and has been a subject of rapid evolution with the advancement of technology including aviation technology, digital communication, and the internet. Aviation industry includes not only the passenger air travel, but the air cargo services, airports and ground support, navigation services, and distribution services that include physical and online travel agents, tour operators and banking intermediaries who facilitate the entire supply chain and value delivery. All these players have rapidly adapted to the technological innovations and perhaps are the forerunners when it comes to using latest information technologies, e.g., global distribution services like Amadeus, Galileo, and Sabre. The GDSs and the Neutral Units of Conversion (NUC)-based billing and settlement plan (BSP) facilitate the communication and transaction settlements in the industry between the airlines. This kind of data exchanges has security and storage needs. The need for a system to ensure authenticity of the data extends to the other stakeholders and governing bodies like ICAO and IATA which publish the rules, codes, sectors of flight, and other information in a coded language to keep the information safe and away from other civilians who are not part of the industry.

This kind of coded language may not be as fool proof as the blockchain-based systems that have evolved in the recent years. A blockchain-based system based on hashing facilitates verification of the data prevents the threats of database getting corrupt and automating various transactions through smart contracts.

Blockchain in aviation industry is relatively new technological adaptation and the industry is a forerunner again to adapt to this new technology. Not only the aviation industry but the blockchain technology has changed the way business process are managed and value is created and delivered throughout the world in many industries. Blockchain technology comes with a potential to solve many transaction and information-related processes through improved tracking of cargo and passengers, enabling airports to become 'smart airports' through smart contracts, preventing cyber-attacks and hacking threats and at the same time reducing the cost for transactions. Bitcoins have already revolutionized the financial sector and airlines are yet to see that transformation.

The aviation industry can benefit by the blockchain technology in management and sharing of data, as it is a distributed ledger and any member on that blockchain can confirm the authenticity of the data. For example, passenger name records (PNR) and e-tickets can be easily validated and the dependence on GDSs can be reduced. Similarly, the loyalty programs are becoming so much complicated when it comes to keep a track of reward points as well as redemption options, smart contracts and real-time transactions can ease the life of customers dealing with alliance firms to the airlines or perhaps enable them to use reward points as currency. In the area of air freight, the digitizing of the various information required in blockchain could reduce cumbersome paperwork.

The Aviation industry is a complex ecosystem consisting of passengers, freight companies, airport authorities, partner airlines, online travel agents (OTAs), global

distribution systems (GDSs), industry associations such as IATA, and regulators like ICAO, public authorities, and other industry players like hotels and car rental companies.

Aviation industry thus always had to deal with sharing accurate information and making accurate payments and commissions to its various partner, e.g., carrier, government agencies, code-share partners, etc. The problem is complicated by accepting money from customers in different currencies and settling the payments in another currency. For long airlines have relied on their global distribution systems (GDS) like Galileo and Amadeus for accurate information and neutral units of conversion (NUC) to overcome these issues. In the absence of technologies like blockchain this has worked well till now but the changes in past few years have put the industry under stress. The trends like shift toward economy class fares, narrowing margins for distributors, increasing prices of fuels, increase in airport charges and government surcharges have strained these distribution systems.

To cut the cost and make the systems efficient the airlines have already started to adopt AI, analytics, and robotics to downsize the workforce and bring in-efficiency. Still, the core needs to share data and seamless digital transactions have remained the same. With AI and digital revolution airlines even have more data at their hand that not just needs to be analyzed and mined but securely saved and transferred, hence, blockchain has many roles to play in the airline industry. Blockchain surely has potential to resolve the current issues of trust, security, control, and transparency in this complex ecosystem of aviation industry. Many forerunners in the industry have started already to leverage on the blockchain technology specifically in areas like customer-related activities; maintenance, repair, ground operations; and revenue accounting (Fig. 1).

Most common applications of blockchain in aviation industry include repetitive processes and payments that can be automated through smart contracts. Smart contracts can be for day-to-day billing tasks among airlines, travel agents, insurance purchase and claims, and regular disbursal of taxes and surcharges on predefined rules. For loyalty rewards, many airlines are experimenting with giving option to redeem ‘miles’ or points at various retail outlets and fashion brands and terms and conditions may vary for each outlet, smart contracts with predefined rule can help in easy reconciliation. Similarly, the smart contract applications extend to payment reconciliation amongst partners and revenue accounting, the dependence on GDS (which control indirect ticket sales because of unaffordable subscription fees for small travel agents) it will provide more flexibility and creative tour packaging by small travel agents. For cargo and luggage shipments smart contracts and distributed ledger can reduce the hassle of shipping and can prevent the cases of frauds and lost luggage pieces (Fig. 2).

The blockchain technology is still in its early stages of application and has its own share of issues; for airline industry, the initial hurdle is the cost of technology and future challenges are to grow from small private networks to industry-wide adaptation, the ecosystem is complex and includes government bodies at various levels and the government policies for blockchain differ a lot across the globe. The

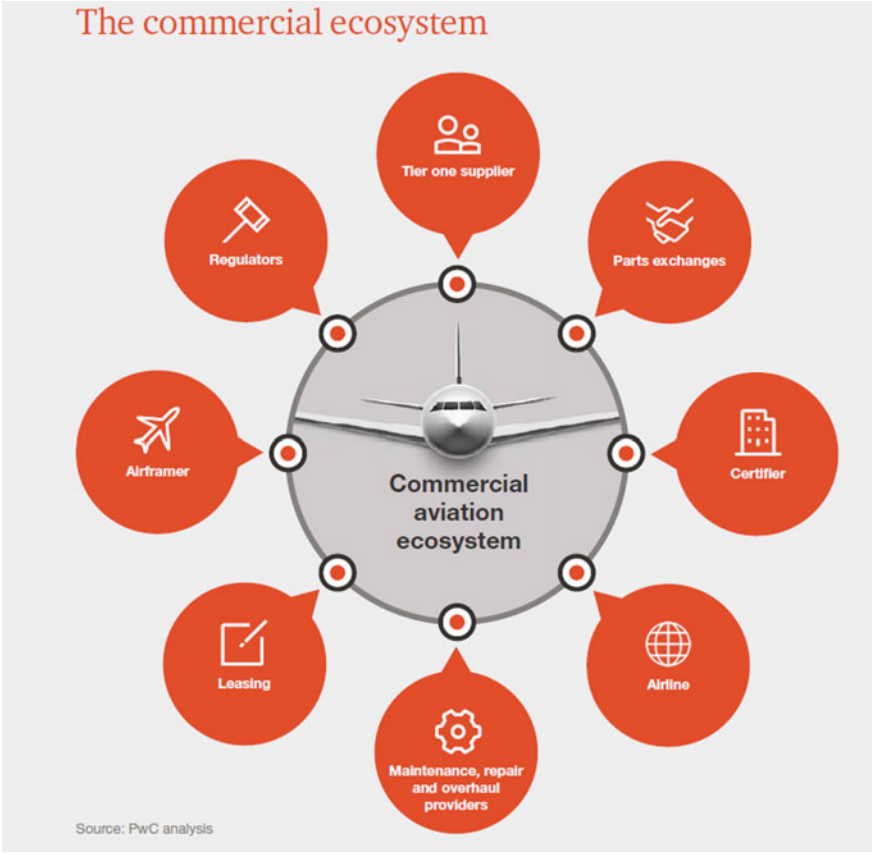


Fig. 1 The commercial aviation ecosystem [1]

IATA travel grid is a concept developed by IATA to manage hassle-free transactions among various stakeholders after years of research and thought process for blockchain integration. It is a common grid that would allow the proliferation of a democratic, yet fast, efficient and flexible environment that provides blockchain capabilities that can be leveraged by the industry. The IT architecture is analogous to Apple's ecosystem concept that has platforms for app developers to create customized apps. Let's understand these application areas further in the coming sections (Fig. 3).

1.1 Blockchain and Aircraft

Let's start with the core equipment in the industry that is the aircraft. The aircraft as we see today has seen a great transformation and technological advancement over many decades. The aircrafts of today are far more sophisticated and better equipped to

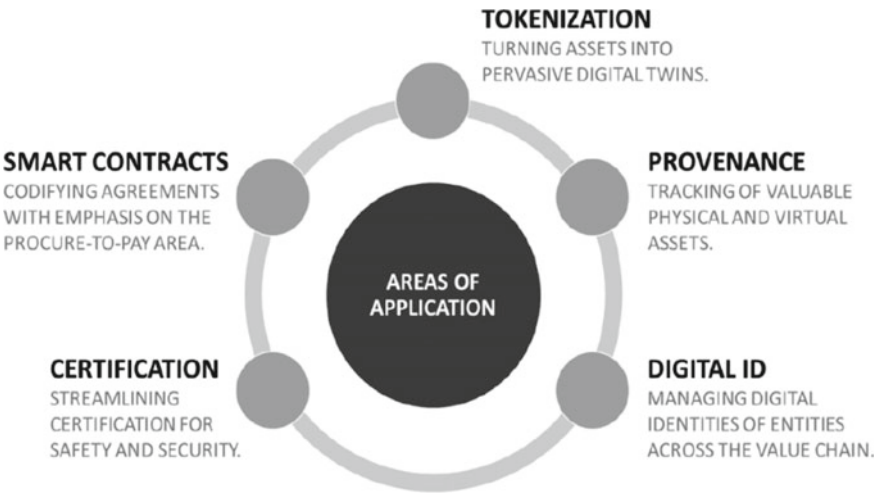


Fig. 2 Possible areas of application of blockchain in aviation industry [2]

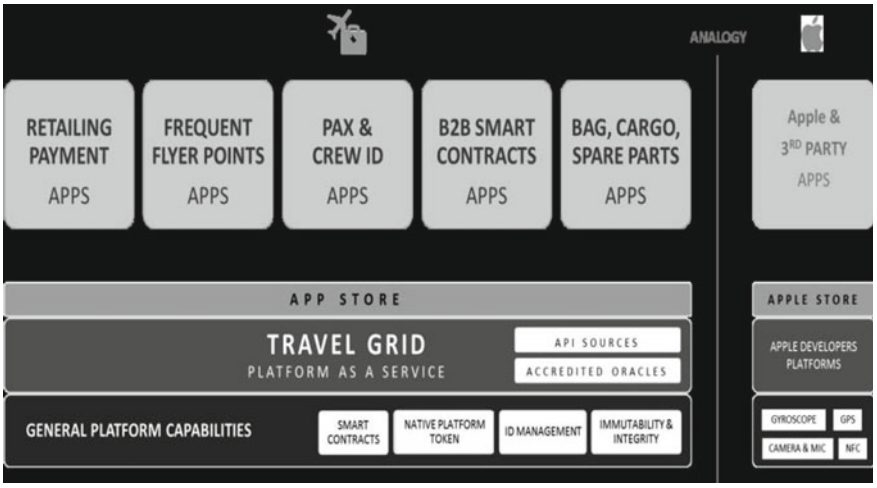


Fig. 3 IATA travel grid concept [2]

withstand the atmospheric and navigational challenges that the aircraft faces during high altitude flight, at take-off, and at landing. Today, aviation industry boasts of the safety mechanisms and monitoring of the aircrafts health to claim the safety of passengers inflight. It is impossible to check each and every piece in the engine and the aircraft in the short turnaround time that most aircrafts have, hence there is a great role played by the automated units that send back data about its proper functioning or other parameters needed to monitor the heath of that piece in the aircraft. Thus,

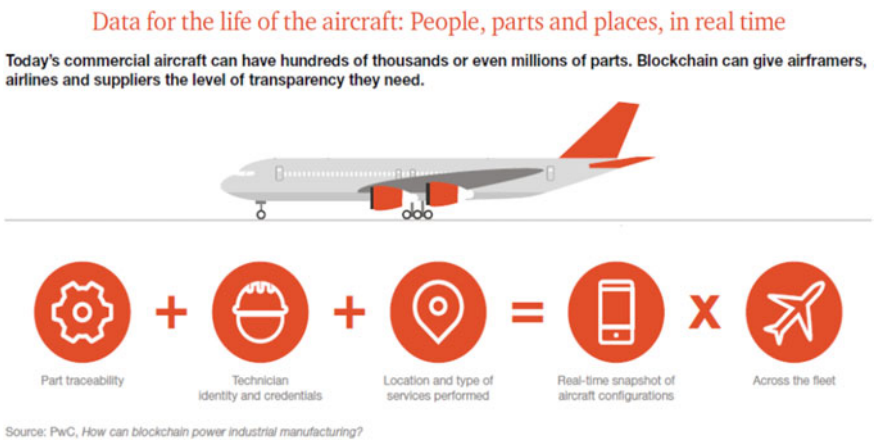


Fig. 4 Data for the life of the aircraft [1]

a huge amount of data is generated by the thousands of sub-units and spread across up to 40 systems (PwC) (Fig. 4).

An accurate maintenance record thus is necessary to evaluate the airworthiness of the aircraft every time it takes off [3]. The blockchain technology can provide a digital birth certificate to the planes as PwC puts it forward, each and every part replaced or serviced, and service records are updated in the automated ledger each time. Unplanned downtime can be minimized to a great extent by blockchain-based smart contract type of arrangement, it will remove the mediating systems and processes to analyze and make a decision for the service by the specialist engineers. It will also reduce the need for a routine check that may not be needed but is done as a protocol to avoid failures.

1.2 Blockchain and Airlines

The International Air Transport Association (IATA) is the trade organization of global aviation industry that governs and facilitates the commercial standards on which the airlines operate and controls almost 82% of the global airline traffic [1]. The IATA has been actively involved in adaptation of blockchain technology in the industry. IATA has advised the airlines to consider adapting to blockchain at a priority for various activities like purchasing and decision making to supply chain flows, aircraft routing, financial relationships with partners, and movements of people through airports [2]. As IATA integrates many stakeholders in the industry, e.g., aircraft manufacturers, airports, ground staff, airlines, travel agents, F&B suppliers, etc., blockchain-based smart contracts can help in real-time settlement of the payments and can reduce possibilities of misinformation and identification of the defecting party. IATA has

been advising the stakeholders to actively use blockchain technology for controlling supply chain, flight routes, and monetary transactions with partners.

These directives are supported by some of the initiatives taken by IATA, e.g., the IATA Coin which is like the bitcoin is a superannuation currency owned by the airlines [3]. The IATA Coin has thus facilitated blockchain-based transaction and at the same time have taken away the possibility of frauds by outsiders by creating their own blockchain in the which the miner nodes are various stakeholders [4]. The previous billing and settlement plan (BSP) system has been replaced by the new IATA Settlement Systems, in which the IATA Clearing House plays the role of the central bank in the earlier system. More efforts are being done to bring other stakeholders at the same level of blockchain technology usage, e.g., IATA digital certification authority has started to issue certifications using Smart contracts, the Digital certification authority (DCA) has adopted blockchain and AI for ID management of passengers, agents, airlines and other OTAs; the Travel Grid is perhaps the most ambitious step toward bringing in transparency, access to all the information regarding industry activities and ensuring safety and authorized access only by leveraging upon block chain technology.

1.3 Blockchain and Airports

Airports play a very important role in air travel. Airports are necessary for uploading the cargo and for the passengers to board and deboard the plane. All this needs to be fool proof without errors and with utmost security. The Airports Council International (ACI) suggests that digital transformation is the key to a seamless flow of activities and passengers at the airports. The digital transformation should integrate various systems, protocols and processes, services by bringing together the partners, airlines, security staff, customs department, ground staff, tour operators, and travel agents. The scope of transformation is thus very broad encompassing all airport activities and perhaps the entire operational and financial activities and in fact should be seen as a transformative business strategy. The technology-enabled information systems can help in lowering the operational costs, increasing the use of resources by better optimization, and reducing the buffers, preventing fail points and thus improving the overall economics of the airports. The long-standing techniques like overbooking and queuing that often cause inconvenience to the travelers can be reduced by real-time, accurate, and easily verifiable information by the user nodes.

In late 2018, SITA Lab came up with their ambitious project FlightChain, it was a test project carried out in collaboration with British Airways and London Heathrow Airport, Geneva Airport, and Miami Airport. The project leveraged on the integration of robotics, artificial intelligence, and IoT to provide a real time and single version of the data to the airlines facilitated by a private permissioned blockchain, implemented on both Ethereum and Hyperledger Fabric. Figure 5, FlightChain Project can help us to understand how blockchain can integrate the stakeholders and provide real-time data about the flights and the airport. To understand how things will work, one can

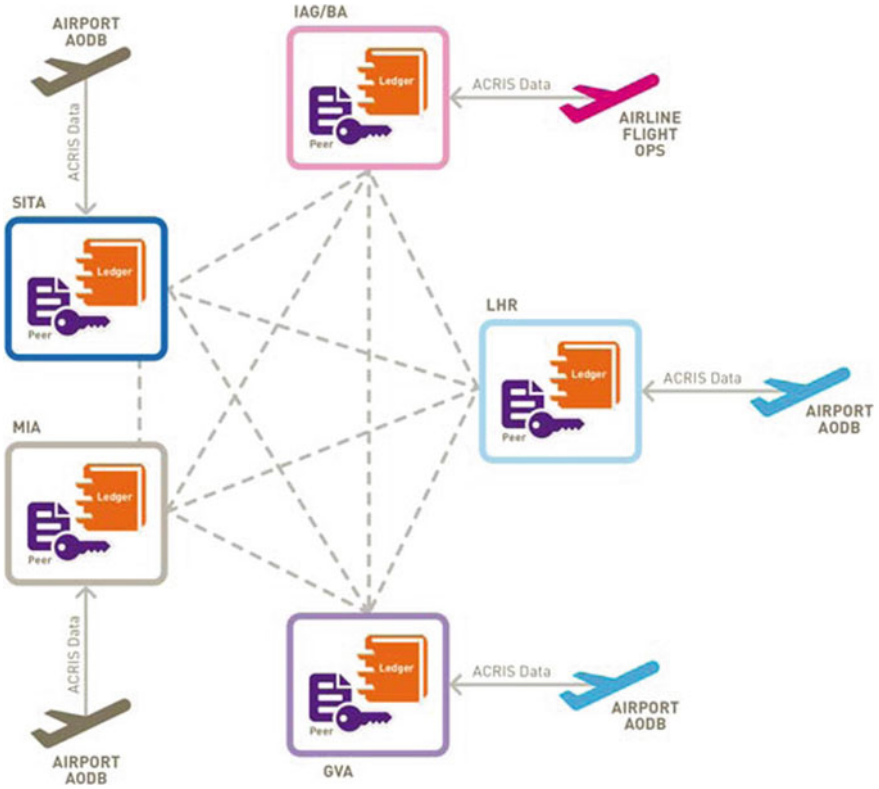


Fig. 5 FlightChain project conceptual overview [5]

imagine more and more participating airlines and airports added to the blockchain if the participants agree to be a part.

1.4 Intra-Industry Payments and Settlement of Accounts

The airline industry around 1970s came up with global distribution system (GDS) that was used to connect individual computerized reservation systems (CRS) to enable real-time tracking of available seats with multiple carriers on each route. When a GDS member travel agent using either Sabre, Amadeus, or Galileo they can get aggregated information about the seat availability, fare rules, and flight scheduling and routing details as per the request. If the passenger agrees a passenger name record can be created in his/her behalf by the agent as per the price and service fee. Even though GDS seems robust but the current market situation where economy class carriers operate on very thin profit margins GDS subscription is a huge burden. GDS though is a robust and secure system but fails to provide much flexibility to find price

breakdowns on the fare or allow second bidding if a consumer is willing to pay a higher price. Another challenge is faced by the airlines who lose the control on their product, airlines are never sure that through which channel GDS will display a seat on their plane and thus can't do much to help their loyal customers when they need the seat most, further the billing and settlement plan provided by IATA again comes at a price and many airlines have no choice but to subscribe to IATA's BSP as it is impossible to get into tie-ups with travel agents all over the globe. A blockchain-based smart contract system can reduce all these problems for the industry be it providing real-time information or real-time payments without compromising the data and channel security. In addition, the data transfer and revenue sharing for codeshare flights and other alliances would be far more convenient and secure.

1.5 Frequent Flyer Programs (FFPs)

Frequent flyer program is a benchmark relationship management program in the airline industry. Whenever a passenger completes a journey with the airlines their membership account is credited with the flyer points or frequent flyer miles. These points then can be redeemed for various merchandise gifts or for another flight or hotel stay. To make these reward points more appealing to the flyers the airlines have tie ups with multiple banks, hotels, merchandisers, credit card companies and other travel businesses, etc. Very often the authentication of the customers and buying back of the miles by the airlines from the partner (such as alliance carriers, credit card issuers, and retailers) where the miles were redeemed by the flyer is a tedious time-consuming process and comes at a huge administrative cost for the process and leaves a room for frauds. Authentication if is not real-time would either make the flyer frustrated or will leave a room for fraud if the airlines agree to buy back miles as reported by the partner. Blockchain can resolve all these issues by making the information readily available with the partners, airlines, and the flyer.

1.6 PNR and Other Records

Airlines have a responsibility to store and transfer the passenger data and prevent the frauds. The passenger's name record or PNR data is collected by the airlines for their operational purposes. The format is provided by the GDS to the travel agent creating the PNR; the details line the itinerary, fare conditions, service requests, and billing information is usually recorded along with the demographic information of the passenger like name, age, nationality, date-of-birth, passport number, credit card, emergency numbers, etc. Often airlines have the onus to border organizations, immigration office, etc., who may need the data in some other format and may have more variables to be added in the database about the traveler. A trusted network based on blockchain technology again can solve such challenges of repeated transfer

of information pieces, cumbersome authentications, and delays that may result in a passenger sitting and waiting in the lounge to get a clearance from the border checks or other government bodies. Medical records, COVID test report verification, vaccination record verification, and many more such contingencies can also be easily managed if the participants are added to the blockchain.

2 Conclusion

The future of aviation industry's progress lies with the blockchain-based systems. As the stakeholders in industry are gearing up there are some examples of first adopters of the technology, e.g., airport collaborative decision making (A-CDM) at Napoli-Capodichino Airport in Italy (Fig. 6).

The blockchain technology has found its applications and acceptance in aviation industry and with time the applications are extending. The major applications that are evident from various sources can be summarized into the flowing heads.

Secured data records: Aviation maintenance records are very crucial to prevent failures in future and reduce the maintenance cost of the aircrafts. Any error in maintaining the previous records of errors, symptoms of failure of some parts need to be properly maintained to do a timely maintenance and save any mishappening

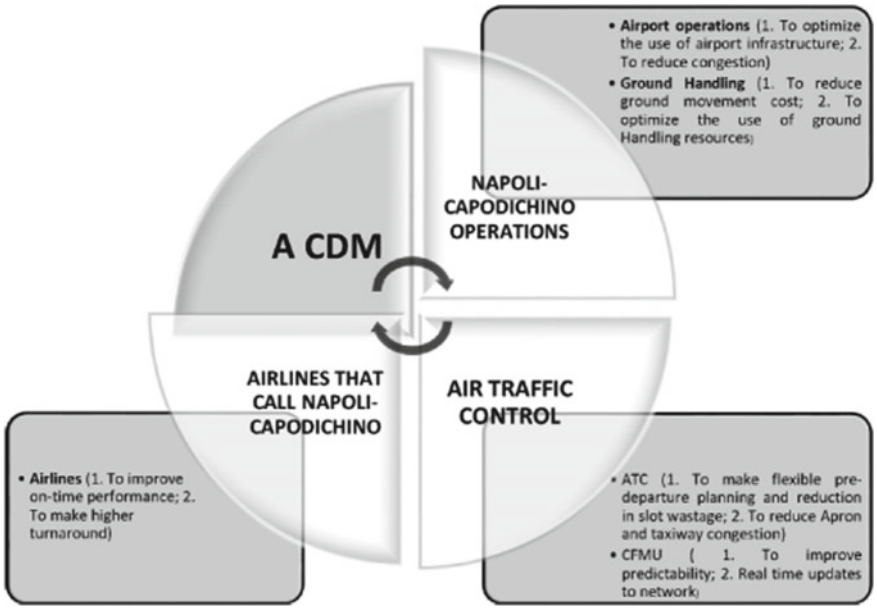


Fig. 6 Airport Collaborative Decision Making System (A-CDM) at Napoli-Capodichino Airport [6]

mid-air. Blockchain creates a provision to store and transfer data and the remains uncompromised even if the data size is huge, it does not just prevents the chances of data manipulation or corruption gives an option to quickly find the fail point by checking the modified hashing as well as recovering the data from previous nodes. The same applies for the day-to-day operations like passenger recordkeeping and transfer, flight operations data like codeshares and luggage transfers, and settlement of payments and tallying the reward points [7] of consumer to name a few.

Ease of Access of the Data: The amount of data generated by operations of airlines and technical data of the equipment like aircraft, cargo conveyors, automatic aerobridges, signal towers, etc., often results in multiple copies of paper documents and digital files. Blockchain technology can enable easy access of the information by many end users like ground staff, managers, service personnel, and passengers; the information can be accessed by searching public or private blockchains within seconds.

Easy of data analysis and timely decisions: It is a tedious task to maintain the history of an aircraft, recording aircraft's data in a blockchain will create a participative environment for various stakeholders, the unstructured information can be easily transformed into easy to interpret systematic information. This will highly reduce the need of audit by some specialist agency, and in case of audits, the relevant and accurate information will be easy to retrieve from the system.

Transparency and confidentiality go hand-in-hand: A decentralized agency as we envision for future will bring together various parties and institutions, e.g., aviation authorities IATA, ICAO, and others which ensure that the fleet of aircrafts is properly managed, airports are properly maintained and operated. As there is no room for hiding poor performance this will give a great push to the workers and managers to ensure that the activities are properly functioning and will create an environment to up their services and guest experience. More transparency can be maintained if the aircraft fleet maintenance and operational data is shared with the partners and stakeholders and will ensure better quality services in the longer run, safer flights, and more customers. The data transparency creates more trust and at the same time the sensitivity and exclusivity can be maintained due to encryption and consensus protocols will ensure access based on rights assigned to role of the member.

Reliability of the data: One of the most important features of a blockchain system is the reliability of the data. The data that is received can be easily verified for authenticity. This builds transparency in the entire system in the longer run and minimizes the cases of defection.

References

1. PwC Data for the life of an Aircraft. https://www.pwc.com/gx/en/industries/aerospace-defence/publications/blockchain-in-aerospace.html. Accessed on 21/03/2021

2. Blockchain in Aviation White Paper, IATA: October 2018, available at https://www.iata.org/contentassets/965ffb686aa54cfaba93fce9f35edb80/blockchain-in-aviation-white-paper.pdf
3. A.G. Andrei, R. Balasa, M.I. Costea, A. Semenescu, Building a blockchain for aviation maintenance records. J. Phys.: Conf. Ser. **1781**(1), 012067. IOP Publishing (2021, February)
4. K. To, *Reimagining the Future of Aviation with Blockchain* (Doctoral dissertation, Ph. D. dissertation, Stern School of Business New York) (2020)
5. Research into the Usability and Practicalities of Blockchain Technology for the Air Transport Industry. https://www.sita.aero/globalassets/docs/white-papers/flightchain-whitepaper.pdf
6. A. Di Vaio, L. Varriale, Blockchain technology in supply chain management for sustainable performance: evidence from the airport industry. Int. J. Information Manage. **52**, 102014 (2020)
7. International Air Transport Association, *Blockchain in Aviation: Exploring the Fundamentals, Uses Cases, and Industry Initiatives* (2018)

Diabetes Mellitus Prediction Using Ensemble Learning Approach with Hyperparameterization



Rashmi Srivastava and Rajendra Kumar Dwivedi

Abstract In today's world, the food you take in your body is not as healthy as it should be. Our body takes energy from the food, and there are some use cases where our body prevents this system by not properly consuming energy from the food we eat. The main disease that arises from this condition is diabetes mellitus. This disease is a silent killer that makes our body weaker by producing less insulin which is important. As diabetes is a chronic disease, it would be more dangerous in extreme cases. It has attracted the research area a lot. Machine learning schemes help in predicting this disease. Therefore, we devised a machine learning-based scheme for diabetes prediction. Missing features need to be found, then only the correlation will be better to other segments of the body. We must compensate for missing values in the dataset by allowing some algorithm to predict them. So, we used an algorithm, viz., naive Bayes to balance the dataset class and reduce the class imbalance factor. Then, we performed classification using an RF classifier. Our proposed work speeds up the execution time by introducing the algorithm of ensemble learning techniques like hyperparameter optimization. Here, we used RandomsearchCV. We used the best estimator like the XGBoost algorithm which increases the speed of execution and, thus, the performance. We used the PIMA dataset (PIMA Indian diabetes dataset) from California University and UCI (Irvine) repository for testing our scheme.

Keywords Diabetes · Deep learning · Machine learning (ML) · Artificial intelligence (AI) · Disease prediction · Feature selection · Health care

1 Introduction

Diabetes mellitus has developed into diseases that are under a metabolic disorder and identified by maximum blood level of sugar. Diabetes mellitus is just like a cluster of diseases that results in an amount of blood sugar exceeds to the significant level. Diabetes disease is mainly caused due to insulin shortfall in the blood, so this shortage is originated from the loss of insulin-produced beta cells in the pancreas.

R. Srivastava (✉) · R. K. Dwivedi
Department of IT & CA MMMUT, Uttar Pradesh, Gorakhpur, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_47

The pancreas is the highest important organ of the body of a human, and it produced insulin affects the metabolism of sugar/fat/protein in daily life energies. There are some additional things in case of diabetes mellitus like it also promotes various skin and another type of infection which reduces the immunity of blood cells because of their inability for soaking glucose. But, by following a healthy lifestyle, regular checkups, proper medication, we can stop its early threatening effects. As we know, in the industry of health care, millions of data, metadata generated like medical records, diagnose data, then it will be converted into a large knowledge which will bring better decision-making support and also reduces the cost. In todays' real-world scenario, many phases of diabetes can be predicted and also can be diagnosed via ML/AI techniques. Likewise, prediction is the first step for any chronic disease. So, the approach is based on clinical data and genetic data, and algorithms can predict the risk of occurrence of diabetes. Machine learning schemes are very helpful for predicting the information from a dataset [1–4].

2 Related Work

To find a solution to the diabetes prediction problem, we have to review all previously done works to give more effective solutions. So, this part of the paper is reviewing all related works (Table 1).

Zhang et al. [5] proposed a technique that uses classification and regression trees (CART's) applied to tackle the problem. Producing a decision tree positioned on datasets of training as well as optimization-regression tree is excluded accordingly. Kumar et al. [6] suggested a system in which machine techniques are used to classify the patients' risk level of diabetes. Sneha et al. [7] a prediction algorithm is designed by machine learning as well as search for the optimal classifier producing the adjacent results. Predictive analysis shows that the decision tree algorithm, as well as random forest, has maximum specificity of 98.20 and 98.00%, reciprocally for prediction. Liu et al. [8] have given an idea to use fuzzy logic for predictions which solves the quality problem of data of train by making synthetic specimen for minority class by using weighting and recovery stepping procedure.

Akash et al. [9] proposed an idea to use multiple dimensions study of the structured as well as unstructured data in medical fields that increase the assessment of prediction of diseases in region-specific context. Ashiquzzaman et al. [10] have given a system of prediction which applies overfitting of data in the predictive model as a dropdown technique. Yahyaoui et al. [11] given a system in which provisional analysis of machine learning, as well as deep learning-relied algorithms for predicting diabetes, is given. Among random forest, SVM, deep learning, random forest performs the best among all three also used.

Table 1 A comparative study of existing schemes

References	Authors	Techniques of ml used for diabetes detection	Accuracy/other parameters	Remarks
[5]	Zhang et al. (2018)	SVM	78%	Prediction of blood press
[6]	Kumar and Umatejaswi (2017)	KNN	78.16%	-
[7]	Sneha and Gangil (2019)	Decision tree, random forest, SVM, and NB	DT (98.00%), RF (98.02%), SVM (77.73), and NB (82.30%)	Able to map the features from low to high dimensions
[8]	Liu et al. (2017)	Fuzzy logic	64.44%	–
[9]	Jamgade and Zade (2019)	K-mean	95%	Observing both structured and unstructured data
[10]	Ashiquzzaman et al. (2018)	A novel form of deep neural network	88.41%	–
[11]	Yahyaou e al. (2019)	SVM, DL, and RF	83.67%	–
[12]	Hasan et al. (2019)	Ensemble learning (AB + XB) MODEL	95.0%	AB- AdaBoost XB- XGBoost

3 Proposed Approach

In our approach, supervised learning is included here. The report of prediction of diabetes from last all references (Table 1) shows that in the datasets samples are not evenly distributed and not also having the accurate and real values, but containing the null values with various null values. It enables a large no. of circumstances that slow down the process of prediction. The flow of my work is like to have in the steps basically including preprocessing and correlation, then ml algorithm applied based on the demand of output that we have then apply ensemble technique along with the best estimator also using boost using a hyperparametric approach. After this use, the cross-validation to validate results and then analysis of performance will be done.

My idea is to change the machine learning algorithm type and infuse the estimator that will give the different better results than previous ones. We have done the preprocessing on these datasets, and afterward, some feature engineering have been done, for example, like firstly check whether any null value is present or not. Then, finding the correlation between fields by using Seaborn library and heatmap to show the correlation between features. Also, mapping has been used by involving mapping function from changing true/false value to 0/1 value. Then, checking our dataset is balanced or not and then splitting involves here by using train_test_split() in 70:30

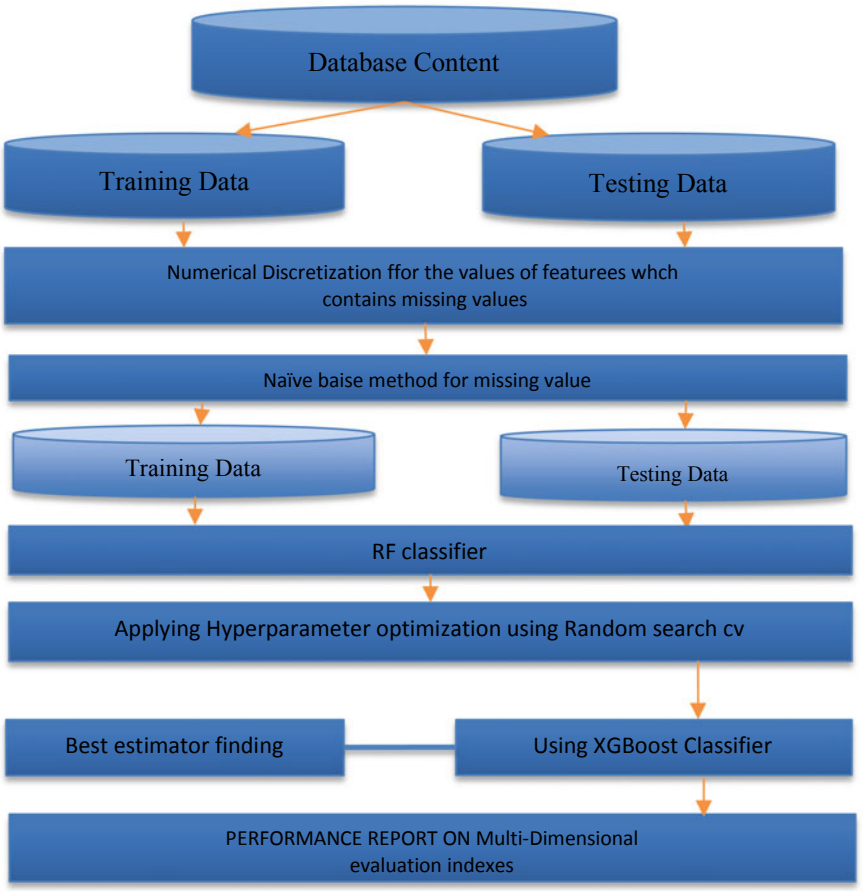


Fig. 1 Working flow of proposal work

ratio. I have also used a timer function which calculated the time means how much time taken by this randomized Search_CV will take and then uses random_search.fit() (Fig. 1).

4 Algorithm Valuation

4.1 Naïve Bayes

NB is a classification-based method [13] that relies on the Bayes theorem following assumptions that each character is not dependent on others. Naïve Bayes classifiers are collections of classification algorithms working on the principles of Bayes

theorem which have a pre-assumption that all the features are independent of each other need of converting continuous var into discrete variables. It works on the Bayes theorem of probability to predict unknown datasets of classes. Taking naïve assumptions as we use here which is independent among the features.

4.2 Random Forest [RF]

Random forest is an ensemble algorithm [11] which is relied on decision tree (DT) methodology. The basic principle is to obtain multiple classification prototypes; here, almost every classifier separably absorbs and makes various predictions. We have used a classification and regression tree. Then, the decision tree is designed as a random forest, for the problem of classification, and the concluding classification results are being estimated by the polling of each n decision tree.

4.3 XGBoost

XGBoost [12] is an open-source library providing a high-performance implementation of gradient boosted decision trees. Here, gradient boosting adds creation and adding decision trees to a step on ensemble modeling method.

5 Performance Evaluation

The proposed work is implemented in Python on PIMA datasets (UCI repository), and performance matrices used here are explained firmly in this section.

A. *Preprocessing of data*
   The idea of the naive Bayes method is to replace null values to mean values. Figure 2 shows the data visualization output mapped by Python's library functions.
B. *Supervised learning approaches to detect diabetes*
   We have used supervised learning approaches for the detection of diabetes data as discussed below. Random forest algorithm is used for classifying the samples having diabetes or non-diabetes characteristics.
C. *Performance measurements*

The parameter used for performance measurements is precision, recall, f1 score, and accuracy. We are using four performance metrics that are based on the confusion matrix.

Precision: It is computed using Eq. 1.

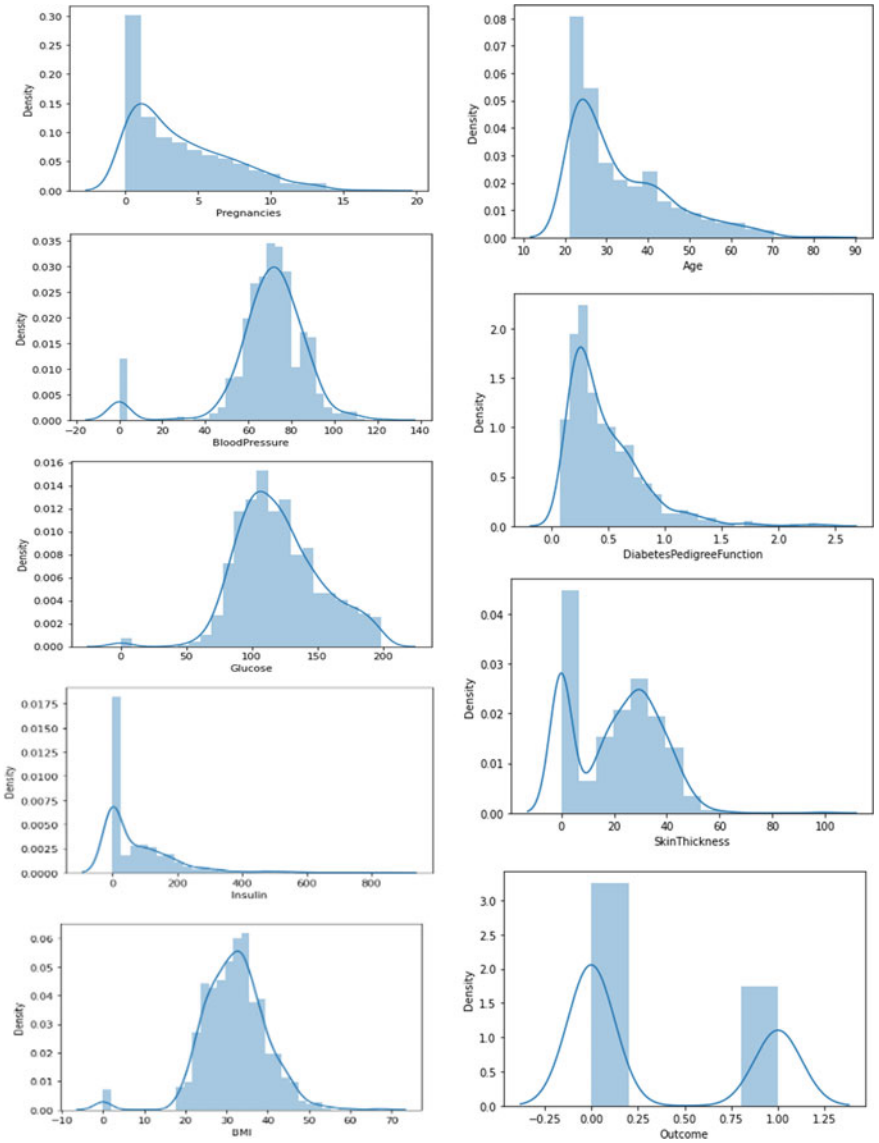


Fig. 2 Graph of dataset's input variation

$$P = \mathrm{TP}/(\mathrm{TP} + \mathrm{FP}) \tag{1}$$

Recall: It is computed using Eq. 2.

$$R = \mathrm{TP}/(\mathrm{TP} + \mathrm{FN}) \tag{2}$$

F1 Score: It is computed using Eq. 3.

$$\mathrm{F1} = 2 * (\mathrm{Precision} * \mathrm{Recall})/(\mathrm{Precision} + \mathrm{Recall}) \tag{3}$$

Accuracy: It is computed using Eq. 4.

$$A = (\mathrm{TP} + \mathrm{TN})/(\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}) \tag{4}$$

Here,
A = accuracy; P = precision; R = recall.
F1 = F1 score; TP = true positive.
TN = true negative; FP = false positive.
FN = false negative.
Our results are calculated based on constructed confusion matrix given below:
where
confusion matrix:

$$\begin{bmatrix} 33 & 14 \\ 13 & 94 \end{bmatrix}$$

Number of true cases (TP) is 268 (34.90%).
Number of false cases (TN) is 500 (65.10%).
Data in training set: test set is 70:30.
Original diabetes true values: false values is 268:500.
Training diabetes true values: false values is 221:393.

6 Conclusion and Future Work

In this paper, we offered an algorithm for diabetes prediction focusing on the null value problem and imbalance property in the dataset along with the data visualizing (Fig. 2) of the patients' records. Our hyperparameterized approach after implementing the classification algorithm on the dataset has given greater accuracy as compared to the existing techniques (Table 2). We have used accuracy, precision, recall, and F1 score for performance evaluation. In the future work, we can enhance

Table 2 Performance metrics

Parameters	NB + RF (%)	NB + RF + XGBOOST (%)
Accuracy	82.5	85.6
Precision	77.4	72.6
F1 score	79.4	80.1
Recall	76.2	79.5

this scheme for predicting other diseases. We can also add time-related modules to this scheme.

References

1. R.K. Dwivedi, R. Kumar, R. Buyya, Gaussian distribution-based machine learning scheme for anomaly detection in healthcare sensor cloud. Int. J. Cloud Appl. Comput. (IJCAC) **11**(1), Article 3, pp. 52–72, IGI Global, January-March (2021)
2. R.K. Dwivedi, A.K. Rai, R. Kumar, A study on machine learning based anomaly detection approaches in wireless sensor network, in *10th IEEE International Conference on Cloud Computing, Data Science & Engineering (Confluence-2020)* (Amity University Noida, Jan 29–31, 2020), pp. 200–205. https://doi.org/10.1109/Confluence47617.2020.9058311
3. R.K. Dwivedi, A.K. Rai, R. Kumar, Outlier detection in wireless sensor networks using machine learning techniques: a survey, in *IEEE International Conference on Electrical and Electronics Engineering (ICE3–2020)*, organized by MMMUT Gorakhpur and North Dakota State University, Fargo, USA, at MMMUT Gorakhpur, Feb 14–15 (2020), pp. 316–321. https://doi.org/10.1109/ICE348803.2020.9122865
4. R.K. Dwivedi, S. Pandey, R. Kumar, A study on machine learning approaches for outlier detection in wireless sensor network, in *Proceeding of 2018 8th IEEE International Conference on Cloud Computing, Data Science & Engineering–Confluence* (ISBN 978–1–5386–1718–2), held at Amity University, Noida, India, pp. 189–192, Jan 11–12 (2018). https://doi.org/10.1109/CONFLUENCE.2018.8442992
5. B. Zhang, Z. Wei, J. Ren et al., An empirical study on predicting blood pressure using classification and regression trees. IEEE Access **6**, 21758–21768 (2018)
6. P.S. Kumar, V. Umatejaswi, Diagnosing diabetes using data mining techniques. Int. J. Sci. Res. Publ. **7**, 705–709 (2017)
7. M. Zeng, B. Zou, F. Wei, X. Liu, L. Wang, Effective prediction of three common diseases by combining SMOTE with Tomek links technique for imbalanced medical data, in *2016 IEEE International Conference of Online Analysis and Computing Science (ICOACS)*, Chongqing (2016), pp. 225–228. https://doi.org/10.1109/ICOACS.2016.7563084
8. S. Liu, J. Zhang, Y. Xiang, et al., Fuzzy-based information decomposition for incomplete and imbalanced data learning. IEEE Trans. Fuzzy Syst. **25**(6), 1476–1490 (2017)
9. A.C. Jamgade, S.D. Zade, *Disease Prediction Using Machine Learning* (2019). e-ISSN: 2395-0056
10. A. Ashiquzzaman et al., Reduction of overfitting in diabetes prediction using deep learning neural network, in *IT Convergence and Security 2017*, ed. by K. Kim, H. Kim, N. Baek. Lecture Notes in Electrical Engineering, vol. 449 (Springer, Singapore, 2018). https://doi.org/10.1007/978-981-10-6451-7_5
11. A. Yahyaoui, A. Jamil, J. Rasheed, M. Yesiltepe,A decision support system for diabetes prediction using machine learning and deep learning techniques, in *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, Ankara, Turkey (2019), pp. 1–4. https://doi.org/10.1109/UBMYK48245.2019.8965556
12. M.K. Hasan, M.A. Alam, D. Das, E. Hossain, M. Hasan, Diabetes prediction using ensembling of different machine learning classifiers. IEEE Access **8**, 76516–76531 (2020). https://doi.org/10.1109/ACCESS.2020.2989857
13. N. Sneha, T. Gangil, Analysis of diabetes mellitus for early prediction using optimal features selection. J. Big Data **6**, 13 (2019). https://doi.org/10.1186/s40537-019-0175-6

Fairness, Accountability, Sustainability, Transparency (FAST) of Artificial Intelligence in Terms of Hospitality Industry



Sunil Sharma, Yashwant Singh Rawal, Sanjeeb Pal, and Rakesh Dani

Abstract Artificial intelligence (AI) is playing very significant role in every domain of life and spreading widely all across the globe. It covers all major fields like automation, hospitality industries, medical sectors, technology industry, and defense services. AI assists the painstaking development of data compilation which is a fundamental element of AI expansion. Since, all are using AI without knowing much about the ethics and fairness of AI and using it only as per their requirements. AI ethics is a set of values, principles, and techniques that utilize generally established values of accurate and inaccurate to direct ethical behavior in the expansion and use of AI technologies. The Organization for Economic Co-operation and Development (OECD) principles on AI introduced to encourage artificial intelligence that is pioneering and reliable and respects human rights and ethical values. Here, in this paper, it is tried to demonstrate FAST track principles, i.e., fairness, accountability, sustainability, and transparency along with OECD. These principles will also can be utilized when we are using this technology in hospitality industry. During the international pandemic situation (COVID-19) when everyone used to avoid stay and visits to hotels and restaurants, AI and some other technologies make it possible to provide safe and hygienic stay to the customers. Here, in this paper, we also cover the benefits and advantages of AI in this domain.

Keywords Artificial ıntelligence · FAST principle · OECD · Hospitality · Ethics

1 Introduction

With the initiation of digital era, artificial intelligence (AI) [1] indubitably seen a spectacular revolution [2] in the background of technology, industry, defense services,

S. Sharma (✉)
Faculty of Engineering, Pacific University, Rajasthan, Udaipur, India

Y. S. Rawal · S. Pal
Amity School of Hospitality, Amity University, Rajasthan, Jaipur, India

R. Dani
Graphic Era Deemed to be University, Dehradun, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_48

and medication processes. Artificial intelligence (AI) was initially commenced in 1955; the magnificent progression of deep learning [3] has transferred the domain of AI from hypothetical studies [4] of science and technology to the extension of realistic functions like astronomic observations [5], drug design, medicinal imaging, flow cytometry, distributed sensing, speech recognition, hospitality industry finance, and advertising [6].

2 AI Ethics

An astonishing era of mankind undertake has been usher by the omnipresence of the ever-expanding accessibility of big data [7], the elevated pace and widen of cloud computing [8] proposal, and the encroachment of progressively more difficult machine learning (ML) algorithms [9]. The outlook of improvement in AI will facilitate humankind to face up to a few of its mainly critical challenges is exhilarating, but justifiable doubts still propagate [10]. AI is no exception.

AI ethics extensively acknowledged principles of true and false to show ethical behavior in the improvement and utilize of AI [11].

Ethical proposal as an accountable deliverance of an AI system

Edifying a project deliverance environment [PDE] [12] facilitates the ethical intend [13] and exploitation of AI systems and involves an effort of multidisciplinary teams [14]. There is a requirement of active collaboration of every participant's from the team in both, i.e., sustaining an intensely embedded ethnicity [15] and in accomplishing ascendancy planning at every point in the improvement and execution of life cycle.

3 The FAST Track Principles

The FAST track principles [16], i.e., fairness, accountability, sustainability, and transparency will be used as better support to a responsible environment (Fig. 1).

All the connected terms are related with the ant delivery system [ADS] [17].

3.1 Fairness

AI systems and technologies are designed and produced for human beings by human beings [18]. Due to data extraction, collection, and pre-processing human inaccuracy, unfairness, and misjudgment can enter into the innovation life cycle [19–21]. Fairness observations play an essential role in customers' behavior [22]. Characterization of different design and use of AI systems are shown in Fig. 2.

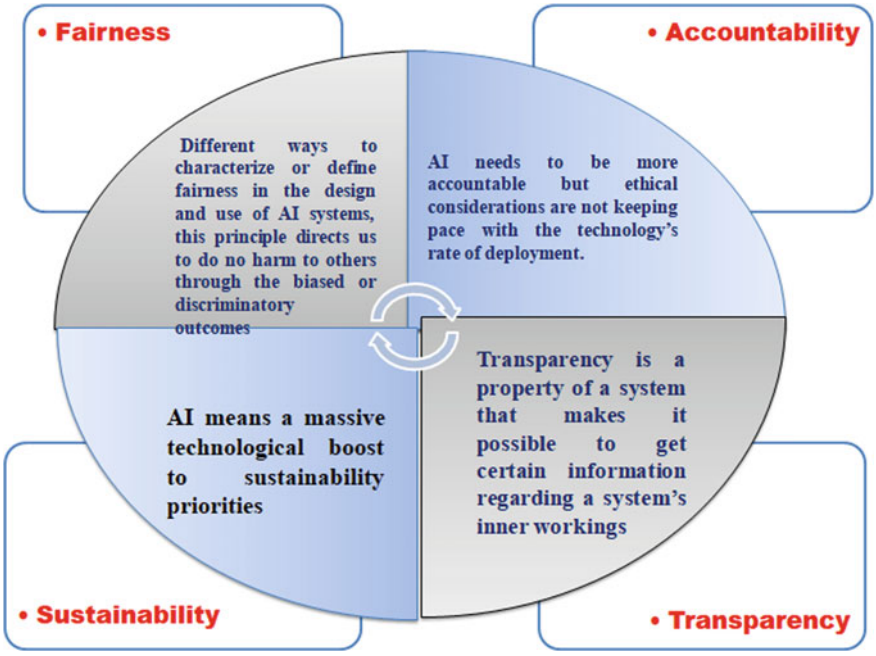


Fig. 1 FAST principle [17]

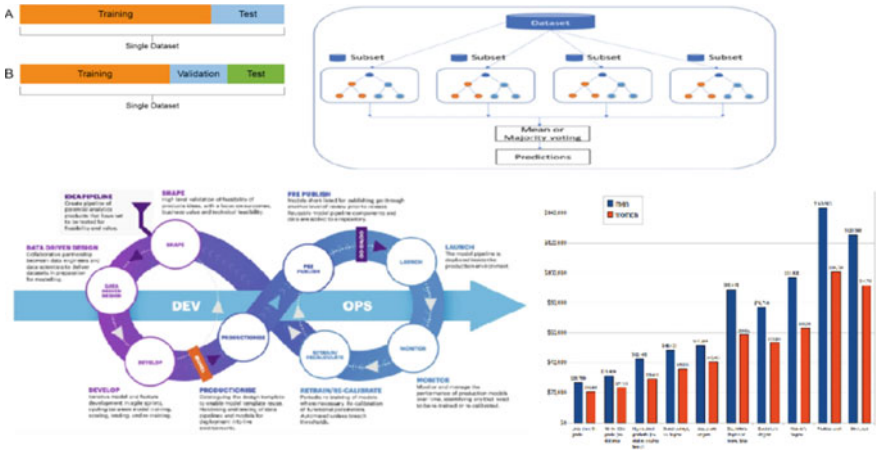


Fig. 2 AI ınnovations [23]



Fig. 3 AI-driven systems [30]

3.2 *Accountability*

Since roles and responsibilities of ethical considerations [24] are not keeping pace with technology's rate of deployment, so AI needs to be more accountable [25]. This is only because of "black box" identity [26] of AI, because without this is impossible to determine why and how an AI makes the decisions [27]. Similar to AI accountability, hospitality [28] sector also needs accountability from each and every staff members who is associated with it. Every enterprise possesses an organization structures [29] in which they are free to ensure for every promised product or service [30] and acknowledged as accountable for the release of the products or services.

Building accountability in AI-driven systems

See Fig. 3.

3.3 *Sustainability*

The AI sustainability center and metric stream [31] are jointly offering an automated tool for risk scanning [32] of data and AI solutions. We are combining the metric stream cloud-based governance, risk management, and compliance platform, and AI allows organizations to effectively gain insights into their use of AI and data-driven solutions [33]. AI means a substantial hi-tech boost up to sustainability precedence (Fig. 4).

Hotels and other hospitality sectors are gradually intriguing more established approach that integrates socially accountable observes toward sustainability [34].

AI unlocks opportunities for major sustainability progress

AI is serving the next generation of business to ease their ecological and social impact [35] by improving effectiveness and emergent innovative products [35].

3.4 *Transparency*

Transparency is a property of a system [36] that makes it possible to get certain information regarding a system's inner workings. Transparency itself is ethically neutral [37] and is not an ethical concept. Transparency is something that can manifest in many different ways, and something that can present a solution for underlying ethical questions [38]. In this sense, transparency is relevant at least to the three following issues (Fig. 5).

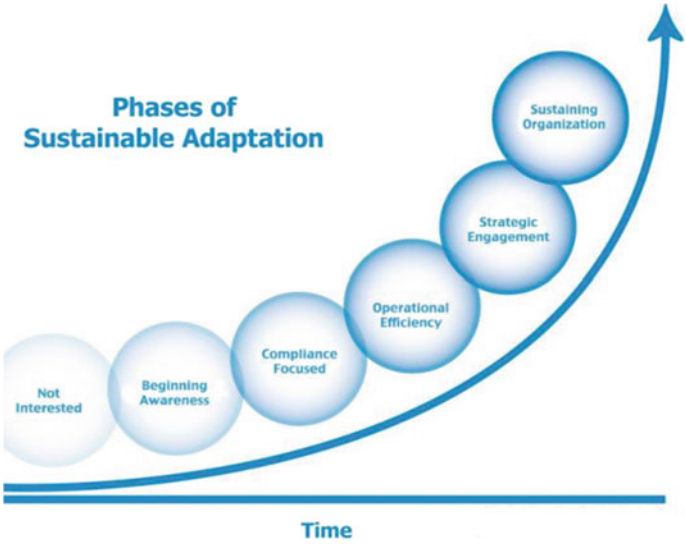


Fig. 4 Sustainability in AI [33]

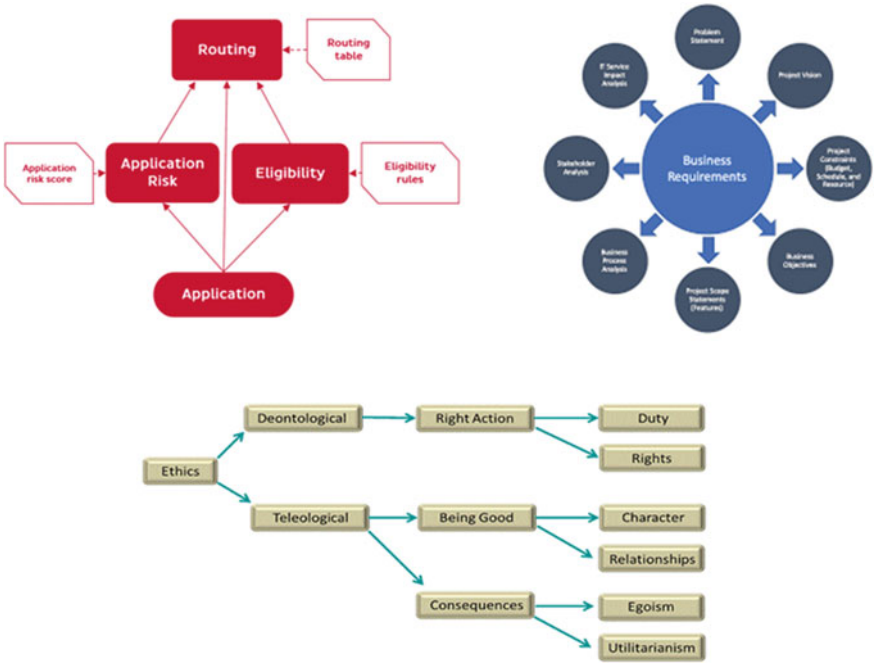


Fig. 5 Transparencies in AI [38]

In hospitality, it stands to courage new practice and to permit one's self to be susceptible. It is more concerning with perspective and dropping ambiguity [39].

4 Role of AI in Hospitality Industry

Perfectly aligned customer services [40] can be used as essential element. It includes (Fig. 6).

4.1 AI and Hospitality Sector

Since 2018, AI's capabilities to advance the communication flow between customers and hoteliers [41] inside the hotels have modernized the interactions among them. It is noted down that the future of hotels will be more beneficial if hotel personnel completely adopted AI chatbot [42] services (Fig. 7).

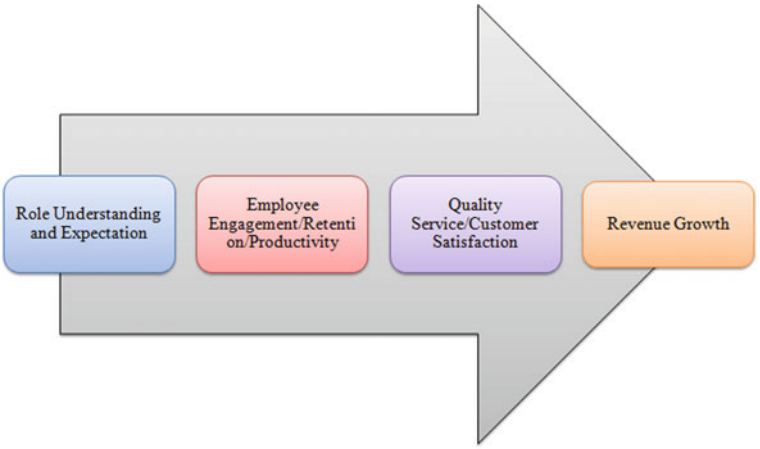


Fig. 6 AI roles in hospitality



Fig. 7 AI and hospitality [42]

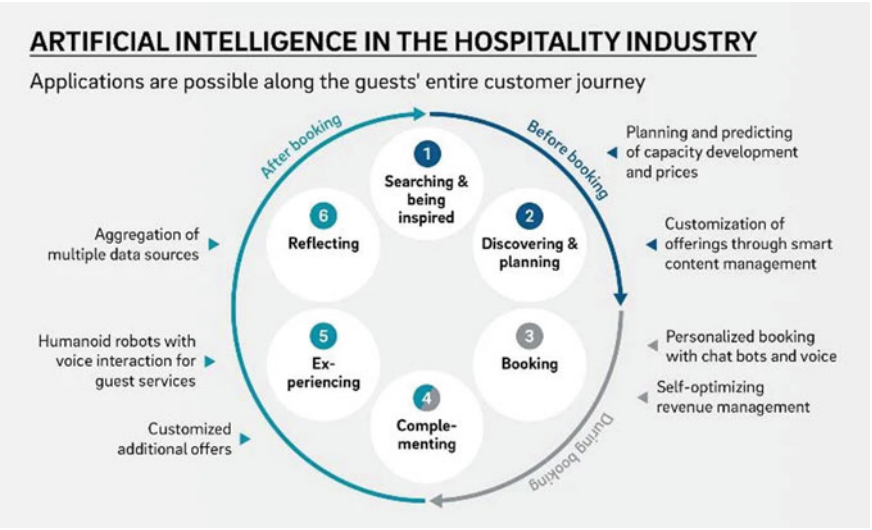


Fig. 8 Technological trends in hospitality sector [43]

In terms of hospitality industry, artificial intelligence could help to compel a cutting edge [42] of innovative prospect. Hotel industries need to improve their work toward a series of sentiment and enclose a widespread approach so as to conclude the consequence of explicit services on regulars [43] (Fig. 8).

Very well-defined set of AI ethics disseminated by the "OECD" can be fashioned into FAST track alternates.

5 Conclusion

AI ethics have been prominently used, but we need to wait to see how these can be involved in AI-adopted fields. Every end-users need to follow these AI ethics and AST track principles before adopting them in their utilities. Keeping so much stress to beat the rivalry in rigid targets and hotels transversely, the sphere will necessitate significant scientific improvements to survive with escalating stipulate. Hoteliers must espouse the inventive synthesis of AI and fused service devices to renovate their space and redefine contemporary service standards. AI FAST track principles with OECD are enhancing the use of these ethics to increase the role of AI in every domain. It is moderately apparent that by assimilating artificial intelligence with hospitality, we can observe elementary redefinition of an incomparable customer services. It is concluded that AI along with its ethics and principles can enhance the outcomes in each industry. If it comes to hospitality, then it plays a significant role to provide unmatched customer services and provide proper hygienic conditions during

worst situations/pandemic like COVID-19 also. In fact, they are satisfying customers need, while they are alone and far away from their loved ones.

References

1. J. Buolamwini, T. Gebru, Gender shades: ıntersectional accuracy disparities in commercial gender classification, in *Conference on Fairness, Accountability, and Transparency*, New York, NY, February (2018)
2. N. Madaan, S. Mehta, T. Agrawaal, V. Malhotra, A. Aggarwal, Y. Gupta, M. Saxena, Analyze, detect and remove gender stereotyping from bollywood movies, in *Conference on Fairness, Accountability, and Transparency*, New York, NY, February (2018)
3. B. Srivastava, F. Rossi, Towards composable bias rating of AI services, in *AAAI/ACM Conference on Artificial Intelligence, Ethics, and Society*, New Orleans, LA, February (2018)
4. F.P. Calmon, D. Wei, B. Vinzamuri, K.N. Ramamurty, K.R. Varshney, Optimized pre-processing for discrimination prevention, in *Advances in Neural Information Processing Systems*, Long Beach, CA, December (2017)
5. S. Shaikh, H. Vishwakarma, S. Mehta, K.R. Varshney, K.N. Ramamurthy, D. Wei, An end-to-end machine learning pipeline that ensures fairness policies, in *Data for Good Exchange Conference*, New York, NY, September (2017)
6. J. McCarthy, *Programs with Common Sense* (RLE and MIT Computation Center, 1960)
7. N. Bostrom, Ethical issues in advanced artificial intelligence, in *Science Fiction and Philosophy: From Time Travel to Superintelligence* (2003), pp. 277–284
8. D. Amodei, C. Olah, J. Steinhardt, P. Christiano, J. Schulman, D. Man´e, *Concrete Problems in AI Safety*. arXiv preprint arXiv:1606.06565 (2016)
9. D. Sculley, T. Phillips, D. Ebner, V. Chaudhary, M. Young, *Machine Learning: The High-İnterest Credit Card of Technical Debt* (2014)
10. B. Goodman, S. Flaxman, EU regulations on algorithmic decision-making and a 'right to explanation', in *ICML Workshop on Human İnterpretability in Machine Learning (WHI 2016)*, vol. 1, New York, NY (2016). http://arxiv.org/abs/1606.08813
11. S. Wachter, B. Mittelstadt, L. Floridi, Why a right to explanation of automated decision-making does not exist in the general data protection regulation. Int. Data Privacy Law **7**(2), 76–99 (2017)
12. L.A. Ray, H. Nicponski, Face Detecting Camera and Method, September 6 (2005). US Patent 6,940,545
13. V. Alexander, C. Blinder, P.J. Zak, Why trust an algorithm? Performance, cognition, and neurophysiology. Comput. Hum. Behav. **89**, 279–288 (2018). https://doi.org/10.1016/j.chb.2018.07.026
14. Y.E. Bigman, K. Gray, People are averse to machines making moral decisions. Cognition **181**, 21–34 (2018). https://doi.org/10.1016/j.cognition.2018.08.003
15. T. Hagendorff, Maschinelles Lernen und Diskriminierung: Probleme und Lösungsansätze. Österreichische Zeitschrift für Soziologie **44**(1), 53–66 (2019)
16. T. Hagendorff, The ethics of AI ethics. *An Evaluation of Guidelines', Minds and Machines*, pp. 1–22 [Online] (2020). Available at https://arxiv.org/pdf/1903.03425.pdf. Accessed 03 Mar 2020
17. M. Haenlein, A. Kaplan, A brief history of artificial ıntelligence: on the past, present, and future of artificial ıntelligence. California Manage. Rev. (2019)
18. J. Schmidhuber, Deep learning in neural networks: an overview. Neural Netw. **61**, 85–117 (2015)
19. D. Silver et al., Mastering the game of Go without human knowledge. Nature **550**(7676), 354–359 (2017)
20. D. Silver et al., A general reinforcement learning algorithm that masters chess, shogi, and go through self-play (2018)

21. Y. Shoham et al., *The AI Index 2018 Annual Report, AI Index Steering Committee, Human-Centered AI Initiative* (Stanford University, Stanford, CA, 2018)
22. R. Hamon, H. Junklewitz, I. Sanchez, Robustness and explainability of artificial ıntelligence—from technical topolicy solutions, EUR 30040, Publications Office of the European Union, Luxembourg, Luxembourg (2020). ISBN 978-92-79-14660-5(online). https://doi.org/10.2760/57493 (online), JRC119336
23. K. Gade, S.C. Geyik, K. Kenthapadi, V. Mithal, A. Taly, Explainable AI in industry, in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (2019). https://doi.org/10.1145/3292500.3332281
24. P. Saleiro, K.T. Rodolfa, R. Ghani, Dealing with bias and fairness in data science systems, in *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (2020). https://doi.org/10.1145/3394486.3406708
25. S. Sharma, Y.S. Rawal, The possibilities of artificial ıntelligence in the hotel ındustry, in *Applications of Artificial Intelligence in Engineering. Algorithms for Intelligent Systems*, ed. by X.Z. Gao, R. Kumar, S. Srivastava, B.P. Soni (Springer, Singapore, 2021). https://doi.org/10.1007/978-981-33-4604-8_53
26. V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St. Martin's Press, Fergusn, A. G., 2018), p. 2017
27. Policing Predictive Policing. Washington Univ. Law Rev. **94**(5). Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/walq94&div=35&id=&page=&t=1559934122
28. S. Mollicchi, Flatness versus depth: a study of algorithmically generated camouflage. Secur. Dialogue **48**(1), 78–94 (2017). https://doi.org/10.1177/0967010616650227
29. P. Molnar, L. Gill, Bots at the gate: A human rights analysis of automated decision-making in Canada's ımmigration and refugee system. Citizen Lab and International [30] Human Rights Program (Faculty of Law, University of Toronto) (2018). Retrieved from https://tspace.library.utoronto.ca/handle/1807/94802
30. M.K. Lee, Understanding perception of algorithmic decisions: fairness, trust, and emotion in response to algorithmic management. Big Data Soc. **5**(1) (2018). https://doi.org/10.1177/2053951718756684
31. S. Zuboff, *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* (Profile Books, 2019)
32. S. Lundberg, S.-I. Lee, *A Unified Approach to İnterpreting Model Predictions.* 1705.07874 (2017). Retrieved from http://arxiv.org/abs/1705.07874
33. B. Mittelstadt, C. Russell, S. Wachter, Explaining explanations in AI, in *Proceedings of the Conference on Fairness, Accountability, and Transparency* (ACM, 2019), pp. 279–288. Retrieved from https://dl.acm.org/citation.cfm?id=3287574
34. C. Molnar, Interpretable machine learning. *A Guide for Making Black Box Models Explainable* (Leanpub, 2018). Retrieved from https://christophm.github.io/interpretable-ml-book
35. J. Kemper, D. Kolkman, Transparent to whom? No algorithmic accountability without a critical audience. Inf. Commun. Soc. 1–16 (2018). Retrieved from https://www.tandfonline.com. https://doi.org/10.1080/1369118X.2018.1477967
36. M. Turilli, L. Floridi, The ethics of information transparency. Ethics Inf. Technol. **11**(2), 105–112 (2009). https://doi.org/10.1007/s10676-009-9187-9
37. A. Weller, *Challenges for Transparency* (2017). arXiv preprint arXiv:1708.01870. Retrieved from https://arxiv.org/abs/1708.01870
38. J.P. Göpfert, B. Hammer, H. Wersing, Mitigating concept drift via rejection, in *International Conference on Artificial Neural Networks* (Springer, Cham, 2018), pp. 456–467. https://doi.org/10.1007/978-3-030-01418-6_45
39. G. Irving, A. Askell, AI safety needs social scientists. Distill **4**(2) (2019). https://doi.org/10.23915/distill.00014
40. P. Kohli, K. Dvijotham, J. Uesato, S. Gowal, Towards a robust and verified AI: specification testing, robust training, and formal verification. DeepMind Blog (2019). Retrieved from https://deepmind.com/blog/robust-and-verified-ai/

41. Z. Kolter, A. Madry, *Materials for Tutorial Adversarial Robustness: Theory and Practice* (n.d.). Retrieved from https://adversarial-ml-tutorial.org/
42. G. Marcus, *Deep Learning: A Critical Appraisal* (2018). arXiv:1801.00631. Retrieved from https://arxiv.org/abs/1801.00631
43. J. Donovan, R. Caplan, L. Hanson, J. Matthews, Algorithmic accountability: a primer. *Data & Society Tech Algorithm Briefing: How Algorithms Perpetuate Racial Bias and Inequality* (2018). Retrieved from https://datasociety.net/output/algorithmic-accountability-a-primer/

Analysis of ECG Signal Processing for Smart Medical Technologies



J. N. Swaminathan, R. Rameshkumar, I. Vidyasagar, I. Divya, and R. Navaneethakrishnan

Abstract Human bodies constantly generate the signal or information which has valuable information about the health. These signals should be extracted from the body, and it has to be processed to diagnose the disease. Using these informations, the blood pressure, haemoglobin levels in blood, brain activities, heart functions, and etc. can be measured invasive and non-invasively. The signal obtained from the human body will contain noises, and it has low-amplitude raw data which cannot be used directly for the diagnose purpose. In order to make it to be useful, the signal should be filtered to remove the noise and amplified to extract the exact information. Signal processing contributes a major role in the medical technologies to diagnose the disease and provide solution to cure. In this review, applications of signal processing particularly in ECG medical technologies are discussed. The methods and algorithms to overcome the ECG noises are discussed briefly. Also, the improvement of those technologies for the betterment of human health care is also discussed.

Keywords Signal processing · Health care · Medical technologies · Signal · ECG noises

J. N. Swaminathan (✉)
QIS College of Engineering & Technology, Ongole, Andhra Pradesh 523272, India

R. Rameshkumar
Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India

I. Vidyasagar
Rise Krishna Sai Gandhi Group of Institutions, Ongole, Andhra Pradesh, India

I. Divya
Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh, India

R. Navaneethakrishnan
Kumaraguru College of Technology, Coimbatore, Tamilnadu, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_49

1 Introduction

The growth of elderly population is expected to increase by 56% by 2030 and to be doubled by 2050 [1]. To provide better health care services to them, there is a significant improvement in the field of medical technologies which will extract the information such as electrocardiogram (ECG), electromyogram (EMG), electroencephalogram (EEG), nerve functions, and biomarkers, [2] from the human body. Human body is the store of valuable informations about the organs and cells. The extracted information cannot be used directly by the clinicians to diagnose the disease. In order to make the raw signal to be useful for the clinicians, it must be processed and converted into the readable biomedical signals which can be analysed by the clinicians.

Biomedical signal processing is the technique which is used for processing the raw data extracted from the human body to readable one [3]. Due to this, there is significant advancements in the field of signal processing especially in medical technologies have started increasing. The engineers and researchers all over the world started working on the development of new algorithms, components, and methods to convert the information into the readable one which has greater insights in diagnosing diseases. Also, there is a gradual upgrade in the measurement techniques from invasive to non-invasive techniques in which the details of the health can be collected without puncturing the body [4].

Biomedical signal processing includes four major stages such as signal acquisition, digitization of signals, signal computation, and interpretation of signals. Figure 1 shows the basic mechanism of the signal processing. Biological signals can be classified into two major groups as stochastic and deterministic. Stochastic signals were classified as stationary and non-stationary signals, whereas the deterministic signals were subdivided into three types such as periodic, transient, and quasi-periodic signals [5]. Biomedical signals are more useful for the system engineers in modelling bioelectrical and mechanical systems. Though the existing tool available for signal processing has high efficiency to detect and process the signals [6], still lot of advancements are needed in this field to make human life easier.

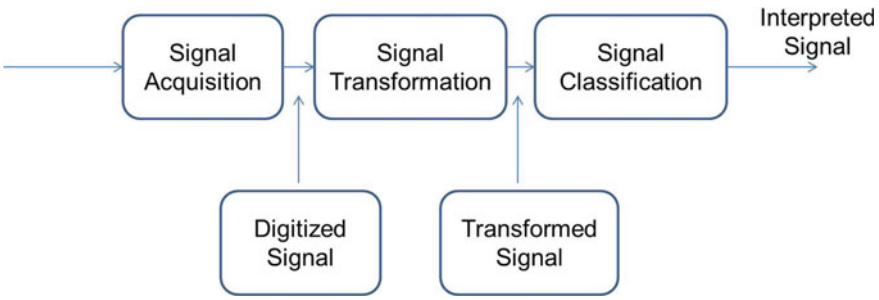


Fig. 1 Block diagram of the biomedical signal processing

Biomedical signals can be categorised into two types as action potential and event-related potential signals. ECG, EEG, and EMG are action potential, whereas other signals such as speech signals, phonocardiogram (PCG), catheter-tip sensor signals, and vibro-arthrogram (VAG) are categorised as event-related potentials [2]. From the above-mentioned applications, ECG signals were mostly used for diagnosing many applications such as cardiovascular problems, sleep apnoea, emotional, and arrhythmias detection [7–10]. ECG signal comprises of PQRST wave form which can be subdivided as P-wave, QRS complex, T-wave, and U-wave [11, 12]. Most of the ECG measurements require signal processing to clean up and provide real ECG signals in order to get the clear data. Apart from these, numerous imaging techniques such as ultrasound imaging, functional magnetic resonance imaging (fMRI), positron emission tomography (PET), and computed tomography (CT) have been used in processing the medical signals. These imaging techniques have been used to diagnose diseases such as cancer, tumour, and brain activities. High spatial resolution functional data generated by fMRI can be used to analyse the working performance of the brain under different condition [13]. It can be used to classify epileptic seizures and designed to detect brain activity changes. Along with the EEG, fMRI was used to study and examine pain in patient diagnose with sickle cell disease. Computed tomography is a non-invasive procedure used to study the high-resolution cardiac anatomy [14] (Fig. 2).

The 3D ultrasound imaging techniques are used for examining the pathology and complex anatomy. Recently, this technique finds applications in the foetal measurements and in vivo nerve movements. Hadjerci et al. have successfully demonstrated the segmentation and nerve detection using ultrasound imaging techniques [15]. The above-discussed all imaging techniques have been used in various diagnoses such as breast cancer, ventricular tachycardia, malignant rhabdoid tumour, and atrial fibrillations. Though image processing has been widely used in the medical applications, signal processing also plays a major role in the medical applications compared to the image processing techniques. In this review, the role of signal processing in the

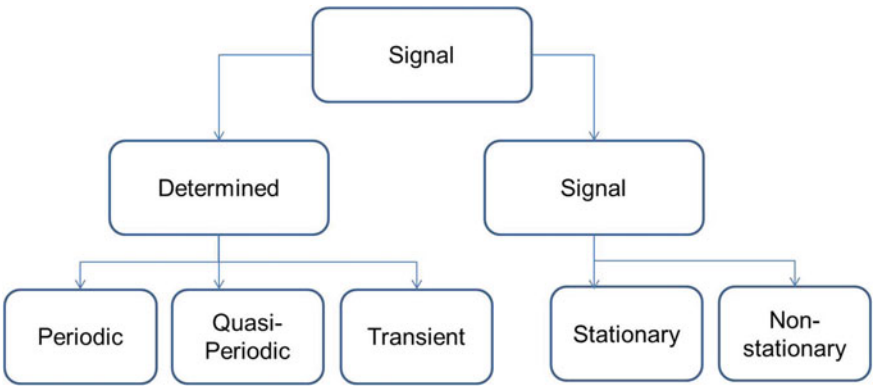


Fig. 2 Classification of signals

field medical technologies is discussed in detail. The noises in the processing of the ECG signals and the methods to eliminate the noises are discussed in briefly. The importance of the signal processing in processing ECG and FECG was also discussed.

2 ECG Signal Processing in Medical Technologies

ECG is a simple, non-invasive measurement which can be used to detect the activity of the human heart. For every heartbeat, electrical signal from the heart has been transferred throughout the body. These signals can be measured with the help of electrodes which can acquire the microvolt signal and transfer it to the processing system. In the signal processing unit, the received signal was passed through the preamplifier and passed through the filter to remove the unwanted noises, then it is passed through the post-amplifier to improve the gain of the signal to interpret the data from the signal.

2.1 ECG Noises

The ECG noises can be categorised as three: baseline wander and abrupt drift (BWAD), powerline interference (PLI), and muscle artefacts (EMG) [16–18]. The BWAD occurs due to the skin–electrode impedance, respiration, poor electrode contact, and body movements. These factors determine the duration and peak amplitude of the BWAD [17]. The BWAD increases when the ECG is recorded under stress which results in increased breathing rate [16]. The PLI is due to inductive and capacitive couplings of powerlines in the ECG circuitry. The low-frequency components present in the PLI were mixed with the ECG signals and distort the entire ECG signal [19]. These noises can distort the amplitude and shape of the ECG signals. The EMG occurs due to the movements of muscles during the ECG measurements. The ECG signals were very sensitive to the muscle movements and get distorted when the subject is in under movement during the measurement [20]. Reports have been recently reported that these muscle artefacts can majorly distort and degrade the ECG signal.

2.2 Signal Processing in ECG Measurements

Recent studies show that the available ECG processing systems produces the unreliable and inaccurate measurements which pave a path to the distorted and noisy ECG signals [21, 22]. These noisy signal results in wrong examination of cardiac problems. Still the existing ECG processing system fails to differentiate between

the noises, artefacts, and real ECG signals [21]. So, in order to get the real accurate ECG signal, these noises should be removed or filtered before to the signal processing using specific signal processing schemes. To overcome this issue and to provide the solution for this, several methods have been developed. Out of that, ECG denoising-based strategy and signal quality index (SQI)-based strategy to extract the real ECG signal are of interest. Numerous ECG denoising methods have been reported to discard and eliminate the noises present in the ECG signals. Adaptive filters, EMD-wavelet method, median filters, empirical mode decomposition (EMD), non-local means method, singular value decomposition (SVD), frequency selective filters, independent component analysis (ICA), discrete cosine transform (DCT), Wiener filters, and nonlinear Bayesian filter are of research interest [20, 23–25] These denoising techniques are highly adapted to remove the noises and artefacts which are different from the ECG signal pattern. But, these results show that these methods may distort the ST segment due to low-frequency component attenuation. Further studies concluded that simple filters are not enough to eliminate the noises due to artefacts without distorting the real ECG signals [20]. The reports show that the major distortion is introduced at the start and end of the QRS complex due to this EMD-based denoising techniques. Some studies have been reported that the severe artefacts due to movement of subject cannot be removed using the linear filters [20]. Also, some paper reported that the most of the denoising methods will majorly change the ECG local waves due to the problems with the ECG noises and artefacts. Though it has advantages, it fails to satisfy the need of the consumer in the ECG signal processing. Hence, researchers were started to find the alternate methods to process the ECG signals.

SQI-based methods were used to overcome the problem caused by the EMD-based denoising techniques. Various signal quality assessment (SQA) methods were reported to tackle the noise problem and to improve the quality of the ECG signals [26–29]. A wide range of SQI was computed for the raw ECG signals and fused to remove the false ECG signals. The SQA techniques can be classified into five major categories such as 1) fiducial features and machine learning-based SQA methods; 2) fiducial features and heuristic rules-based SQA methods; 3) non-fiducial features and heuristic rules-based SQA methods; 4) non-fiducial features and machine learning-based SQA methods; and 5) filtering-based SQA methods. In all the methods, initially, the signal is pre-processed to filter the noise which uses digital filters and decomposition techniques. Then, the extraction is carried out in order to extract the ECG signal or noise, and finally, the signal is classified into groups based on the signal quality which can be achieved with the help of machine learning techniques and artificial intelligence. In order to measure the exact hear rates, the signal quality indices (SQIs) have been reported by Orphanidou et al. [30]. Using the template matching and heart beat features, the quality of the signal was determined. They have checked this method based on the PICC and ambulatory ECG records. It is founded that this method is used to extract the accurate QRS detection under movement. Myocardial ischaemia detection using real-time ambulatory ECG signals was reported [31, 32] This method was tested by considering the motion artefacts and

noise stress database. The results obtained from the method show that it has an efficiency of 0.89 to classify the signals correctly. Also, it is observed that this method can generate better results with changing PQRST signals and heart rates.

Johannesen et al. reported a two-step algorithm in which errors due to lead missing and shifts in amplitude were eliminated from the ECG signals first, and it eliminates the ECG noises [33]. The spline function along with the high pass filter in the design was used to identify and remove the noises due to artefacts, powerline, and baseline wanders. An accuracy of 92.3% and 90% was obtained from the train set and test set, respectively. Analysis of ECG signals using the modified Tomkin's detection algorithm was reported by Tat et al. [34]. After processing the signals from the algorithm, a group of threshold rules were used to remove the noises from the ECG signals. The reported method has 92% SQA result. Hayn et al. presented a signal processing algorithm to improve the quality of the ECG signals using the simple signal quality characteristics [35]. This algorithm is mainly designed for analysing the ECG in mobile phones. The reported algorithm has high efficiency compared to the existing methods. Castiglioni et al. reported an online analysing of ECG signals using the cepstral-based method [36].

3 Result and Analysis

Though lot of papers and studies have reported on elimination of ECG noises to get a clarity ECG signal under different conditions such as subject on movement, resting, and ambulatory, still lot of improvement is needed. Lot of methods have been focussed on eliminating the false alarms, and few of the methods were reported on the extraction of ECG signals. Furthermore, all the methods were focussed only on the performance evaluations based on the accuracy and reliability not on the energy efficiency. Being reading the ECG signals in the handy device, power consumption is also one of the major factors to be considered. Hence, research on signal processing in the application of ECG in medical technologies still needs improvements based on the power consumption (Table 1).

Table 1 Performance comparison of different methods for ECG signal processing

Signal	Event detection	Performance	References
ECG and PPG	R-peak	Good	[30]
ECG	QRS complex	Good	[31]
ECG	PQRST shape	Clean/contaminated	[32]
ECG	QRS complex	ROC analysis	[33]
ECG	QRS complex	Good/bad	[34]
ECG	QRS complex	Good/bad	[35]
ECG	QRS complex	Classification in spectrum	[36]

4 Conclusion

Day to day increases in the cardiac problems forced the human beings to monitor their heart functions regularly. In the busy life, it is difficult to visit the hospital and laboratories every day to monitor their health. Lot of technology innovations help people to take care of their health using the handy devices. In that, signal processing plays a major role which helps in converting the raw data to be understandable. In this review, the role of signal processing, especially in the application of ECG, has been discussed. The ECG noises and their characteristics were discussed. Also, the signal processing techniques and algorithms reported recently and their performance on the signal processing have been discussed.

References

1. S. Chatterji, J. Byles, D. Cutler, T. Seeman, and E. Verdes, "Health, functioning, and disability in older adults - Present status and future implications," The Lancet. 2015.
2. S. Kaçar and Ü. Sakoğlu, "Design of a novel biomedical signal processing and analysis tool for functional neuroimaging," Comput. Methods Programs Biomed., 2016.
3. K. Najarian and R. Splinter, Biomedical signal and image processing. 2005.
4. S. S. Dhanabalan, S. Sriram, S. Walia, S. R. Avaninathan, M. F. Carrasco, and M. Bhaskaran, "Wearable Label-Free Optical Biodetectors: Progress and Perspectives," Adv. Photonics Res., 2021.
5. H. Van Bemmel, M. a. Musen, and U. De Stanford, "Handbook of Medical Informatics," Statistics in Medicine. 1997.
6. R. Karthikamani, P. S. Y. Prasath, M. V. Sree, and J. Sangeetha, "Wireless patient monitoring system," Int. J. Sci. Technol. Res., 2019.
7. C. Brüser, C. H. Antink, T. Wartzek, M. Walter, and S. Leonhardt, "Ambient and unobtrusive cardiorespiratory monitoring techniques," IEEE Rev. Biomed. Eng., 2015.
8. M. Forouzanfar, H. R. Dajani, V. Z. Groza, M. Bolic, S. Rajan, and I. Batkin, "Oscillometric blood pressure estimation: Past, present, and future," IEEE Rev. Biomed. Eng., 2015.
9. J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "ECG Authentication for Mobile Devices," IEEE Trans. Instrum. Meas., 2016.
10. S. Kiranyaz, T. Ince, and M. Gabbouj, "Real-Time Patient-Specific ECG Classification by 1-D Convolutional Neural Networks," IEEE Trans. Biomed. Eng., 2016.
11. C. Ye, B. V. K. Vijaya Kumar, and M. Tavares Coimbra, "An Automatic Subject-Adaptable Heartbeat Classifier Based on Multiview Learning," IEEE J. Biomed. Heal. Informatics, 2016.
12. U. Satija, B. Ramkumar, and S. M. Manikandan, "Real-Time Signal Quality-Aware ECG Telemetry System for IoT-Based Health Care Monitoring," IEEE Internet Things J., 2017.
13. U. Sakoglu and V. Calhoun, "Temporal Dynamics of Functional Network Connectivity at Rest: A Comparison of Schizophrenia Patients and Healthy Controls," Neuroimage, 2009.
14. P. Lamata et al., "Images as drivers of progress in cardiac computational modelling," Progress in Biophysics and Molecular Biology. 2014.
15. O. Hadjerci, A. Hafiane, D. Conte, P. Makris, P. Vieyres, and A. Delbos, "Computer-aided detection system for nerve identification using ultrasound images: A comparative study," Informatics Med. Unlocked, 2016.
16. G. M. Friesen, T. C. Jannett, M. A. Jadallah, S. L. Yates, S. R. Quint, and H. T. Nagle, "A Comparison of the Noise Sensitivity of Nine QRS Detection Algorithms," IEEE Trans. Biomed. Eng., 1990.

17. G. D. Clifford, "ECG statistics, noise, artifacts, and missing data," in Advanced Methods and Tools for ECG Analysis, 2006.
18. U. Satija, B. Ramkumar, and M. S. Manikandan, "Automated ECG noise detection and classification system for unsupervised healthcare monitoring," IEEE J. Biomed. Heal. Informatics, 2018.
19. J. A. Van Alsté and T. S. Schilder, "Removal of Base-Line Wander and Power-Line Interference from the ECG by an Efficient FIR Filter with a Reduced Number of Taps," IEEE Trans. Biomed. Eng., 1985.
20. U. Satija, B. Ramkumar, and M. S. Manikandan, "A unified sparse signal decomposition and reconstruction framework for elimination of muscle artifacts from ECG signal," in ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings, 2016.
21. C. Orphanidou and I. Drobnjak, "Quality Assessment of Ambulatory ECG Using Wavelet Entropy of the HRV Signal," IEEE J. Biomed. Heal. Informatics, 2017.
22. L. M. Eerikäinen, J. Vanschoren, M. J. Rooijakkers, R. Vullings, and R. M. Aarts, "Decreasing the false alarm rate of arrhythmias in intensive care using a machine learning approach," in Computing in Cardiology, 2015.
23. J. Oster, J. Behar, O. Sayadi, S. Nemati, A. E. W. Johnson, and G. D. Clifford, "Semisupervised ECG Ventricular Beat Classification with Novelty Detection Based on Switching Kalman Filters," IEEE Trans. Biomed. Eng., 2015.
24. E. Prabhakararao and M. S. Manikandan, "On the use of variational mode decomposition for removal of baseline wander in ECG signals," in 2016 22nd National Conference on Communication, NCC 2016, 2016.
25. U. Satija, B. Ramkumar, and M. S. Manikandan, "A robust sparse signal decomposition framework for baseline wander removal from ECG signal," in IEEE Region 10 Annual International Conference, Proceedings/TENCON, 2017.
26. C. Daluwatte, L. Johannesen, L. Galeotti, J. Vicente, D. G. Strauss, and C. G. Scully, "Assessing ECG signal quality indices to discriminate ECGs with artefacts from pathologically different arrhythmic ECGs," Physiol. Meas., 2016.
27. R. He et al., "Reducing false arrhythmia alarms in the ICU using novel signal quality indices assessment method," in Computing in Cardiology, 2015.
28. M. J. Rooijakkers et al., "Influence of electrode placement on signal quality for ambulatory pregnancy monitoring," Comput. Math. Methods Med., 2014.
29. J. Schumm, B. Arnrich, and G. Tröster, "Probabilistic Appraisal Of Unobtrusively Measured ECG Signals," in ISSNIP Biosignals and Biorobotics Conference, 2010.
30. C. Orphanidou, T. Bonnici, P. Charlton, D. Clifton, D. Vallance, and L. Tarassenko, "Signal-quality indices for the electrocardiogram and photoplethysmogram: Derivation and applications to wireless monitoring," IEEE J. Biomed. Heal. Informatics, 2015.
31. P. X. Quesnel, A. D. C. Chan, and H. Yang, "Real-time biosignal quality analysis of ambulatory ECG for detection of myocardial ischemia," in MeMeA 2013 - IEEE International Symposium on Medical Measurements and Applications, Proceedings, 2013.
32. P. X. Quesnel, A. D. C. Chan, and H. Yang, "Signal quality and false myocardial ischemia alarms in ambulatory electrocardiograms," in IEEE MeMeA 2014 - IEEE International Symposium on Medical Measurements and Applications, Proceedings, 2014.
33. L. Johannesen and L. Galeotti, "Automatic ECG quality scoring methodology: Mimicking human annotators," Physiol. Meas., 2012.
34. T. H. C. Tat, C. Xiang, and L. E. Thiam, "Physionet challenge 2011: Improving the quality of electrocardiography data collected using real time QRS-complex and T-wave detection," in Computing in Cardiology, 2011.
35. D. Hayn, B. Jammerbund, and G. Schreier, "QRS detection based ECG quality assessment," Physiol. Meas., 2012.
36. P. Castiglioni, P. Meriggi, A. Faini, and M. Di Rienzo, "Cepstral based approach for online quantification of ECG quality in freely moving subjects," in Computing in Cardiology, 2011.

Technical Analytical Study to Forecast the Buy-Sell Signal to Determine Investment Strategy for Maximize the ROI



Amit B. Suthar, Hiral R. Patel, and Satyen M. Parikh

Abstract The motivation behind this investigation is to figure out which pointers are more equipped for demonstrating more precise trade and purchase indicators on the NIFTYFIFTY record by utilizing the oscillator marker MACD, BB and RSI. An outcomes in current examination demonstrate that the trade sign be able to caught well by the BB and MACDmarkers, yet it cannot be caught appropriately through RSI, and capacity can be little or caption and inside manners, despite the fact the MACD assumes a too moderate function in catching the sign purchase contrasted with Bollinger groups and RSI. The utilization of a solitary pointer will not ever appearance a purchase and trade signal which is truly exact, and this depends on the aftereffects of exploration that spectacles the distinction in idealness in BB, RSI and furthermore MACD which is the fusion of a few sorts of markers will be improved contrasted with utilizing single markers. Despite the fact that in measurements there are no critical contrasts, there are just contrasts in augmentation and improvement in the situation of existing qualities; however, in this situation, the request for this worth is pivotal for dealers since it requires high precision to decide the correct choice in day by day exchanges. Further, the investigation has indicated that, however, both RSI and MACD generate signals earlier, yet they are unsafe as the quantity of bogus signs produced by them is additionally discovered to be very high. The examination is significant as the discoveries can be utilized by financial specialists, choice brokers and portfolio administrators to get create beneficial exchanging signals and acquire great danger to compensate proportions.

Keywords BB (Bollinger band) · EM · Investment strategy · MACD (moving average divergent convergent) · ROI · RSI (relative strength index)

A. B. Suthar (✉) · H. R. Patel · S. M. Parikh
Faculty of Computer Applications, Ganpat University, Kherva, Gujarat, India
e-mail: abs01@ganpatuniversity.ac.in

H. R. Patel
e-mail: hrp02@ganpatuniversity.ac.in

S. M. Parikh
e-mail: satyen.parikh@ganpatuniversity.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_50

1 Introduction

In this epoch of universalization, contributing has convert a recognizable term and has turn into a typical thing that is finished by the realm network, particularly Indonesia. As indicated by Tandelilin author in (2017), venture is a pledge to various assets or different assets made at that point, with the point of getting various advantages later on. Numerous decisions of speculation handle as of now happen currently and individual of them is stock. As indicated by the Hermuningsih [1], stock is one of the speculation handle that is very appealing, however, has a high danger. Speculators can put resources into stocks utilizing a drawn out procedure for the benefit; however, there are different ways that can be utilized to create assets from stock ventures, specifically exchanging exercises [2]. In each stock exchanging exchange, financial specialists or speculation directors are confronted with the decision to purchase or sell shares. Each slip-up in settling on speculation choices will cause misfortunes for financial specialists. In this way, an exact and dependable examination should have been utilized as the reason for speculation dynamic. There are two sorts of examination in the realm of stock venture, in particular major investigation and specialized investigation [3]. Concurring Ahmar [4] said that in directing specialized investigation utilizing past value developments as well as other market information, for example, exchange volumes, to aid the dynamic cycle on the exchanging resource market. This choice is generally gotten by actualizing some straightforward guidelines on the stock value hierarchy). Technical examination comprises of different pointers to help dynamic with a few classifications of markers. A few classes of pointers are pointers to decide patterns used to decide if commercial circumstances are in an upturn or downtrend. The pointer class used to decide the sign when purchasing and retailing is an oscillator marker [3]. An oscillator is a pointer that goes before or drives value developments. Driving indicator can rapidly anticipate value developments, for the most part used to enumerate that over bought or over sold (Ahmar 2018). Vigorous capital market exercises in a nation will outline the great state of the business atmosphere in the nation concerned. A decent capital market execution is an indicator for the soundness of the economy which will prompt speculator excitement to re-visitation of contributing (Tandelilin et al. authors 2017), where the file is an impression of stock value developments in the money market. In this manner, the course and extent of variations in the list in the money market are single benchmarks for financial specialists so as to put resources into the capital market. The motivation behind speculators in contributing is to amplify returns, without overlooking venture hazard factors that must be tended to [5]. There are a few wellsprings of danger that can impact the greatness of a speculation hazard, including market hazard, financing cost hazard, expansion hazard, liquidity hazard, political danger, etc. Political occasions are one of the non-monetary dangers that can influence financial specialists' choices in putting resources into the capital market, in light of the fact that a nation's political circumstance essentially influences the nation's monetary conditions. Due to anomalies during the political race up to the initiation of the president to be specific on January 2019 to till date with sketches acquired on or after by IDX, where list is at

basic levels, this specialized marker research utilizes information after the premier's overview to acquire typical and steady diagram another time as a target for trying and perception. In view of the information, the targets of this investigation are [2–4]:

- To see if bollinger band can show solid and exact signs in settling on a choice to buy or sell partakes in the financial exchange.
- To see if MACD can show a solid and precise sign in settling on a buy or sell choice on the securities exchange.
- To see if RSI can show solid and exact signs in settling on a buy or sell choice on the financial exchange.
- To see if the mix of the three pointers above can give a sign condition and give a more grounded signal contrasted with a particular sign.

This exploration is required to be valuable for brokers as information and assessment of interest in dividends. The current examination is relied upon to give study material and contribution to future analysts who need to look at similar articles and subjects [1, 5].

The primary thought of specialized examination is to utilize information from past value developments to figure out where costs will move straightaway [6]. The most significant thing from specialized examination is the means by which the investigation can perceive patterns as right on time as could reasonably be expected. Specialized examination is finished by using examples of file or value developments now and again. The historical backdrop of value developments can be information like clockwork, minutes, hours, weeks, months, or possibly yearly information, and contingent upon needs. Subsequently, specialized investigation clients accept that whenever utilized effectively, specialized examination can give a more functional and quicker direction so it can give more ideal advantages. Specialized investigation is utilized dependent on three presumptions [7] to be specific:

- The market limits all relevant information.
- Price moves in patterns.
- History will in general recurrent itself.

The market markdowns every relevant information. MACD which is pattern that expressions of two moving middle points the connection cost is determined by deducting the 26 day EMA of the 7 day EMA. The "signal," a 14-day exponential moving average depicted on the MACD's head, acts as a catalyst for purchase and sell signals. In accordance with Ivanovski et al. (2017), the MACD line and the sign line are the two lines that make up the MACD. In the EMA 30—EMA 14 layout, the first lines are usually blue. In the EMA 7 design, indicator lines are typically red. MACD can generate buy and sell signals. When such MACD line exceeds the sign line, a purchase indicator appears. When the MACD value passes beneath the sign line, it is supposed to be a trade signal [6–8].

2 Literature Survey

Many research papers on specialized investigation have been distributed. A large part of the current research is focused on the usefulness and precision of specialized pointers. The majority of examiners and analysts regard specialized inspection as a crucial tool for merchants to conduct competitive stock exchanges. In the past, the usefulness of specialized sharing rules and markers has been thoroughly studied in the prose. Many prior research has demonstrated the success of a specialist examinations in successful monetary market exchange sectors (2003), including those of Fama and Blume (1966) and Gencay (1998) and Kestner (2001). According to studies by Loh (2005) and Lento (2009), when pointers are consolidated together, advanced examination can be more effective in profiting from repetitive value designs. Mohd Nor et al. (2017) studied the use of a widespread specialized pointer and found that MA rubrics were behaving differently before, during and after the crisis. During the 2008–2009 global financial crisis (GFC), they were moving normal rubrics in the Malaysia stock market. Pandya et al. (2013) investigated the use of advanced examination for exchanging listed Indian IT (data innovation) companies. EMA, MACD, ROC and RSI were the indicators he used. Nithya and Thamizhchelvan et al. (2014) looked at both as far as financial component stocks are concerned. In order to question the efficient market hypothis, Subranian and Balakrishnan et al. (2014) used enhanced MACD indicators showing consistent market beating is difficult. Through their research, Chong and Ng (2008) discovered that both rules were effective in generating abundant returns on the London Stock Exchange. Metghalchi et al. (2012) have been investigating the usefulness, from 1990 to 2006, of several specialized trading regulations for 16 European securities exchanges. They propose that extending moving normal guidelines had a significant predictive force, resulting in beneficial exchanging. Rosillo et al. (2013) applied the RSI, MACD, electricity and stochastic guidelines to value data from recorded Spanish companies in order to provide buy and sell recommendations to small financial experts. Similarly, the examination's findings address the issues that arise if there is any doubt in the pointers for the merchants. To identify viable purchase and sale signals, Gold (2015) used a variety of methods. He reasoned that the proportions of a stock's execution were multi-dimensional and, as it were, past return proficiency. Bhargavi et al. (2017) investigated the suitability of RSI in Indian business sectors and discovered that it was successful in Indian financial markets. Roy et al. (2013) examined major and specific examinations and addressed the general choice of market participants at different times. Boobalan et al. (2014) used specialized pointers of the chosen organizations' defences to comprehend the value behaviour of the deals, the signals they gave, and the significant determining moments of the business expense. In order to prove that no pointer is trusted when it is provided with solid exchange signals, Subraman and Vikneswaran (2016) employed three specialty markers, MACD, RSI and the stochastic oscillator, if employed in accordance with the normal pre-set guidelines. They also found RSI superior to the two others. A literature review suggests that study into the viability of specialized markers is general, but is limited to many

indicators or potentially organizations. In the flow study, we are proposing to test a more complete arrangement of specialized points of view on companies recorded across sections over a longer period, which is more essential in terms of possible dynamics, recognizing this gap in literature [9, 10].

3 Proposed Model

MACD is a pattern ensuing force indicator that illustrations the fitting together between two moving midpoints of costs, determined by taking away the 26-day EMA from the EMA of twelve days. The "indication line," which combines the EMA of nine days and the MACD, is then plotted on the MACD's pate, acting as a trigger for purchase and trade alerts. Ivanovski et al. (2017) state that the MACD stroke and the sign line are the two lines that make up MACD. In the setup EMA of twenty-six days and EMA of twelve days, MACD strokes are normally blue. In an EMA with a nine-day arrangement, the indication lines are usually red. MACD can produce purchase and trade signals. When the MACD line passes the sign line, it signals a purchase. When the MACD line crosses below the sign line, it is considered a trade signal. When using bollinger bands, you will get a channel with upper, lower, and centre bollinger bands. As AsiaPac Finance stated in their report, the computations should be possible as is Seker et al. [9, 11]

$$\text{UB} = \text{EMA}(n) + \text{STOCH}(n)$$
$$\text{LB} = \text{EMA}(n) - \text{STOCH}(n)$$
$$n = \text{period(default : 2)}$$
$$\text{STOCH means Stochastic Oscillator}$$

Stochastic looks at the deviation or contrast of current point with most noteworthy and absolute bottom in a predefined period and the recipe is used. By utilizing this equation, we can figure various purposes of %K for a while in notable informational collection by partitioning the information in various groups for example 14 which can days, weeks, months and so on. These focuses are then plotted on a diagram as line outline. The %K esteem portrays the degree of current cost in the think back high-low range considered, in the event that its close 0%, at that point that is named as close to base level and if it is close to 100% that is named as close to most significant level. This pointer results can be very sudden because of its affectability to showcase developments, which can be limited by averaging the value focuses. This implies by taking moving normal whether straightforward, exponential or weighted and so on.

A centreline and dual value channels (groups) above and underneath it make up BBs. The value channels are the SD of the stock being considered, and the midline is an EMA.

As the value activity of a problem becomes unstable (extension) or becomes bound into a tight exchanging design, the groups will expand and contract (compression).

According to Ivanovski et al., the overall quality file (RSI) is a force pointer devised by Welles Wilder that considers the size of late increases and misfortunes over a fixed period to calculate the pace and change of value developments of a protection (2017). The RSI is established by the combination of the above two markers and below a specialist believes it is easier to collect data on trend direction, or inversion, with each stock value travels to the greater or lower band. This information can be used to determine the best times to buy and sell stocks. A purchase signal indicates if a financial professional is buying or selling a stock. Looking at market value trends on stock value graphs, as well as the volume of interest and gracefully, can be used to regulate purchasing signals. The value creation diagram is usually considered as a purchase signal from an ascending point and supported by an amount of interest below the flexible volume (Abdul-Rahim et al. 2016). An inventory is sold or denied by a speculator, according to a sell signal. Selling signals can be tracked by looking at stock cost growth, interest growth, and flexibility on stock value chart. The results can be tracked. If the diagram to create a value faces up, then down at some point, and accompanies a request volume more than a graceful volume, it might be considered the sale signal.

The MACD pointer was decoded using the following three methods: (1) Hybrids: A bearish indicator comes when the MACD crosses below the sign line, signalling that it is time to sell. It is a bullish indicator when the MACD crosses the sign line, and it is a good opportunity to buy the stock. (2) Disparity: When the price of the stock diverges from the MACD, the pattern is over. A rising stock price and a dropping MACD, for example, might signal the end of the convention. Alternatively, if stock prices are falling while the MACD is rising, a positive inversion could be approaching. (3) Sensational ascent: The protection is overbought and will soon return to normal levels when the MACD rises rapidly, showing that the shorter moving normal is drawing away from the longer term moving normal. Guppy's Multiple Moving Average (GMMA) This Daryl (Guppy et al. 2003) pointer is based on a relationship between two sets of moving midpoints, one of which has a shorter time duration than the other. A collection with a restricted time horizon determines the mobility of transient traders. The shifting midpoints are commonly determined over a period of 3, 5, 8, 10, 12 or 15 days. The other package, which covers a longer time period, is used to evaluate long-term investors' performance. This range's moving midpoints are commonly 30, 35, 40, 45, 50 or 60 days. This is a positive trend when transient moving midpoints are above long haul moving midpoints. Momentary moving midpoints are lower than long-term moving midpoints, indicating a downward tendency. Welles (Wilder 1978) invented the RSI, a force oscillator that monitors the pace and shift of value developments. This indicator is mostly used to distinguish between markets that are overbought and oversold. The RSI is a measurement that ranges from 0 to 100. Overbought is defined as RSI above 70, while oversold is defined as RSI below 30.

MACD appearances the contrast among the EMA, which is quick and delayed than the end cost. MACD is a pattern ensuing marker and is intended to distinguish changes in indications (drifts) and is for the most part not suggested for use in unpredictable economic situations.

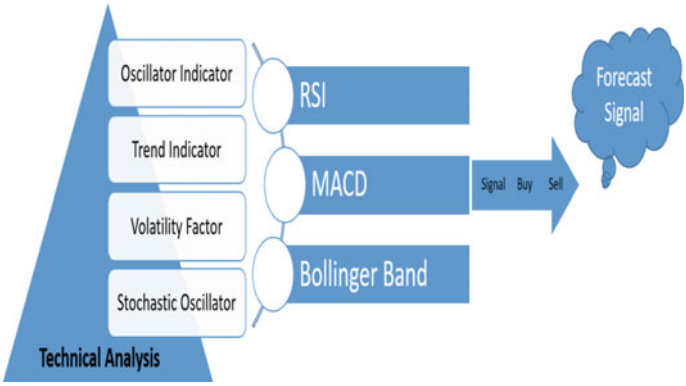


Fig. 1 Proposed model

$$\begin{aligned} &\text{RSI} = 100 - 100/(1 + \text{RS}) \\ &\text{RS is Avg Profit/Avg Loss} \\ &\text{Avg Profit} = \text{EMA(Upper Band)}/n \\ &\text{Avg Loss} = \text{EMA(Lower Band)}/n \end{aligned} \tag{1}$$

Figure 1 shows the overall modelling of model which auto generate the signal for buy and sell to maximize ROI based on the portfolio overall.

4 Implementation and Result Implementation

Since the knowledge in this analysis has different units of estimation, it must first be modified (normalized) before it can be examined. In this regard, it is critical to convert it to a z-score. According to Solimun, if the information contains various units and the scale is uneven, the units can be deleted and the scale becomes uniform (-4 to $+4$) by applying shift into standardize information methods. In this investigation, auxiliary data is normalized; after that, the Z-score information will be used for all assessments, ranging from ordinariness, example presumption tests and speculation testing. We started reverse testing of specialized pointers with stocks that are part of India's Nifty 50 record. The 50 is a crucial BSE record. Because file stocks have the biggest market capitalization and are important members of their respective divisions, we opted to focus on equities involving the Nifty 50. We also gathered data from all Nifty 50 segment stocks' daily traded estimations, split the top 20 by an annual weighted average, and matched them to sector pioneers. Both of these methods were shown to be effective in locating NIFTY daily stocks, which were around 15 stocks with the biggest market cap in their respective divisions and were also Nifty 50 bits.

We concentrated on sectorial pioneers so that we could evaluate the feasibility of all points in reference to each and every primary component.

After implementing the model, investor directly gets the signal for buy or sell the stock. The model is implemented through python library excellent support (Figs. 2 and 3).

According to the different mechanism and established investment strategy, the signal is generated. The below figures show the main selected five companies graph to represent the investment strategy and its ROI maximization.

Below graph shows the results on CIPLA stock by applying model in Fig. 4. Figure 5 represents the result of DREDDY. Figures 6, 7 and 8 represent the result of the stock companies RELIANCE, SBIN and TCS, respectively. The selected companies represented which are from different sectors and top most which gives the overview of investment strategy.

Date	Symbol	Open	High	Low	Close	Prev Close	Volume	%Deliverbl	EMA_10	RSI_14	STOCHFk_14	STOCHFd_3	STOCHk_5	STOCHd_3	ISA_9	ISB_26	Signal
2019-01-01	RELIANCE	1125.25	1127.3	1110.1	1121	1121.25	4455850	0.2933							0	0	
2019-01-02	RELIANCE	1114.5	1127	1101	1106.4	1121	7144970	0.356		0					0	0	
2019-01-03	RELIANCE	1107.5	1114.6	1090.1	1092.75	1106.4	7446457	0.3872		0					0	0	
2019-01-04	RELIANCE	1097.4	1104.45	1081.1	1098.65	1092.75	8465141	0.4131		2.817395					0	0	
2019-01-07	RELIANCE	1107	1118.45	1101	1104.75	1098.65	5513559	0.3878		5.758634	51.19047619				0	0	
2019-01-08	RELIANCE	1105.1	1109.95	1096	1104.65	1104.75	5625153	0.4024		5.755574	51.30718954				0	0	
2019-01-09	RELIANCE	1112	1117	1098.7	1110.75	1104.65	5766805	0.3475		8.918349	79.38420348	60.62728974			0	0	
2019-01-10	RELIANCE	1107.75	1111	1103	1107.5	1110.75	4080283	0.5013		8.750711	70.68273092	67.12470798			0	0	
2019-01-11	RELIANCE	1107.6	1113.8	1088.6	1098.05	1107.5	6463903	0.3686		8.266619	31.65829146	60.57507529	56.84457832		0	0	Buy
2019-01-14	RELIANCE	1095	1100.5	1086.4	1096.8	1098.05	4111782	0.4504	1102.624	8.202311	33.9869281	45.44265016	53.4038687		0	0	Buy
2019-01-15	RELIANCE	1105	1132	1105	1129.65	1096.8	10062875	0.4169	1108.145	24.69672	94.84649123	53.49723693	62.11172904	57.45339202	0	0	Buy
2019-01-16	RELIANCE	1135	1145	1130.35	1135.9	1129.65	6382777	0.3256	1113.69	27.35747	84.47098976	71.1014697	63.12908629	59.54822801	0	0	Buy
2019-01-17	RELIANCE	1144.45	1147.9	1130	1134.45	1135.9	7487963	0.3354	1117.765	27.11928	78.1300813	85.8158541	64.61855637	63.28645723	0	0	Buy
2019-01-18	RELIANCE	1148.8	1189.9	1135.25	1184.35	1134.45	25684142	0.2858	1130.647	44.83018	94.63768116	85.74625074	77.21443431	68.32069233	0	0	Buy
2019-01-21	RELIANCE	1194	1239.95	1188.65	1237.7	1184.35	22038534	0.2916	1151.12	56.84368	98.33271582	90.36682609	90.08359185	77.30552751	0	0	
2019-01-22	RELIANCE	1232.85	1246.95	1219.6	1235.15	1237.7	16552819	0.2642	1167.041	56.21678	89.91021804	94.29353834	89.09633722	85.46478779	0	0	
2019-01-23	RELIANCE	1233.3	1244.2	1222	1226.3	1235.15	8829502	0.3534	1178.183	54.00216	82.34288157	90.19527181	88.67071558	89.28354822	0	0	Buy
2019-01-24	RELIANCE	1225	1253.2	1220.1	1247.45	1226.3	13155185	0.2851	1191.126	58.21684	95.12505299	89.12605087	92.06970992	89.94558757	0	0	
2019-01-25	RELIANCE	1250.45	1264.7	1235.4	1246	1247.45	8550836	0.2763	1201.329	57.82763	75.41091387	84.29294948	88.22435646	89.65492732	0	0	
2019-01-28	RELIANCE	1250.5	1255.95	1222.4	1229.55	1246	8569265	0.3717	1206.554	53.48153	22.06208426	64.19935037	72.97023015	84.42143217	0	0	Buy
2019-01-29	RELIANCE	1231	1231.65	1201.35	1210.65	1229.55	9328866	0.4881	1207.31	48.95257	14.68034728	37.38444847	57.92425599	73.0396142	0	0	Buy

Fig. 2 Generated sheet with all statistics and signal

Date	Symbol	Open	High	Low	Close	Prev Close	Volume	%Deliverbl	EMA_10	RSI_14	STOCHFk_14	STOCHFd_3	STOCHk_5	STOCHd_3	ISA_9	ISB_26	Signal
2019-06-06	RELIANCE	1361.9	1361.9	1321.1	1327.35	1351.65	7664319	0.4648	1331.433	50.17922	19.13793103	58.57517724	59.19573286	54.79116538	1369.125	1309.2	
2019-06-07	RELIANCE	1325.95	1327.25	1305.6	1314.9	1327.35	6730595	0.2922	1328.427	47.61531	13.54697742	33.48175027	51.59294304	56.06100118	1369.125	1309.2	
2019-06-10	RELIANCE	1320.9	1327	1310.1	1319.15	1314.9	5380148	0.3691	1326.74	48.57631	19.73780944	17.4742363	41.80206192	50.86357927	1371.125	1309.95	
2019-06-11	RELIANCE	1321.85	1334.5	1318	1329.15	1319.15	5253790	0.3768	1327.179	50.84943	34.30444283	22.52974023	30.89749882	41.43083459	1373.25	1311.75	
2019-06-12	RELIANCE	1334.7	1338.4	1325	1332.15	1329.15	4707716	0.3123	1328.082	51.538	47.15808171	33.73344166	26.77704668	33.15886914	1374.325	1311.75	
2019-06-13	RELIANCE	1330	1334.7	1308.65	1327.25	1332.15	7171189	0.4797	1327.931	50.30471	66.00609756	49.15620736	36.15067999	31.27507516	1374.05	1311.75	
2019-06-14	RELIANCE	1321.9	1325	1309.4	1317.55	1327.25	6831331	0.5154	1326.044	47.87485	29.91596639	47.69338188	39.42447778	34.11740149	1354.85	1311.75	
2019-06-17	RELIANCE	1320	1320	1278.5	1282.3	1317.55	6815554	0.4083	1318.09	40.29626	6.343906511	34.08865682	36.745699	37.44028559	1334.625	1311.75	
2019-06-18	RELIANCE	1278.9	1287.95	1269.1	1281	1282.3	7679193	0.427	1311.347	40.04577	17.17171717	17.81053002	33.31915387	36.49644355	1331.25	1311.75	
2019-06-19	RELIANCE	1286.9	1302	1262.6	1277.35	1281	6625604	0.3403	1305.165	39.31068	20.45769764	14.65777377	27.97907705	32.68130997	1322.5	1311.75	Sell
2019-06-20	RELIANCE	1280	1300	1278	1296.75	1277.35	4914012	0.3793	1303.635	45.05438	54.7275641	30.78565964	25.72337036	29.00720043	1322.5	1311.75	Sell
2019-06-21	RELIANCE	1295.95	1296	1275.55	1279.5	1296.75	10623098	0.6904	1299.247	41.3281	29.44250871	34.87592349	25.62867883	26.44370875	1322.5	1311.75	Sell
2019-06-24	RELIANCE	1272.15	1276.45	1257.1	1262.4	1279.5	5150998	0.414	1292.548	37.99086	11.80400891	31.99136057	26.72069931	26.0242495	1318.825	1311.75	Sell
2019-06-25	RELIANCE	1258.9	1298	1254.25	1295.85	1262.4	6842363	0.3055	1293.148	46.96633	87.12041885	42.78897882	40.71043964	31.01993926	1316.875	1313.25	Sell
2019-06-26	RELIANCE	1291	1304.6	1286.35	1294.15	1295.85	5299942	0.2685	1293.33	46.59905	79.24528302	59.38990359	52.46795672	39.96636522	1303.125	1318.05	Sell
2019-06-27	RELIANCE	1293.15	1296.9	1271	1274.15	1294.15	11385972	0.5373	1289.843	42.41785	39.52331664	68.6296795	49.42711123	47.5351692	1309.875	1318.05	Sell
2019-06-28	RELIANCE	1277.1	1282.85	1248.65	1253.1	1274.15	8659721	0.5715	1283.162	38.52024	7.953529937	42.24071653	45.12931547	49.00812781	1309.875	1318.05	Sell
2019-07-01	RELIANCE	1258.05	1272.65	1246.45	1268.85	1253.1	6162080	0.2797	1280.56	42.73824	38.52106621	28.6659776	50.47272693	48.34305121	1316.125	1322.5	Sell
2019-07-02	RELIANCE	1273.95	1281	1263.3	1278.5	1268.85	4638751	0.3075	1280.186	45.20607	55.11607911	33.86355842	44.07185898	46.55796713	1317.125	1322.5	Sell
2019-07-03	RELIANCE	1282.9	1286.5	1275.05	1282.55	1278.5	4026032	0.3785	1280.615	46.24777	71.55599604	55.06438045	42.53400159	45.6928625	1321.9	1322.5	Sell
2019-07-04	RELIANCE	1281.4	1291	1280	1284	1282.55	4275148	0.4049	1281.231	46.63692	84.28731762	70.31979759	51.48679778	46.03088612	1322.25	1322.5	Sell

Fig. 3 Generated sheet with buy/sell signal

Fig. 4 CIPLA

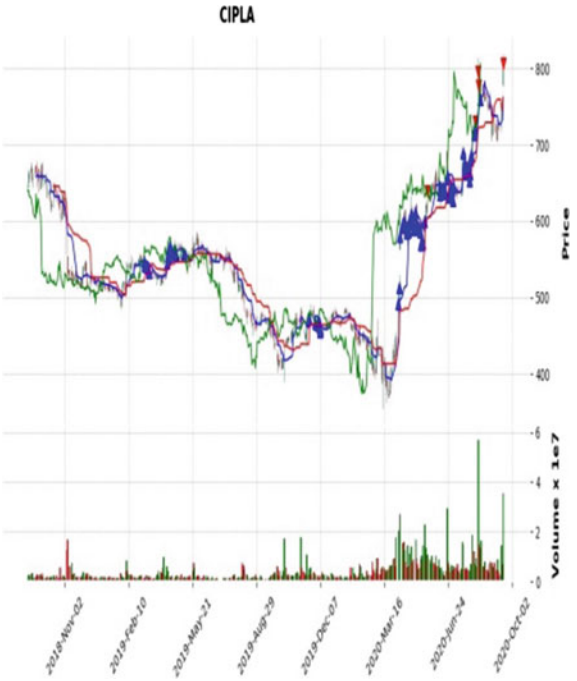


Fig. 5 DREDDY



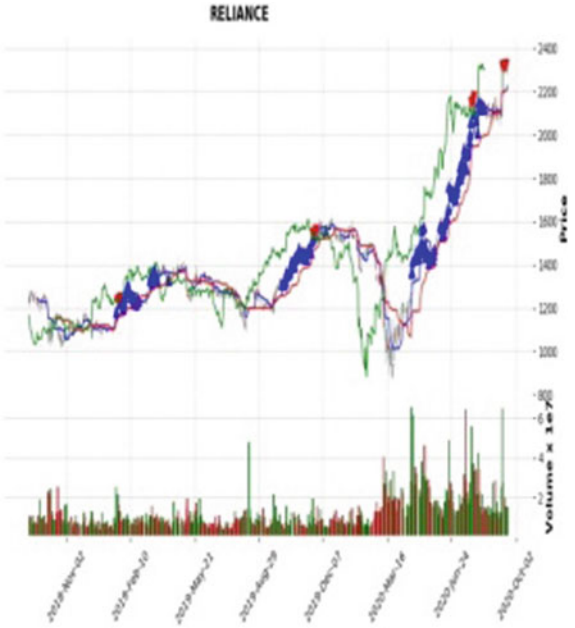


Fig. 6 RELIANCE

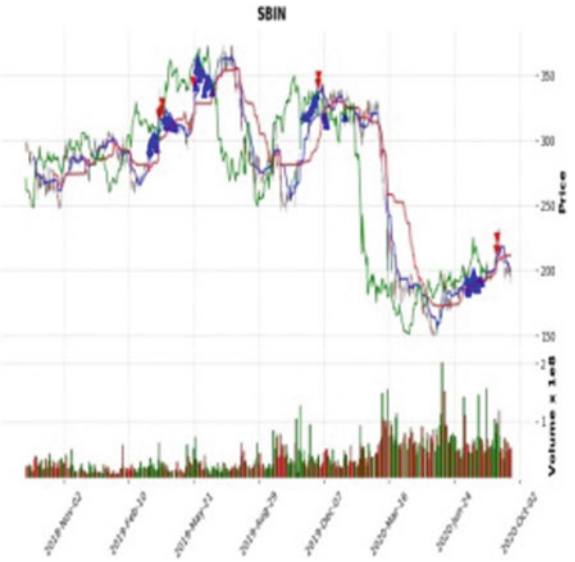


Fig. 7 SBI

Fig. 8 TCS



5 Conclusion

The despicable explains the unfavourable experimental results, which indicate a number of declines when compared to the average. The growth in appreciation is, thus, explained by a ranking sum with the know how N of the prior results is described. As a result, the difference between each chart in displaying the records when compared to the most recent stock price can be summarized as follows.

Beginning on October 24th, there was a situation between BB and RSI in which the RSI diagram in the map diagrams nearly contacted as far as it was possible. This condition suggests a suitable sale signal, despite the fact that it is not visible in the MACD because there are no fast and moderate line crosses on the pointer. However, on November 7th, MACD produced a trade signal, indicating that the sign had exceeded the point of no return for the dealer to answer and make a decision, similar to the sign that occurred on November 29th, when the important indications were RSI and BB. Both the BB pointer and the RSI are regarded to be effective at spotting the sale signal. MACD performance was overly slow in catching buy and sell signals when compared to BB and RSI. Depending on the stocks picked for investing, this might be based on a combination of all measurements and signals for SBI, all of them for ICICI Bank, and so on. For four and five tests, the idea is to use pointers.

These suggestions are amazingly significant and can fortify the influences of practice looking to exchange effectively financial exchanges in India.

The scope defined scientifically by testing for different stocks and attempting to reach some area explicit inferences. They can likewise in past views also make their examination more vigorous. Further, times of emergency can be recognized, and the

specialists can investigate if the exactness of pointers stands the pressure of variances or substantial just during the times of security.

References

1. S. Hermuningsih, Pengantar Pasar Modal Indonesia. Yogyakarta: UPP STIM YKPN (2017). Z. Ivanovski, N. Ivanovska, Z. Narasanov, Technical analysis accuracy at Macedonian Stock Exchange. UTMS J. Econ. **8**(2), 105–118 (2017)
2. B.S. Abbey, J.A. Doukas, Is technical analysis profitable for individual currency traders? The J. Portfolio Manag. **39**(1), 142–150 (2012). https://doi.org/10.3905/jpm.2012.39.1.142. R. Abdul-Rahim, A. Taqiyaddin-Arizan, S. Mohd-Nor, Analisis Teknikal dan Implikasinya Terhadap Kecekapan Pasaran Saham di Malaysia. Jurnal Pengurusan (UKM J. Manag.) **48**, 3–20 (2016)
3. A.S. Ahmar, A. Rahman, A.N.M. Arifin, A.A. Ahmar, Predicting movement of stock of "Y" using Sutte indicator. Cogent Econ. Finance **1347**, 123–132 (2017). A.S. Ahmar, *Sutte Indicator: An Approach to Predict the Direction of Stock Market Movements* (Department of Statistics, Faculty of Mathematics and Natural Sciences, Universitas Negeri Makassar, 2018)
4. A.S. Ahmar, Sutte indicator: a technical indicator in stock market. Int. J. Econ. Financ. **7**(2), 223–226 (2017). https://doi.org/10.17576/pengurusan-2016-48-01
5. G.D.I. Anghel, Stock market efficiency and the MACD. Evidence from countries around the world. Procedia Econ. Finance, **32**, 1414–1431 (2015) Makassar. https://doi.org/10.1016/S2212-5671(15)01518-X
6. B., Pushpe, C., Sumithra, H. Madhuri, Investment decision making using technical analysis: a study on select stocks in Indian Stock Market. IOSR J. Bus. Manag. 24–33 (2007)
7. A. Prabhata, Efektifitas Penggunaan Analisis Teknikal Stochastic Oscillator dan Moving Average Convergence-Divergence (MACD) Pada Perdagangan Saham-Saham Jakarta Islamic Index (JII) di Bursa Efek Indonesia. Sinergi: Kajian Bisnis dan Manajemen **13**(1), 1–14 (2012). https://doi.org/10.20885/js.v13i1.3825
8. R. Praditha, A.H.H. Haliah, Y. Rura, Market overreaction on LQ45 stock index before and after Asian games 2018. Management **9**(2), 117–125 (2018). https://doi.org/10.6007/IJARAFMS/v9-i2/6047
9. S.E. Seker, C. Mert, K. Al-Naami, N. Ozalp, U. Ayan, Time series analysis on stock market for text mining correlation of economy news. Int. J. Soc. Sci. Humanit. Stud. **6**(1), 69–91 (2013)
10. R. Pramudya, Technical analysis to determine buying and selling signal in stock trade. Int. J. Finance Bank. Stud. **9**, 58–67 (2020) (2147-4486). https://doi.org/10.20525/ijfbs.v9i1.666
11. S. Talwar, S. Pranav, S. Utkarsh, Picking buy-sell signals: a practitioner's perspective on key technical indicators for selected indian firms. Stud. Bus. Econ. **14**, 205–219 (2019). https://doi.org/10.2478/sbe-2019-0054

A Machine Learning and Deep Neural Network Approach in Industrial Control Systems



S. Ribu Hassini, T. Gireesh Kumar, and S. Kowshik Hurshan

Abstract The two major components in monitoring and controlling industrial processes are SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control System). Since their demand has been increased all over the World, they have gained more attention and because of their efficiency and high performance, these systems became mandatory in all countries. In recent times it has become an interesting target for adversaries because most of the infrastructure is automated but security is not strong enough to protect the entire system. Many loopholes make the attacker a way to exploit the vulnerability, hence protecting these systems is becoming more critical. A Hardware-in-the-loop testbed is used in this paper and its main purpose is to simulate power generation units and various attacks are performed on this testbed as well as the attack dataset is also exploited. In this research paper different machine learning algorithms are applied to the dataset and it is found that AdaBoost has better accuracy and performance compared to other algorithms and when it comes to deep learning CNN has the best accuracy compared to other ones.

Keywords Industrial control systems · Supervisory control and data acquisition · Deep learning · Machine learning · Data mining

S. Ribu Hassini (✉) · S. Kowshik Hurshan
TIFAC-CORE in Cyber Security, Coimbatore, India
e-mail: cb.en.p2cys19013@cb.students.amrita.edu

S. Kowshik Hurshan
e-mail: cb.en.p2cys20019@cb.students.amrita.edu

T. Gireesh Kumar
Department of Computer Science and Engineering, Amrita School of Engineering,
Amrita Vishwa Vidyapeetham, Coimbatore, India
e-mail: t_gireeshkumar@cb.amrita.edu

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_51

1 Introduction

SCADA (Supervisory Control and Data Acquisition) has two main purposes. They are Data acquisition and Telemetry systems. It means the data collected from field devices like sensors, actuators, pumps, valves, etc. are monitored and controlled via SCADA systems. These data are then forwarded onto a Telemetry system to transmit it through a medium to different sites. The main components of SCADA systems are PLC (Programmable Logic Controller), HMI (Human Machine Interface), RTU (Remote Terminal Unit), and Field devices. ICS (Industrial Control Systems) is used almost everywhere since it is fully automated and its main purpose is to manage and control entire industrial processes. Nowadays automation and internet connectivity is increased and this became a threat and made them more vulnerable to various attacks. The attacks on these systems are becoming as high as their importance in industrial systems. It is very clearly understood that though these systems have high demand, securing them is also becoming mandatory. Before looking into security measures, the vulnerable areas need to be concentrated more. There are many factors of SCADA systems being vulnerable, they are internet exposure, weak segregation, default configuration, weakness in ICS protocols, and lack of security awareness. These factors lead to various attacks such as malware threats, insider attacks, Denial of service, by-pass logic attacks, and so on. The datasets used in this paper are collected in a power generation testbed by measuring the sensor values for several days and this labeled dataset is generated by performing multiple attacks on the system. This dataset is generated in 2020 and it is available on paper[1]. In this paper different machine learning and deep learning techniques are implemented to find which among these are best in detecting stealthy attacks on ICS. From the results obtained it is found that AdaBoost has the best performance in machine learning and Convolutional Neural Network in deep learning compared to other supervised algorithms in proposed datasets. In Sect. 3, the collection of datasets is explained in detail. The methods of data mining and feature selection are given in detail in Sect. 4. Section 5 gives a detailed explanation of the proposed machine learning and deep learning model. Section 6 consists of the implementation of these algorithms as result and discussions. In the later section, the conclusion and future work is given.

2 Related Works

At present many types of research have started on various kinds of cyber-threats against ICS and SCADA systems. According to paper [2], anomalies are detected on ICS and several machine learning algorithms are applied. Abnormal behavior in the system is monitored using a measurement intrusion detection system(MIDS). Also, multiple algorithms are examined but only the algorithm with the best accuracy is chosen to be applied on MIDS. Attacks on PLC have increased because PLC has a major contribution in controlling the processes. In this paper [3] a detailed

explanation is given on access control attacks on PLC vulnerabilities and a sequence of attacks are performed on Siemens PLC after finding out their weakness and this causes some delay or even loss of data in communications from the phasor data concentrator (PMU) to the data concentrator. A research carried out by Sandaruwan [4] gives a good understanding of how to perform various attacks on PLC and also techniques for protecting them are also explained. In this paper the vulnerabilities of PLC are analyzed by performing several attacks like by-pass logic attack, brute-force output attack and replay, MITM, and exploits on Siemens S7 PLC are also given in detail. The paper [5]is all about how to create a SCADA simulation and to perform a malicious attack on it. According to Peter Maynard [6], they have done practical experiments on implementing and performing MOTS attacks against two Industrial Control Network by injecting falsified command responses to the victim. At last, three leading NIDS is performed to analyze the detection of attacks and their mitigation strategies are also discussed. Multiple attack scenarios are created and implemented in paper [7]. Particular attacks mainly focus on SCADA hybrid testbeds in which energy distribution is reproduced in an electrical grid. In this paper, [8] firewall protection is given by an IoT hardware device and a detailed explanation on protecting SCADA systems using this is given. A lightweight cybersecurity measure is also proposed here. Honeypot implementation is clearly explained in the paper [9] by building a honeypot to mimic the services of ICS and also it is developed to detect the network attack on SCADA systems. The primary goal of this paper [10] is to implement an efficient real-world testing platform. The testing is done in a scaled-down model of 33KV sub-station using SCADA. Advanced Persistent Threat(APT) is malware that remains undetected for a long time. In this paper [11] Long short-term memory neural networks method is proposed for APT to examine a large number of event logs in Security Information and Event Management(SIEM). Hence most of the literature survey gives a clear understanding of how to perform an attack on SCADA systems and PLC then the mitigation strategy is also discussed.

3 Dataset Collection

The dataset is built by collecting 59 points every second from the testbed. The dataset is classified into normal and abnormal situations corresponding to 34 attack scenarios. For almost 7 days, the normal situation was collected and the attack dataset was collected with 34 attack scenarios on six control loops in PLCs and DCS. The term control loop refers to the system comprising all the software functions that are wanted in measuring and adjusting the variables that control the given process. The first method is the introduction of the most significant attacks in ICS. After collecting the dataset, the next step is the appropriate features are chosen and unwanted features are filtered. At last machine learning model is trained and the particular features classify the output data. The HIL-based augmented ICS is given in Fig. 1.

There are four main processes in the testbed system and the boiler process consists of four main controllers such as flow-rate controller, temperature controller, pressure

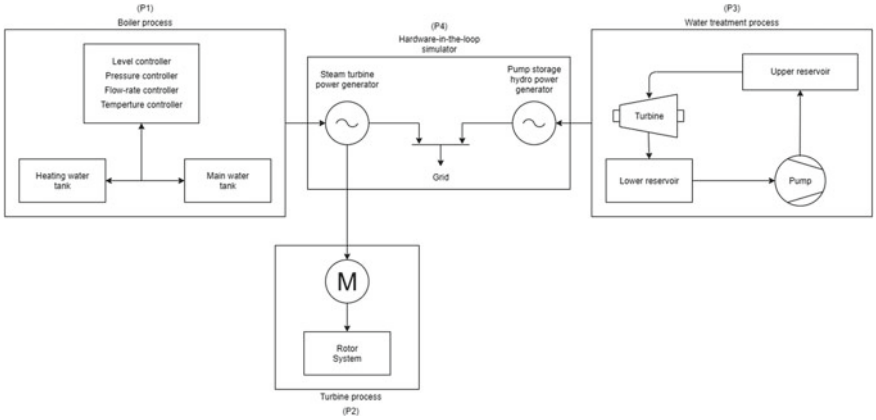


Fig. 1 HIL-based augmented ICS [1, 2]

controller, and level controller. The primary work of the boiler is that the water coming from the main tank is heated and the water is transferred from the upper to the lower reservoir. The level control pump is managed using a level controller in the water treatment process. There is a motor speed controller in the turbine process which rotates the turbine. HIL simulator consists of a steam turbine power generator and pumps storage hydropower generator connected with a power grid to feed the electrical load.

4 Methodology

The first step is the collection of data and then choose the most appropriate features. Then the dataset is trained using machine learning and a deep learning model. At last, the output data is classified corresponding to the features. The framework diagram of the dataset using a machine learning model is given in Fig. 2.

4.1 Data Mining

Imbalanced datasets lead to a classification problem in which the total number of observations per class is not equally distributed, here the prediction becomes a problem. Hence ADASYN (Adaptive Syn Sampling) technique is used for balancing the dataset. It is slightly varied from SMOTE (Syn Minority Over-Sampling Technique). Here according to the data density, ADASYN creates synthetic data that is inversely proportional to the minority class. That is synthetic data are formed in a large number where the minority class has low density. Sample Code: Adasyn = ADASYN (ran-

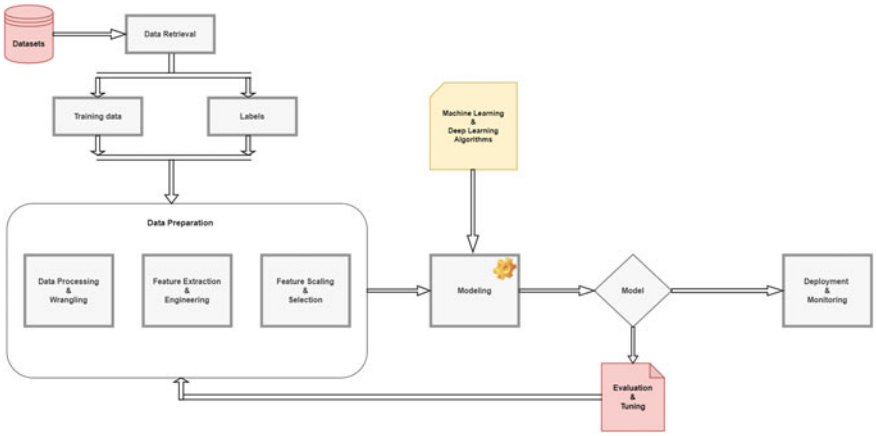


Fig. 2 Machine learning and deep learning approach on datasets

dom_state = 101). The random state is used to fetch testing data into balanced testing data. This balanced dataset is much needed in the splitting of normal and abnormal data in the training and testing phase. From the whole dataset, 0.3% is considered to be test data. The calculated splitting iteration and re-shuffling are counted as 10 and the random state is 42.

4.2 Feature Selection

To develop a predictive model, feature selection has an important role in reducing the number of input variables. Another role of feature selection is that it trains the model faster which enhances the accuracy of the model. Hence the two major goals are the preparation of a proper input dataset and improving the performance of machine learning models. It is also said to be a filtering method and the technique used in this paper is linear correlation coefficient techniques. This technique is used to measure the correlation that is a statistical relationship between two variables. If the product is 1 then the relationship is strong. If the coefficient comes near to −1, it means that it has negative relation. Similarly, if the linear coefficient is zero then there is no relation between the given data. A threshold value is set as a target for choosing the feature with high correlation. The one with a lower correlation to the target is dropped.

For the scaling of the input data in the pre-processing step, the Min-max scalar is used to scale the feature values. The formula used here is,

$$m = (x - x_{\min})/(x_{\max} - x_{\min})$$

where, m is the new value, x is the original cell value, x_{min} is the minimum value of the column and x_{max} is the maximum value of the column.

5 Proposed Model

5.1 Machine Learning Models

In this paper for training the machine learning model, various algorithms are applied for listing out which one has more accuracy compared to other algorithms. The chosen algorithms are Gradient Boost, AdaBoost, Random Forest, Support Vector Machine, and Logistic Regression.

5.1.1 Gradient Boost (GB)

It is used for regression and classification problems which produce a predictive model in the form of an ensemble of weak prediction models, similar to decision trees. The objective is to define a loss function and minimize it and the calculation is,

$$\text{loss} = \text{MSE} = \sum (y_i - y_i^p)^2$$

where $Y_i = i$th target value, $y_i^p = i$th prediction, $L(y_i, y_i^p)$ is loss function.

5.1.2 AdaBoost

This also known as Adaptive Boosting has been developed for binary classification and also the accuracy of the decision tree is also improved. It is mainly used to build the one best classifier by combining multiple weak classifiers. In the training dataset, to set the initial weight and each instance is weighted using this formula,

$$\text{Weight}(xi) = 1/n$$

where ith training instance is xi and the number of training instances is n.

5.1.3 Logistic Regression (LR)

This is one of the supervised classification algorithms in which a separate set of classes are assigned to observations. The output of probability value is transformed using a logistic sigmoid function and this is outlined to two (or) more separate classes.

5.1.4 Random Forest (RF)

This is one of the classification algorithms which combines many decision trees. When trying to build an uncorrelated forest of trees in creating each tree, feature randomness and bagging are used. It combines many tree classifiers to get more accurate and stable predictions.

5.1.5 Support Vector Machine (SVM)

It is used for two main functions, they are classification and regression challenges but it is used mostly in classification problems. Linearly separable data are classified using SVM.

5.2 Deep Learning Models

5.2.1 Convolutional Neural Network (CNN)

In CNN, the input given is the image in which the appropriate significance that is the biases and learnable weight to several objects in the image is differentiated from one to another. Because of its high accuracy, it is used in image classification and recognition.

5.2.2 LSTM+RNN

LSTM (Long short-term memory) It is best in classifying, processing, and making predictions based on time series data because there may be some delay of unknown duration between particular events in a time series. It extends the memory of recurrent neural networks. RNN (Recurrent Neural Network) The main principle of RNN is that the output of one layer is saved and it is fed back as input to predict the output of that particular layer. They can handle sequential data, can accept current input data as well as previously received input. Due to their internal memory, the previous inputs are memorized.

5.3 Model Evaluation Metrics

Two metrics are used to compare different models. They are the confusion matrix and ROC curve.

5.3.1 Confusion Matrix

To describe the performance of a machine learning model to identify the actual/predicted values from test data results. It has four combinations of predicted and actual values. They are used for specificity, accuracy, precision, AUC-ROC curves. The four combinations are True positive (TP), True negative (TN), False positive (FP), and False negative (FN).

5.3.2 ROC and AUC Curve (Receiver Operator Characteristic)

They are mainly used for the measurement of performance to avoid classification problems. ROC is a probability curve and AUC is a measure of separability. To identify the best model AUC must be higher compared to other models.

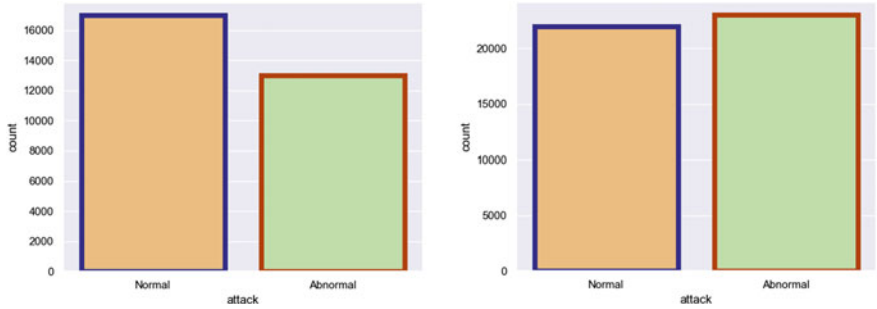
6 Result and Discussion

In this paper to control SCADA attacks, machine learning and deep learning algorithms are used. Initially have datasets for developing these models. The datasets are well trained and tested using the python programming language. Training and testing are done many times, out of that best models are chosen in both machine learning and deep learning. These procedures for the implementation of these algorithms from the dataset are given in Fig. 2.

Raw dataset is collected from warehouse and unnecessary data are removed because the huge collection of data's leads to less accuracy and high prediction time and this is mainly used for future (reinforcement learning) development. There are two problems in classification datasets, they are correlation and residue. This problem in data processing is solved by choosing the best method called linear correlation coefficient is used. When it comes to correlated feature, have selected 40 features out of 60. The remaining 20 features are the most correlated features with the target values that are chosen among residue features.

Another main problem in the training dataset is the imbalanced target data hence normalization of a dataset is important. Adaptive synthetic sampling is used to normalize the data (balanced data). This is mainly used to avoid overfitting and underfitting. Hence this is proved to be imbalanced and this may cause some issues in the performance evaluation of the trained models. From the balanced dataset, 3% is used for testing and 97% for training. The dataset before and after normalization is given in Fig. 3.

After pre-processing phase, the dataset is trained using some of the machine learning and deep learning supervised algorithms. The machine learning algorithms are Gradient boost, Random Forest, Support Vector Machine, Logistic Regression, and AdaBoost. CNN (Convolutional Neural Network), LSTM + RNN (Long short-term memory + Recurrent Neural Network) are the deep learning algorithms used.



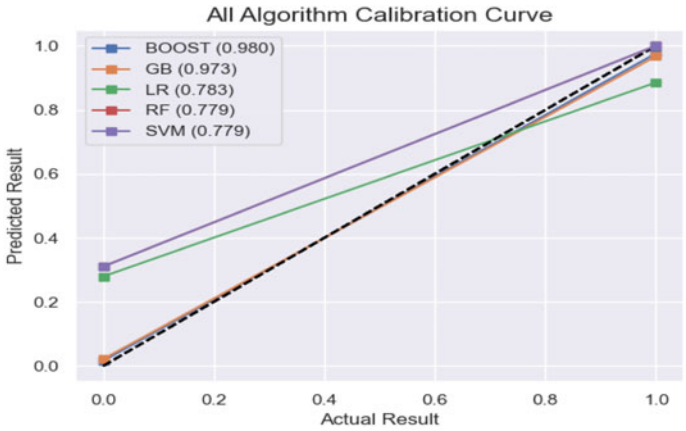
(a) Before dataset normalization (b) After dataset normalization

Fig. 3 Normal and abnormal conditions distribution

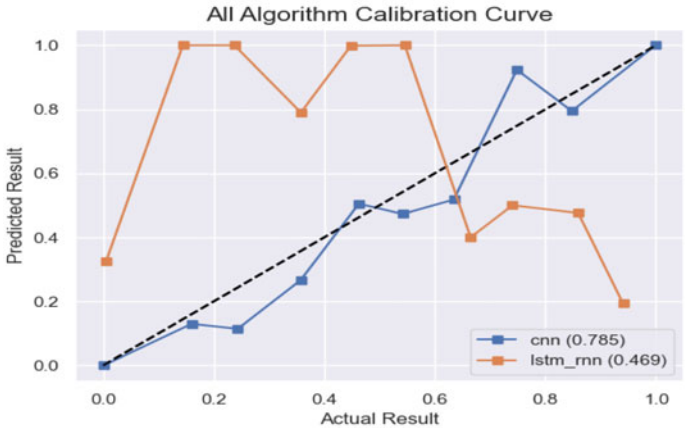
These classification algorithms are used because of their high accuracy and fast computation. Machine learning algorithms selected here are based on a binary search tree which always has better accuracy in individual results (Example: 0–98% and 1–2%). They also give better results because they are selected based on margin level. Deep learning is chosen because a neural network is created and can be customized. This will be helpful in the future because if the dataset is changed then current accuracy will also change and this is easy to customize in deep learning neural networks compared to machine learning. There are many algorithms in deep learning but here have chosen CNN, LSTM + RNN. LSTM and RNN give high accuracy in classification problems because RNN is trained in looping and LSTM stores short memory data. Hence it is best for binary classification. CNN has more chance of achieving high accuracy because max pooling and neural network are used. In a neural network, there are many configuration methods but here hidden layer = 100 is chosen for its accuracy. In the future, if the hidden layer count is changed then accuracy will also change. Thus, for the prediction of accuracy and performance various machine learning and deep learning algorithms are applied to this dataset. Their overall performance for machine learning is given in Fig. 4a, and for deep learning, it is given in Fig. 4b. In the table shown below computation time for those algorithms and the performance is compared. This is used in the prediction of the test dataset and for fitting the training dataset.

Confusion Matrix is one of the best methods for calculating accuracy, specificity, sensitivity, F1-score, and precision. In machine learning AdaBoost and deep learning Convolutional Neural Network has the best accuracy compared to supervised classification algorithms and their Confusion Matrix is below in Fig. 5.

Performance Comparison is given in Fig. 6. This figure shows a clear comparison of accuracy using five machine learning algorithms and it is understood that AdaBoost is said to have the best accuracy in anomaly detection. The ROC curve illustrated in Fig. 7a indicates that the AdaBoost in machine learning and CNN(Convolutional Neural Network) in deep learning as shown in Fig. 7b has remarkable performance in anomaly detection.



(a) Overall performance graph of Machine learning algorithms

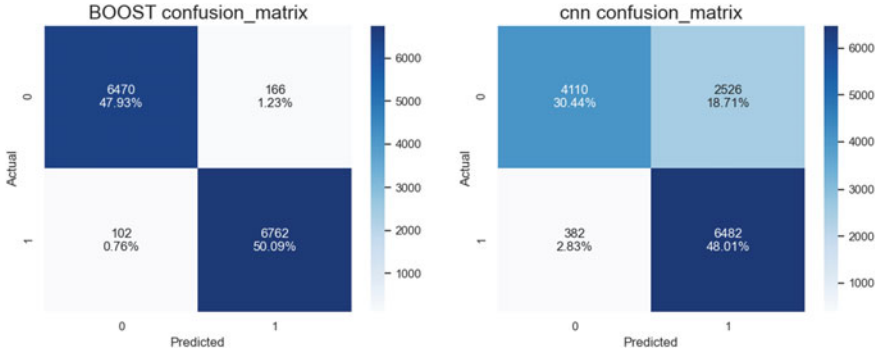


(b) Overall performance graph of Machine learning algorithms

Fig. 4 Overall performance graphs

7 Conclusion and Future Work

SCADA is mainly used for monitoring and controlling the entire industrial process. Although many security measures are implemented attacks are also increasing day by day. Since these systems are interconnected if SCADA is attacked then the components of those systems such as PLC (Programmable Logic Controller), HMI (Human Machine Interface), RTU (Remote Terminal Unit), and Field devices are also compromised as well as machines connected to those systems are also compromised. To



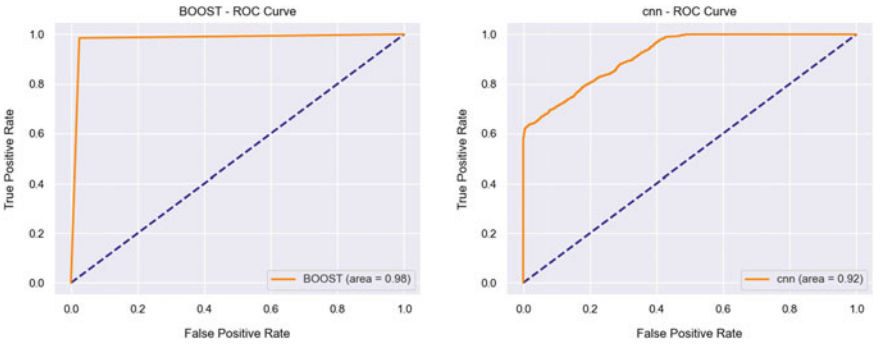
(a) Confusion matrix for AdaBoost algorithm

(b) Confusion matrix for CNN

Fig. 5 Confusion matrix for the best models in machine learning and deep learning is given above

Classification Report											
Tech	Algorithm	Accuracy	precision		recall		f1-score		Tested Datas		
			0	1	0	1	0	1	0	1	OverAll
Machine Learning	AdaBoost	**0.98**	0.98	0.98	0.97	0.99	0.98	0.98	6636	6864	13500
	Gradient Boosting	**0.97**	0.98	0.97	0.97	0.98	0.97	0.97			
	SVM	**0.82**	0.69	1	1	0.56	0.82	0.72			
	RF	**0.78**	0.69	1	1	0.56	0.82	0.72			
	LR	**0.78**	0.72	0.89	0.91	0.66	0.81	0.76			
Deep Learning	CNN	**0.78**	0.91	0.72	0.62	0.94	0.74	0.82			
	LSTM + RNN	**0.47**	0.48	0.21	0.94	0.02	0.63	0.03			

Fig. 6 Models performance comparison



(a) ROC curves for Machine learning algorithms

(b) ROC curves for Deep learning algorithms

Fig. 7 ROC Curve graphs

avoid this advanced machine learning and deep learning techniques are implemented to control the attacks. The accuracy obtained is 98.01% and this gives the best performance as well. The Future work is to develop Reinforce learning technique, that is there is no need to teach the model when the dataset is changed. It learns by itself and it also chooses the best algorithm automatically.

References

1. S. Choi, HIL-based Augmented ICS (HAI) security dataset (2020)
2. S. Mokhtari, et al. A machine learning approach for anomaly detection in industrial control systems based on measurement data. Electronics **10**(4), 407 (2021)
3. Y. Wang, et al., Access control attacks on plc vulnerabilities. J. Comput. Commun. **6**(11) (2018), 311
4. G.P.H. Sandaruwan, P.S. Ranaweera, V.A. Oleshchuk, PLC security and critical infrastructure protection in *2013 IEEE 8th International Conference on Industrial and Information Systems* (IEEE, 2013)
5. C. Queiroz, A. Mahmood, Z. Tari, SCADASim-A framework for building SCADA simulations. IEEE Trans. Smart Grid **2**(4), 589–597 (2011)
6. P. Maynard, K. McLaughlin, *Towards Understanding Man-on-the-Side Attacks (MotS) in SCADA Networks*. arXiv preprint arXiv:2004.14334 (2020)
7. L. Rosa, et al., Attacking SCADA systems: a practical perspective, in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (IEEE, 2017)
8. B.R. Yogeshwar, et al. A light-weight cyber security implementation for industrial SCADA systems in the industries 4.0, in *International Conference on Information and Communication Technology for Intelligent Systems* (Springer, Singapore, 2020)
9. R.S. Ramachandruni, P. Poornachandran, Detecting the network attack vectors on SCADA systems, in *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (IEEE, 2015)
10. S. Smrithi, et al. Development of SCADA automated 33kV substation model as testing platform, in *2015 International Conference on Industrial Instrumentation and Control (ICIC)* (IEEE, 2015)
11. P.V.S. Charan, T. Gireesh Kumar, P. Mohan Anand, Advance persistent threat detection using long short term memory (LSTM) neural networks, in *International Conference on Emerging Technologies in Computer Engineering* (Springer, Singapore, 2019)

Positioning Based on Global Navigation Satellite System

V. Tanuja and Sumalatha Aradhya

Abstract The statistics on the vehicle such as locations visited, driver status logs and usage of the vehicle is needed by the authority for validating the vehicular information. We need a black box solution to capture the live details of the vehicle. GNSS can be used as a tool to view the digital map with the help of digital tachograph. Using the coordinates of different countries in the form of latitude and longitude, we are proposing a solution to view the digital map of different digital tachograph-supported countries from European Union. The proposed solution is implemented by keeping the road safety rules suggested by European Union. The solution framework is deployed as part of vehicle unit and hence can fetch and store the coordinates of locations traveled by the vehicle. The unit of time is implemented as per recommended minimum specification sentences. The sentences are used to validate the coordinates. If the position is valid, the tachograph can record the location details, otherwise location is ignored. With the valid result, the tachograph in the vehicle extracts the value from HDOP from GSA. The security policy is applied and the value available on the settler system is considered to process the validated values. The DTCO with version R4.1 has a highly sensitive integrated GNSS module with access to satellite system such as Galileo, GPS and GLONASS. GNSS uses NMEA0183 conventions and generates time conflict and GNSS time difference more than one minute. GNSS allow users with capable device to determine their position, velocity and time from the satellite and we propose a solution as visual verification tool to map the DTCO R4.1 GNSS. The tool uses the data and protocol deployed in the vehicle unit and accurate positioning information data is transferred.

Keywords GNSS (Global Navigation Satellite System) · DTCO (Digital Tachograph) · GPS · GSA · RMC · Vehicle tracking

V. Tanuja (✉) · S. Aradhya
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumakuru, India

S. Aradhya
e-mail: sumalatha@sit.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_52

1 Introduction

1.1 Usage of GNSS in Digital Tachograph

GNSS system enables users to determine their position with respect coordinates of different DTCO-supported countries. GNSS is used for liability-critical application and commercial sensitive location-based services information about the position or velocity in the basics for legal decision or economic transaction. GNSS is used to record the position and time. Satellite signals of GNSS are used to calculate the vehicle position, speed and distance. GNSS receiver is deployed as part of the vehicle unit.

GNSS stands for global navigation satellite system which uses various positioning system like GPS GLONASS and various others. Indian and Chinese GNSS are used locally because they are satellites, so they work only around their country. GNSS will be used to find the current starting position of the daily working period, and after every 3 h, driver has to accumulate the driving time. And GNSS is used to determine the ending place, where the driving hours of working period completed.

1.2 Criteria for Measuring Performance GNSS in Digital Tachograph

There are four criteria to measure the performance. The criteria are accuracy, integrity, continuity, and availability. Through the accuracy, the portion of the vehicle is measured at given time. Through the integrity, an accurate data flows to the system and a timely warning are provided to the user. Through the continuity, the capacity of the function outside disturbance is measured. Through the availability, a service provided to the system within the specific area is measured. NMEA sentence is basically US-based marine electronics trade organization which sets standard of communication between marine electronics, which is also extended to all satellite basic systems. NMEA defines protocol standards under NM EA 0183 which allows all various GNSS to use common protocol. NMEA is correct for both the arrangement of smart tachograph with and without external GNSS facility. Few such NMEA sentences are like $–RMC, $–GGA, $–GSA, $–GSV where each type of the sentence which have specific parameter information like latitude, longitude, time, and date. NMEA (National Marine Electronics Association) sentence recommended minimum specific (RMC) is based on location data of GNSS. The size of RMC sentence is structured as per NMEAV4.1 Standards [1]. By referring to the message format, the GNSS accuracy, integrity, continuity and availability are measured [2].

2 Literature Survey

Applying deep learning method on the huge set of images in the neural network for received GPS data is discussed in the paper [3]. Deep learning application uses Kera's framework as wrapper. Machine vision and deep learning are used to improve the accuracy of geo coordinates. The image captured by the camera is respect to another reference point where the image is captured by the GPS position at that point using machine vision technique. GPS positioning error is created by sensor noise, ionospheric effects and consider for improvement in finding the position [3], however visualization of digital map is not done.

The image captured by the camera is respect to another reference point where the image is captured by the GPS position at that point using machine vision technique [4]. Research field has application in sector such as security, finance and business. On the other end, interactive visualization allows analyst to evaluate the data of sensor. Visual analytics occupy interactive visualization to incorporate skills and deduction capacity into numerical/algorithm data examination process. The growing reputation of visual analytics in recent years creates broad survey and to guess the recent development in the field [5].

Attention has received to ADAS in recent decades and accidents of car are caused by drivers' negligence, drowsiness and fatigue [6]. Supervised machine learning is used to separate the type of GNSS pseudo range, but results give accurate reorganization of advanced vehicles is just 95.8% [7]. The interchange of parallel positions inside the divides is real, however, there is no linear connection in the middle [8]. New conceptualization is empirically examined for the factors that replicates or reduces autumn ability. It recognizes and feature possible chance to support upon changes in the current trends to maintain a systematic transition away from automobility towards a culture of multi-mobilities [9]. Using a threshold weight, a zonal enhancement approach is suggested, but implementation of visualization tool to get the polygon is missing [10].

3 Existing System

Currently, limited work is done by using GNSS implementation in DTCO.

3.1 Approaches to Convert GNSS Coordinates to RMC

There are two approaches to convert the coordinates to RMC [1]. In one approach, an online tool mentioned in [11, 12] is used to convert the GNSS to RMC. In another approach, a manual calculation is done to convert the GNSS to RMC. Consider, the latitude value 12.954850. A multiple fraction degree value with 60 is computed by

keeping the decimal degree value aside, i.e., 0.954850*60 = 57.291. The latitude is read as 1257.291 (combination of decimal degree and the fraction degree value multiple with 60).

3.2 GNSS Implementation in DTCO

The functionalities of GNSS in DTCO are to record vehicle position, to validate speed data of motion sensor, to validate RTC time of DTCO with GNSS time and adjust if configured to do so [13, 14]. To perform these functionalities, few parameters information is required from GNSS are latitude, longitude, altitude, speed and time. GNSS Chip from STMicroelectronics has few proprietary commands through which specific NMEA sentences [1] can be requested, again which has specific parameter information. We have used similar approach in our proposed solution for implementation of GNSS logics.

However, in both the approaches, the visualization tool to see the travel path of vehicle is missing. We are proposing an algorithm to do the digital mapping of the vehicle's visit and motion analysis.

4 Proposed System

Our proposed solution addresses issues such as verification of raw geo data, optimization of geo coordinates, detection of features as per standard DTCO R4.1 and validation of geo coordinates.

4.1 Proposed System Architecture for Usage of GNSS in Digital Tachograph

Figure 1 depicts proposed GNSS configuration framework for calibrating the received data.

GNSS Chip used in DTCO is ST's STA8090GA and a communication protocol between AppCon and GNSS receiver is I2C. Using DMA will ensure AppCon is free enough to do other work while waiting for complete data reception or transfer. DMA will trigger interrupt only once after reading or transferring given number of bytes. GNSS chip has specific proprietary commands through which initialization, suspend kind of operation can be performed and specific information can also be sent or request to receive. To get that information, we request specific NMEA sentences from GNSS which as that parameter information. When requested, GNSS chip responds with standard type of NMEA sentences [15].

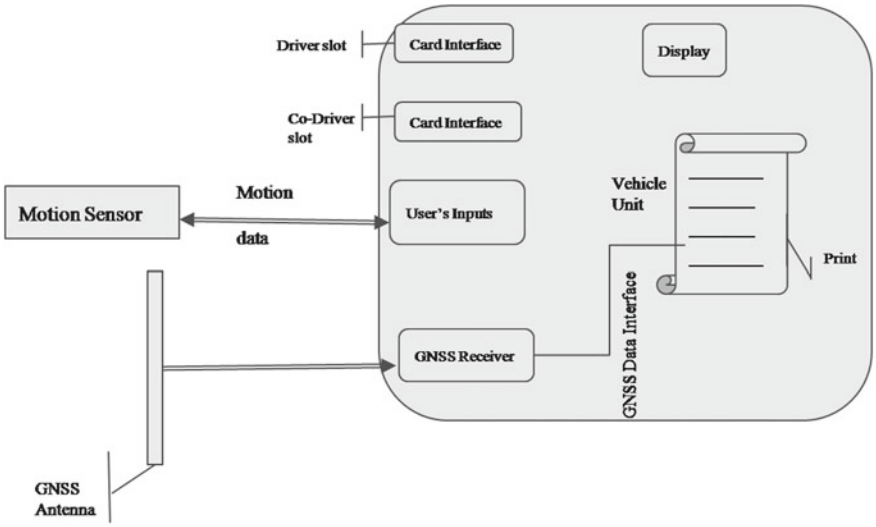


Fig. 1 System architecture for global positioning

The received data is validated against the RMC sentence, and valid positions are considered for recording in the vehicle unit. For preparing requested data, a specific time delay (500 ms) to GNSS chip is given. When delay is over, then we read data (normal I2C read request) and once data is received via DMA, specific required information is interpreted, computed and stored into vehicle database.

4.2 Proposed Design Flow for Recording GNSS in Digital Tachograph

The design framework is represented in Fig. 2

The raw data received from the motion sensor and GNSS receiver are checked to validate the geo coordinate positions, and once the validation is done, the RMC standard check is initiated. If the coordinates are not in format, then the conversion as per RMC standard is done automatically. After the validation of both position and standard, the data is recorded to vehicle unit data base. The country name is fetched through the user interface as per the coordinates automatically. Once the name is valid, the visualization tool is instantiated to draw the polygon by joining the coordinates of the background map.

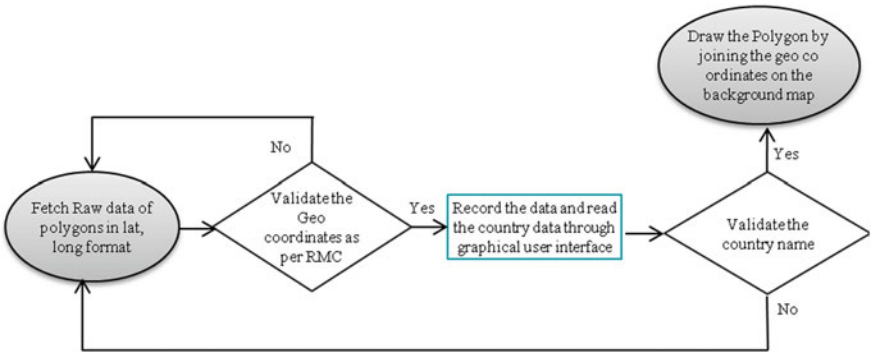


Fig. 2 Design flow for validating and recording GNSS data

4.3 Proposed Algorithm for Visualization of Digital Map

Figure 3 represents the pseudo code of the proposed algorithm to visualize the digital map from the validated geo ordinates received from vehicle unit. The algorithm reads the input data from a text file and after the stepwise processing of input data mentioned in the algorithm, a final view of the plot is displayed at the user interface. While performing the validation of the position, the performance measurement of GNSS is analyzed as well. Once the validation is through, a final polygon plot of the corresponding country is visible through interface. While performing the validation of the position, the performance measurement of GNSS is analyzed as well. The visualization tool is developed by using Python scripting language. The user interface created using Python script then the combo box is created contains the list of countries supported by the DTCO. Once the validation is through, a final polygon plot of the corresponding country is made visible through interface.

```
Input :read the data in text file in the form of co-ordinates of the country
Output: print the coordinates separately in the form of latitude and longitude
 Step 1: Define draw map of single polygon
Step 2: Split the coordinates as lat and long
Step 3: initialize the tkinter tool
Step 4: DrawMapFromRawdata using drawMapOfSinglePolygon structure
Step 5: Plot the Polygon with background map interface
Step 6: Write the variants using FigureCanvasTkAgg
```

Fig. 3 Pseudo for generating polygon plot

5 Results and Analysis

The usage of the visualization tool and the results are analyzed in this section. A data is fetched from vehicle unit in the form of text file and the file contains polygon coordinates of different DTCO-supported countries. Coordinates separately represented in the form of latitude and longitude. Each coordinate is separated by a comma and each pair values should be on a new line. The text file content format is represented as shown in Fig. 4.

After reading the text files as latitude and longitude, the visualization tool switches to user interface mode for creating infographic as shown in Fig. 5. By selecting

```
"C:/Users/uie13008/PycharmProjects/pythonProject3/read the text file.py"
42.466445,19.830998
42.471029,19.835677
42.478992,19.838093
42.479083,19.845289
42.479126,19.848765
42.483922,19.855696
42.481738,19.864582
42.483856,19.870044
42.495419,19.87797
42.494173,19.884338
42.485459,19.897806
42.496303,19.904869
42.506694,19.906347
```

Fig. 4 Reading text file as latitude and longitude separated by commas



Fig. 5 Graphical interface to select and plot polygon regions

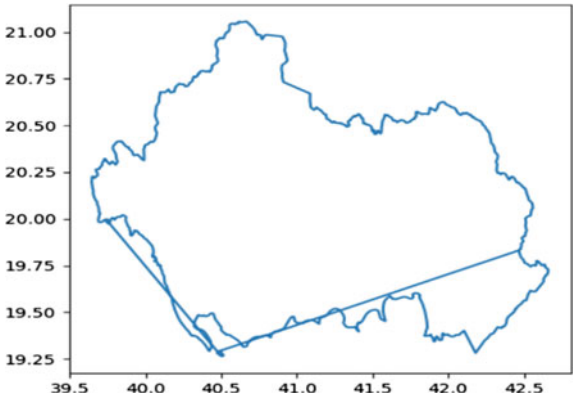


Fig. 6 Polygon plot of simple navigation

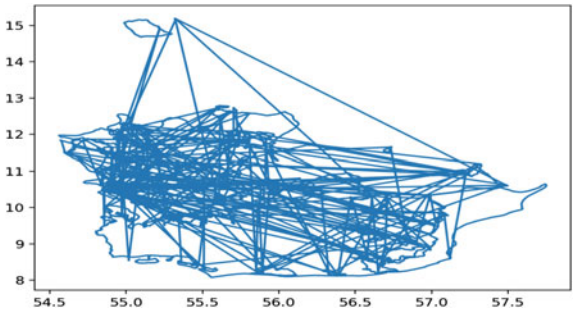


Fig. 7 Polygon plot with multiple navigation

the region from the drop-down box, the appropriate polygon plot is drawn as superimposed graph over world map on a click of button plot.

Figure 6 represents simple polygon plot for the DTCO-supported region drawn by using the visualization tool. Figure 7 represents the multiple polygon plot of DTCO-supported region. The unwanted connecting lines in the region are clipped and actual outline is drawn for the polygon using visualization tool. The *x*-axis represents the latitude and *y*-axis represents longitude coordinate values of the region visited by the vehicle. After plotting the map using the coordinates, we can draw the map of the regions over Google Map plotter using GNNS if needed in future. One can validate the result with the tachograph extracted value in the vehicle from HDOP of GSA. The security policy is applied, and the value available on the settler system is considered to process the coordinate values as concluded values.

6 Conclusion

The paper proposes a solution to visualize the digital map of vehicle unit in real time. These exist very limited work to analyze the global positioning using digital

tachograph (DTCO). The proposed solution provides accuracy of the geo coordinates along with standard policy validation check. The DTCO will record border crossing, thereby making it easier for authorities to monitor the compliance with the rules and compliance, the data will register border crossing by means of satellite positioning and record the location where the vehicles are loaded and unloaded using the coordinates in the form of latitude and longitude of different DTCO-supported countries. As a proposed solution a tool is developed to view the digital map of DTCO by following the rules of European Union standards. As proposed approach, a tool framework for automatic validation of the coordinates, performance evaluation of GNSS received data, and validation of each checkpoints visited vehicle is implemented. The resulting polygon plot will provide the effective view of the coordinates at the user interface. The next future work is to remove unwanted connecting lines of country having multiple polygons and extracting the test coordinates from map.

References

1. K. Betke, NMEA 0183 protocol specification, August 2001
2. N. Zhu, J. Marais, D. Betaille, M. Berbineau, GNSS position integrity in urban environments: a review of literature. IEEE Trans. Intell. Transp. Syst. 17 (2018). https://doi.org/10.1109/TITS.2017.2766768, hal-01709519
3. Q. Cao, X. Yan, X. Guo, H. Zhu, S. Liu, J. Yu, Temperature evolution and heat transfer during the release of CO_2 from a large-scale pipeline. Int. J. Greenhouse Gas Control **74** (2018)
4. A.K. Aggarwal, Enhancement of GPS position accuracy using machine vision and deep learning techniques. J. Comput. Sci. **16**(5), 651–659 (2020)
5. G.D. Sun, R.H. Liang, F.L. Wu, H.M. Qu, A web-based visual analytics system for real estate data. IEEE Trans. Visual. Comput. Graph. **19**(2), 278–290. (2013)
6. Y.-C. Kuo, N.-S. Pai, Y.-F. Li, Vision-based vehicle detection for a driver assistance system. Comput. Math. Appl. **61**(8) (2011)
7. L. Hsu, GNSS multipath detection using a machine learning approach, in *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC)* (2017), pp. 1–6. https://doi.org/10.1109/ITSC.2017.8317700
8. Y.C. Lin, The global distribution of the burden of road traffic injuries: evolution and intra-distribution mobility. J. Transp. Geogr. **56**(C), 77 (2016)
9. J. Marais, J. Beugin, M. Berbineau, A survey of GNSS-based research and developments for the European railway signaling. IEEE Trans. Intell. Transp. Syst. **10**(18), 2602–2618 (2017). https://doi.org/10.1109/TITS.2017.2658179, hal-01489152v3
10. D. Lu, E. Schnieder, Performance evaluation of GNSS for train localization. IEEE Trans. Intell. Transp. Syst. 16(2) (2015)
11. R.T. Ioannides, T. Pany, G. Gibbons, Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. Proc. IEEE. **104**, 1174–1194 (2016). https://doi.org/10.1109/JPROC.2016.2535898
12. E. Cardellach et al., Consolidating the precision of interferometric GNSS-R ocean altimetry using airborne experimental data. IEEE Trans. Geosci. Remote Sens. **52**(8), 4992–5004 (2014). https://doi.org/10.1109/TGRS.2013.2286257
13. D. Borio, F. Dovis, H. Kuusniemi, L.L. Presti, Impact and detection of GNSS Jammers on consumer grade satellite navigation receivers. Proc. IEEE. **104**, 1233–1245 (2016). https://doi.org/10.1109/JPROC.2016.2543266
14. L. Cucchi, J. Fortuyn, G. Baldini, A GNSS Jamming spoofing test suite for smart tachograph applications, in *European Commission, Joint Research Centre (JRC), Italy I*, ed. by Cucchi,

J. Fortuny, G. Baldini. Fernandez-Hernandez, European Commission, Defence Industry and Space, Belgium B. Martinez, European Commission, DG MOVE, Belgium G. Vecchione, Rhea Group, Belgium

15. European Parliament and European Council Regulation (EU) No 799/2016 of the European Parliament and of the Council of 18th March 2016 on the Requirements for the Construction, Testing, Installation, Operation and Repair of Tachographs and Their Components. Accessed on 14 May 2018

Online Teaching Tools: Challenges and Their Solutions During a Pandemic Available in India



Nitin S. More and Ram Vankadara

Abstract The COVID-19 has bought drastic changes in the life styles of the people. It mainly changed the educational system from offline class room teaching to online virtual teaching from schools to higher post-graduation studies. This paper discusses various comparisons and challenges of online teaching tools available in India during pandemic. Different pros and cons of the mostly used virtual platforms are mentioned here so that educators can choose the better tool to make their e-learning easy. Different challenges and constrains of the virtual or online teaching are showcased and their possible solutions are also enlightened. Constrains and solutions include the involvement of students, teachers and also the parents to make their e-learning most efficient.

Keywords Comparison · Issues · Challenges · Online teaching tool · Pandemic · Security · Privacy · Ease · Zoom · Google Classroom · Microsoft Teams · Solutions

1 Introduction

In March 2020, almost many schools across the India were closed most of the teachers going to provide instruction online to students for extended periods of time. Nowadays, as there are ample amount of online teaching tools available, it is the need of the hour to check the challenges and issues available with them [1]. With differing degrees of passion and worry, every educators approach this new model. With respect to online learning, are they positive or cautious? Are they crucial in discussing how the delivery of distance learning will strengthen their teaching and give their students unparalleled educational experiences, or do they want to explore what they going

N. S. More (✉)
Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Greenfields, Vaddeswaram, Guntur 522502, Andhra Pradesh, India
e-mail: drnitinsudam@kluniversity.in

R. Vankadara
Atmospheric Science Department, Koneru Lakshmaiah Education Foundation, Greenfields, Vaddeswaram, Guntur 522502, Andhra Pradesh, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_53

to be up into when they prepare and execute their virtual classes? In order to be best prepared to meet the challenge of working in this modern world and accept the new possibilities it has to bring, it is necessary to understand both the positives and negatives of online education, strong points or deficiencies. In higher education today, there are several explanations why online programs have become a common method of distance learning. The online world creates unparalleled opportunity for individuals who otherwise would have restricted access to schooling as well as a new model for teachers to create dynamic teachings of the best standard. Though online schools has significant strengths which provide unique access to quality education, there are lower mean in use of the such platform that can raise potential challenges to any online system's growth.

2 Interactive Teaching Tools Available for Online Teaching

Lots of nations along with India are now planning to teach most of their students online through interactive teaching tools. There are many online interactive tools available which can be accessed through mobile, tablet, and laptop. Indian government had also started offline pre-recorded lectures series through televisions to schools and college students.

Let's discuss some online interactive teaching tools available for teaching in India. Many mobile applications and tools are available online which teach students and used by educators, but only few of them are widely used. Some of the mostly used tools are given below.

- Google Classroom
- Microsoft Teams
- Zoom
- Virtual Labs
- YouTube
- Cisco Webex Meetings
- Kahoot
- Seesaw
- Khan Academy
- EPathshala

2.1 Google Classroom

Google Classroom [2] is a free, online available tool for delivering online lectures, sharing educational deliverable like presentations and other stuff. In Google Classroom, it is very easy to present, share and examine students by creating different assignments and quizzes. During online classes, students can ask teaching staff with their doubts and get it answered just like offline classes. Apart from the lecture

delivery, teachers can create assignment and get it checked and evaluate in terms of grades after students upload the completed assignments. Google Classroom uses all facilities provided by Google Cloud like Google Drive for sharing and storing study materials. Google Slides, Sheets, and Docs for writing, Google Calendar for timetable schedule, and Gmail for mailing.

2.2 Microsoft Teams

Microsoft Teams [3] from Microsoft already had tie up with many higher education institutions in India. Students will be enrolled with their basic contact details and can be identified with unique identification number like roll number. Many Microsoft Teams, just like offline classes, can be created, and schedule like offline time table can be created in Calendar tab present within Teams. You can check the activity of each student and staffs from activity tab. Chat section provide you the direct messaging feature. Assignments section allows you to create test and assignments which can be evaluated online or manually by teacher. There are many other applications available like Microsoft Share Point, Microsoft Form for full utility of the software.

2.3 Zoom

Zoom [4] is a very user-friendly, popular, and one of the mostly used applications for online teaching. Teacher can create a meeting which required a password to connect. Teacher can share that link with all the students and then they can join the meeting. Teacher will present the power point presentation and share study materials with students. Teacher can create waiting rooms and breakout rooms as per their need. Students will ask their queries through chat section. Teachers will also schedule the meeting in advance. After adding contacts of students, teacher can create different Channels for conducting the online lectures daily.

2.4 Virtual Labs

Virtual Labs [5] is the initiative of Government of India by its Ministry of Human Resource Development Department, for online study and implementation of various laboratory assignments coming under the different engineering departments. It provides virtual environment for executing assignments, experimenting with the available resources and coming up with the problem solving approach by the students. Teachers can formulate, test, and evaluate the assignments. It was developed by eminent higher education institutes like Indian Institute of Technology (IIT's), National Institutes of Technology (NIT's), and government engineering colleges

present in India. Engineering colleges can register themselves after which they can use, contribute to the Virtual Labs for benefit of students.

2.5 YouTube

YouTube [6] is one of the video sharing platforms that now acts as a subsidiaries of Google. On YouTube platform, teachers can record and share the lectures to all over the world. Teachers will also go with live sessions with questions, answering on this platform. Students can be benefited with the sessions for long time, and they can see the sessions as and when they need it. YouTube also allows their users to download the video for watching them offline. When in doubt, students can ask their queries in comment section of the video, which will be answered by video creator. It allows video creator to earn some extra money for their efforts taken. Ample amount of quality teaching, learning videos are present free of cost on this platform.

2.6 Cisco Webex Meetings

Cisco Webex Meeting [7] is again one more widely used free video conferencing and online meeting application. Many school, colleges, and universities are using it for securely conducting online webinars, conferences, and meetings. Like all other applications, it allows teachers to teach students available at wherever they are with ease of technology. It offers high-definition video and audio quality with one thousands participants capacity at a time. It also have all other features like screen sharing, one-to-one and group messaging, breakout rooms, recording of the sessions along with transcript of the same and calendar integration for schedule of meetings. It also has paid plans with better features.

2.7 Kahoot

Kahoot [8] is a gamified version of teaching and learning process tool. It allows students to learn and get them evaluated through games which called it as Kahoot, i.e., multiple choice questions. This tool can be accessed through Web browser from almost all devices, questions are displayed on teachers projector screen, and students can answer them from their mobiles. Teachers will have to create multiple choice questions and discuss it with students online. This application allows new dynamic way of teaching in classrooms with fun and interactive educational environment.

2.8 Seesaw

Seesaw [9] tool allow students to freely document their learning's at institutes, inside a user-friendly learning portfolio. Students can utilize text, photos, drawings, videos, links, and notes and with Seesaw's built-in audio recordings, drawing tools to present their learning's assimilate and also describe how they find their solutions. Student's outputs are kept securely in the cloud. Seesaw can be accessed through a variety of different platforms, like Android, Chromebooks, iOS devices, computers, and also through Kindle devices. Students and parents can also track their ward's learning.

2.9 Khan Academy

Khan Academy [10] is a non-profit organization designed to provide a variety of online resources that can allow students to learn different lessons and topics in a simpler way. In the form of videos, the Khan Academy produces short lessons both on the YouTube channel of the Khan Academy and on its highly popular website, www.khanacademy.org. Additional practice activities and materials for educators are also available on the website. You will learn all for free through the Khan Academy. Lessons are presented by images, collaborative assignments, and quizzes. Teachers will also use Khan Academy to complement their teaching and also provide their students with additional work and assist them with all or challenging material.

2.10 EPathshala

In November 2015, EPathshala [11], a portal initiated by the Ministry of Human Resources Development and the National Council for Educational Research and Training, was launched as one of the Digital India movement initiatives. Students can access all the necessary resources via EPathshala, including textbooks, audio, video, newspapers, and a number of other paper form and non-print resources and can be accessed by the individual for intermittent use without any download restrictions. EPathshala often helps users, as enabled by their computer, to hold several books. These books make it easy for users to electronically pinch, pick, zoom, highlight, browse, share, and write notes.

3 Comparison of Tools

There are many parameters for comparing available online teaching tools, but only few of them were discussed here. Comparison of above tools with respect to following parameters like-

- Offline Availability
- Network Requirements
- Ease
- Security
- Privacy

3.1 Offline Availability

From the above-discussed parameters, only YouTube and Virtual Labs are having the facility to work offline. YouTube allows users to download teaching videos to see it later when there is no network. Virtual Labs provides student with offline study material which can be downloaded and studied later.

3.2 Network Requirements

Most of the online teaching tools require good quality of network for their full functionality. It also depends on the number of users present in the meeting and the content shared. Google Classroom works best for low-quality network and hence used by most of the users. Microsoft Teams require little high network to operate with full ability as it provides many features at one place. All other tools are working quite well with low-network bandwidth.

3.3 Ease

Students ought no longer to make daunting trips to their classes and can now explore the learning style that suits them better. Microsoft Teams and Cisco Webex meetings are moderately easy while all other online teaching tools are quite simple in use and having graphical user interface.

3.4 Security

Most of the online teaching tools are providing security for joining online classes with password, but still there are chances that intruder may get link of the meeting and misuse it. More security like two-way factor authentication should be encouraged. The lack of oversight of education platforms in India has contributed to uncertainty, vagueness, and asymmetry of information between educational institutions and the services they have appointed. It also leads to a lack of knowledge on treatment of sensitive data by sites that pose unnecessary or unintended privacy and security risks, such as infringements and improper processing.

3.5 Privacy

Almost every online teaching tool is collecting teacher and students data in the form of email, contact number, etc. Maintaining privacy of this data is an utmost important thing. Many of the teaching tools are following online teaching privacy act, but it is the responsibility of institutions to adhere it appropriately. If the institute administration stores a class's videos or depends on external, cloud-based providers are also a major concern. Lack of approval, lack of security protections, and post-hoc data trail surveillance breach a student's anonymity, self-expression, and independence.

4 Challenges During Use of Online Teaching Tools

With coronavirus throwing schooling globally into chaos, more and more teachers are being required to teach their students from home using virtual platforms. You might have not registered for online learning, so it is time to chuck the lesson plan out of the window in true instructor spirit and make the most of a poor scenario.

- Technological challenges
- Lack of desire among online learners
- Separation
- Time consuming
- Remembering schedules

4.1 Technological Challenges

Before you even start, determine whether your students have reliable access to resources. Not all homes will necessarily have a secure internet link for students to have or a laptop that is accessible. An initial relatives email, letter, or text would

give them the chance to notice these concerns so that you can arrange to handle those students in advance. It is also important to note that many of them are not so proficient when it comes to tackling unfamiliar technologies or using it in a responsible way, regardless of all the talk of our students being "tech-savvy". Therefore, an initial "mentoring" session for learners is a smart idea.

4.2 Lack of Desire Among Online Learners

As difficult as online education may be for educators, it is actually much more difficult for the students. They have gone from classes primarily built to facilitate education, to residences and kitchen tables where there are ample distractions, and there is not always professional support on site. No doubt more than a handful would be inclined to sign out. The greatest form of inspiration is simple, measurable priorities. Line them up periodically so that there is plenty for learners to concentrate on. Instead of establishing and quitting an open-ended mission, following things can be considered.

- Students should focus their time on the mission,
- An observable or tangible consequence
- A way of transparency
- The return date.

Game-based software [12] and services, particularly in the formative years, may be seen as another way to boost motivation. This was specially built in independent settings for student interaction, so it avoids a lot of the trouble.

Even, when it comes to preserving students learning at home, do not neglect that parents can be your best strength. Having them on the team pays off.

4.3 Separation

It can be difficult to learn from home. It is no wonder that some students will start to feel a deep sense of alienation that eventually erodes their motivation to learn even without buzz of the classroom environment and the company of their peers. Withstanding what they claim, since the option is to be desk-bound at house, many students will feel that they skip school. Separation will also disrupt all of the teaching techniques in institutions that take for granted. Community work, class discussion, and group practice will totally vanish from the curriculum if they are not vigilant, and the resulting degrees of student involvement and enriched learning generated by those interactions go with them. Fortunately, there are some measures that have in a modern world to keep the classroom dynamic and keep things personable.

- Organize the tasks of a shared community using chats, message boards, or collaborative cloud resources.

- Present your face and let your voice be heard by pupils, using video or audio files. Do not let one become automation who communicates only through text.
- If you have the opportunity, arrange daily check-ins with students via email or chat. Pay close notice primarily to those at risk of disengagement.

4.4 Time Consuming

Users have to rely on resources to do the work for them because users can no longer just stand in front of the class and teach. And it takes time to build them. Even the spoken directions must be converted into crystal clear written texts that can be accessed and interpreted by all students. It is a bit like organizing a day off relief lesson; for all the time that goes into planning material for someone else to offer, user end up believing that only taking the class them self will take less commitment.

4.5 Remembering Schedules

Learners are not the only ones in a distance education system that might experience reduced responsibility. For students, too, it can be a war. It would be quick to return to "set and forget" mode, assigning some jobs online and only wishing for the best, without the face time and classroom environments that remind so much of their task.

5 Conclusion

In this paper, authors presented various challenges and issues being faced during online teaching in India. Ten most used online teaching tools are selected and tested with parameters like ease, security, privacy, offline availability, and network requirement. Lastly, concluded with challenges faced during online teaching by educators as well as by learners along with the possible solutions. The major solutions include giving an advance notice to the relatives of the pupil with no internet or resource availability. The educator must also follow up the students and their respective parents with poor learning skills through virtual mode. An introductory demo for how to use the virtual platforms to both student and the parent is necessary. Finally, the student should be continuously proctored by the parent and teacher for achieving the highest efficiency of learning through virtual mode, and there are many other problems are mentioned above and their feasible solutions are also given.

References

1. R.K. Bisht, S. Jasola, I.P. Bisht, Acceptability and challenges of online higher education in the era of COVID-19: a study of students' perspective. Asian Edu. Dev. Stud. (2020)
2. H.S. Kashkool, Google classroom in teaching writing composition for college students. J. Edu. Psychol. Res. **18**(68), 749–768 (2021)
3. D Pal, V. Vanijja, Perceived usability evaluation of Microsoft Teams as an online learning platform during COVID-19 using system usability scale and technology acceptance model in India. Child. Youth Serv. Rev. **119**, 105535 (2020)
4. M. de Oliveira Dias, R. de Oliveira Albergarias Lopes, A.C. Teles, Will virtual replace classroom teaching? Lessons from virtual classes via zoom in the times of COVID-19. J. Adv. Edu. Phil. **4**(5), 208–213 (2020)
5. R. Bose, Virtual labs project: a paradigm shift in internet-based remote experimentation. IEEE Access **1**(1), 718–725 (2013)
6. A. Srinivasacharlu, Using YouTube in colleges of education. Shanlax Int. J. Edu. **8**(2), 21–24 (2020)
7. C. Salceanu, Higher education challenges during COVID-19 pandemic. a case study. Revista Universitara˘ de Sociologie **XVI**(1), 104–114 (2020)
8. https://kahoot.com/
9. G.K. Lavanya, Enriching education through E-Learning. Int. J. Sci. Res. **9**(5), 270–273 (2020)
10. https://www.khanacademy.org/
11. https://epathshala.nic.in/
12. F. Gao, L. Li, Y. Sun, A systematic review of mobile game-based learning in STEM education. Edu. Tech. Res. Dev. **68**(4), 1791–1827 (2020)

Cloud Computing in a Distributed Environment Implemented with Networking Technologies

S. Sai Satyanarayana Reddy

Abstract With the advent of cloud computing, data can be distributed in remote servers. Data is distributed in remote servers instead of keeping all the data in the local server, and the principles of cloud computing are applied to all the servers that hold data. This paper uses a cloud simulator that works in a distributed environment using two server models that holds data from the Computer Science and Engineering department of our college. Then, we apply the dogma of cloud computing to the data present in the servers. Distributed cloud environment reduces overheads of communication, latencies and costs by offering efficient storage resources and orderly computation. This paper tries a build a model of networking as service that gives a virtual and flexible environment to the users for doing computation work. It also helps the users to dispatch their requirements using this virtual domain.

Keywords Cloud computing · Distributed computing · Network as services

1 Introduction

Cloud computing over distributed system plays a major role in scalability and resource utilization. It also plays a major role in on-demand resource allocation. Cloud system can provide timely service for accessing the resources that are scattered through the network [1]. With the help of cloud computing, the scattered resources can be accessed with the help of heterogeneous platforms like mobile phones, PDA's etc. The computing resources can be used to provide many customers and a variety of services on the demand of the customers. There is elasticity in services which means that the providers can scale in or scale out the computing resources whenever it is requested by the consumers [2].

Cloud system can also monitor and measure the service provided by deploying a metering system at some point in the computing system. One of the greatest attributes of the cloud system is that they provide transparency of services that they provide [3]. It is well known for delivering software services, platform and infrastructure. This

S. S. S. Reddy (✉)
Sreyas Institute of Engineering and Technology, Hyderabad, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_54

paper proposes an algorithm that designs a CloudSim that is used to simulate a cloud computing environment on two nodes. The proposed CloudSim can also simulate network connectivity among the computing resources. The CloudSim provides a virtualized scope of computing that helps the users to access the data centre within no time. It also keeps in mind the security concerns for accessing such kind of data by making use of virtualization [4].

Cloud computing acts as a business tool that offers a variety of services under one umbrella. So consumers use these services as and when they need them. These papers aim to provide services using a cloud mathematical model in which resources are deployed, controlled, run and monitored through the internet. This networking of the cloud computing environment is provided by virtualization and abstraction [5, 6]. The proposed algorithm also provides user-friendly ways to access the cloud environment with the Guaca-integrated platform. The VMs in the proposed work are isolated and are robust enough to withstand any fault [7].

2 Related Work

We have tried to create a distributed system based on four deployment models of the cloud. In order to manage a cloud environment, we adhere to some specific factors. Some policies need to be written down to decide on decision-making principles, and also, it is required to implement those decisions. Certain decisions are very important for the deployment of cloud environment like access control, efficient allocating of computing resources, network load balancing, so on and so forth.

The proposed algorithm is designed after referring few CloudSims. CloudSims that can be used for a distributed environment and that provides some concepts of virtualization is available in the market. The proposed CloudSim does not only provide cloud services in a distributed environment but also can provide service of cloud networking. We have used the DAG approach to allocate the resources [8]. There is some hardware used for building the cloud infrastructure that is stated in the next section of the paper. We have used PSO-based heuristic algorithm for assigning tasks in the data centre. PSO-based heuristic algorithm is a widespread self-compromising optimized algorithm which is similar to other generic algorithms [9]. This algorithm trusts the behaviour of individual agents. We are also using HTML version 5 to support us with internetworking. It also provides a convenient platform for the users to access remote services [12–15].

We have also used VMware vSphere to create the virtual environment. We have used JAVA code for accessing the applications using API. The proposed algorithm provides us with some features like.

- Ability to simulate with a high degree of flexibility and configurability
- It can be easily extended etc. [10, 11].

Kumar et al. [16–20] proposed an object detection method for blind people to locate objects from a scene. They have used machine learning based methods along with single SSMD detector algorithm to develop the model.

3 Proposed Model

The proposed model uses a cloud simulator that is applicable in a distributed environment. The cloud simulator contains educational data and other relevant data pertaining to our college's Computer Science and Engineering Department. The cloud simulator contains two stripped-down servers that use less space, consumes less energy and utilizes nominal power. The hardware used for the proposed simulator are

1. Intel Core i5 processors (2 in numbers).
2. Each core supports 16 GB of RAM.
3. Two Hard Disks each 1 TB capacity.
4. 10GBE network adaptor.

In our proposed model, the datacentres can use PSO-based heuristic algorithm for assigning tasks in the data centre. We have used DAG to represent a set of applications deployed in the distributed resources. We will be computing the mean computation time of a task denoted as ZK on a computer resource PCi. We also compute the cost of computation of a task that is inversely proportional to time. The proposed algorithm also uses HTML version 5 that gives users an interactive environment to access the virtual system. The users can use the features of HTML to manage the virtual resources and organizing data between data centres.

The proposed architecture has two parts. Our data centres first contact the webserver present in the non-home network. We also keep one layer of firewall around our data centre. It passes all the security tests and then contacts the gateway for accessing the basic services. In our model, we use VMware vSphere to provide us with the virtualization solution. The VMware vSphere provides an interface Vcenter and ESXi having through the API documentation and some JAVA code.

This virtual system is based on control element separation and forwarding principles. The system can also be divided into two planes control axis and the data axis. The data axis performs the actual operation of filtering and packet routing. The control axis is the main control centre of the virtual system. We use open-source Java Script compatible with HTML 5. The Java Script, along with HTML allows the users to manipulate graphics and can also add monitors. We work with JSON data, i.e. the vital of a number of devices and lines. Each part of the system contains configuration information of the other devices and also the knowledge of the end of the line. This information is worked upon in the background using Java code that ultimately helps in the network topology. We also build a cloud desktop using Guaca, which is a Web application that is compatible with HTML version 5 (Fig. 1).

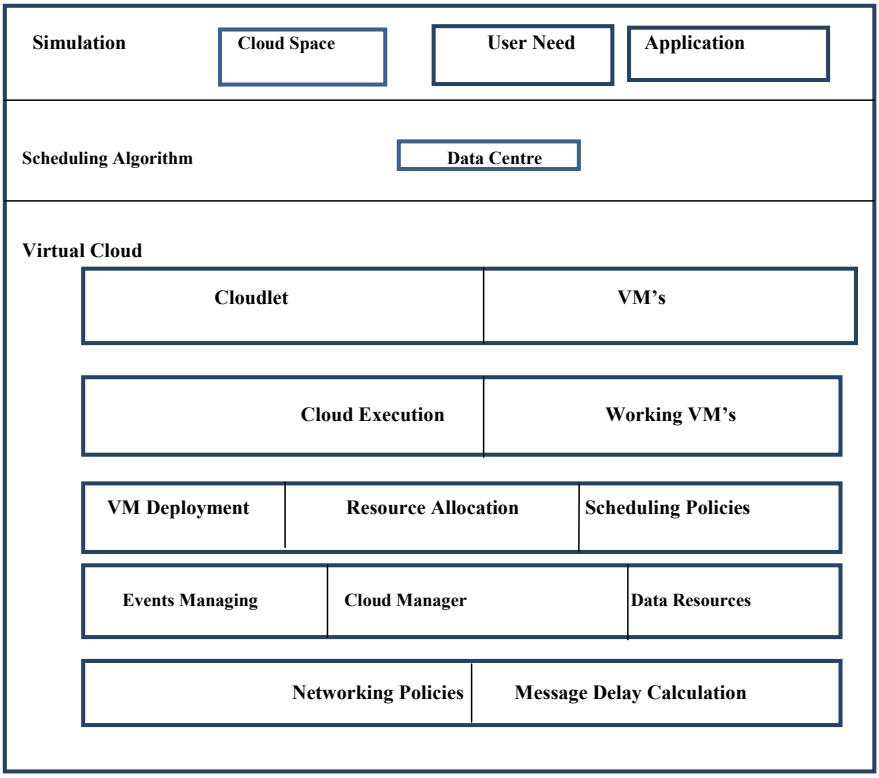


Fig. 1 Diagrammatic representation of the proposed algorithm

4 Result Analysis

In the proposed algorithm, we have assumed that the cost of unit data from resource "*i*" to resource "*j*" is known. The cost of the transfer can be calculated depending on the bandwidth of the site. The cost metric is used as a parameter of evaluation of our algorithm. We have evaluated the proposed algorithm using three tasks. The average cost of computation of all tasks at the resources is given by the TC matrix shown in Table 1.

Table 1 Cost computation matrix

	R_1	R_2	R_3
Z_1	1.32	1.10	1.14
Z_2	1.36	1.12	1.22
Z_3	1.21	1.23	1.15

Table 2 Communication cost matrix

	R_1	R_2	R_3
R_1	0	0.26	0.17
R_2	0.26	0	0.22
R_3	0.21	0.22	0

Z_1, R_1 is the cost of execution of a task at a particular resource. As we know that the computational cost is detrimentally proportional to time, so the cost is more for those resources that complete the work quickly.

The cost of communication between different resources is shown in CM matrix below (Table 2).

The communication cost is also detrimentally proportional to time.

The data size is taken as ten for each resource. If we compare our algorithm with the other scheduling algorithms, it can be shown that our algorithm incurs three times of lower cost for 1000 MB data. It is also seen that the tolerance limit of our proposed algorithm is ± 8.06 that is lower than the other scheduling algorithms. The main reason for this type of performance of our algorithm is the way it allocates task also takes into account dependencies between the tasks. When we calculate the cost of a child task, we also take into account the data transfer cost of the output transferred from the parent node. This step is repeated for the entire task to achieve an optimal scheduling algorithm based on the cost metrics. Our algorithm distributes tasks based on the data size. Since, the proposed algorithm has considered a uniform data size of ten so that is uniformly distributed between the available resources. We have implemented routing information protocol to test the virtual cloud. We use one router between two PCs. The principle of the Vnet cloud will provide the required resources for the users. There are pair of network cards that are responsible for connecting two devices (Fig. 2).

The above routing table shows how data is routed using routing information protocol. If one router stops working, then it is required to reroute the data.

5 Conclusion and Future Work

In this proposed algorithm, we have used a heuristic-based algorithm to calculate the cost of computation using a directed acyclic graph. This algorithm has also proven that it can minimize the cost of computation in a distributed cloud environment. We have also obtained the total cost of communication by changing the cost of the resources. We have compared our proposed algorithm with the existing algorithm and found that our algorithm has incurred three times lesser cost and the tolerance limit of our algorithm is also low. Our algorithm also does a proper load balancing of the tasks on the resources available. This algorithm can be applied to any number of tasks and resources by changing some parameters only. As a part of future work,

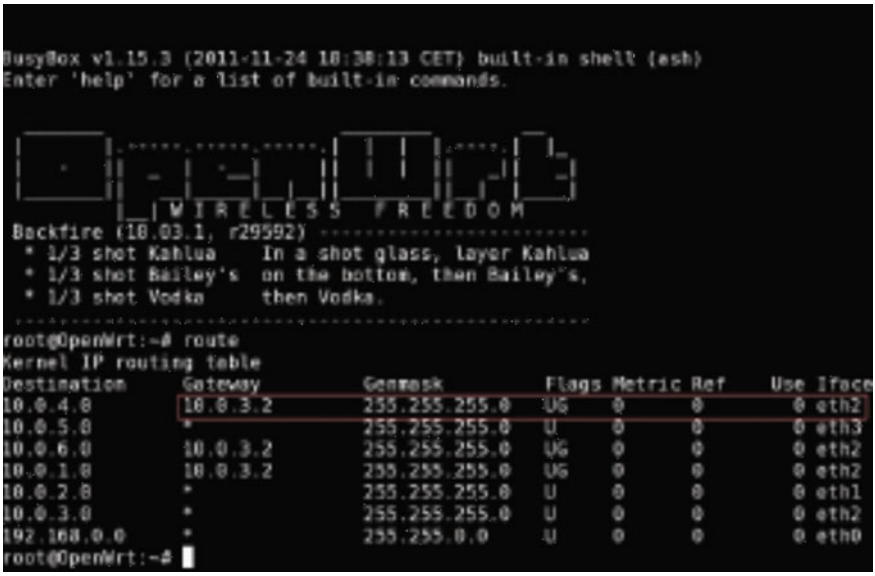


Fig. 2 Routing table

we want to use make use of our algorithm on real-time data and also in some field of medical imaging.

We have also made our algorithm to create the environment of virtual Network. Our algorithm is based on Vnet cloud that provides us with the infrastructure and resources required to build a cloud network. The users also get an interactive and convenient environment to work on. The users can work on Guaca integrated platform to work upon. In future, we would also like to add on features like user customized icons, uploading of some files etc.

References

1. P. Garbacki, V.K. Naik, Efficient resource virtualization and sharing strategies for heterogeneous grid environments, in *IFIP/IEEE International Symposium on Integrated Network Management* (2007), pp. 40–49
2. R. Buyya, C.S. Yeo, S. Venugopal, Market oriented Cloud computing: vision, hype, and reality for delivering IT services as computing utilities, in *Proceedings of IEEE/ACM Grid Conference* (2008), pp. 50–57
3. R. Aoun, E.A. Doumith, M. Gagnaire, Resource provisioning for for enriched services in cloud environment, in *International Conference on Cloud Computing Technology and Science* (2010), pp. 296–303
4. I. Foster, Y. Zhao, I. Raicu, S. Lu, Cloud computing and grid computing 360° compared, in *Proceedings of the Grid Computing Environments Workshop (GCE '08)*, November 2008, pp. 1–10

5. Z. Shen, S. Subbiah, X. Gu, J. Wilkes, CloudScale: elastic resource scaling for multi-tenant cloud systems, in *Proceedings of the 2nd ACM Symposium on Cloud Computing (SOCC '11)*, October 2011
6. S.S. Manvi, G.K. Shyam, Resource management for Infrastructure as a Service (IaaS) in cloud computing: a survey. J. Netw. Comput. Appl. **41**(1), 424–440 (2014)
7. M.F. Bari, R. Boutaba, R. Esteves et al., Data center network virtualization: a survey. IEEE Commun. Surv. Tutorials **15**(2), 909–928 (2013)
8. M. Banikazemi, D. Olshefski, A. Shaikh, J. Tracey, G. Wang, Meridian: an SDN platform for cloud network services. IEEECommun. Mag. **51**(2), 120–127 (2013)
9. T. Zhang, J. Wang, J. Huang, Y. Huang, J. Chen, Y. Pan, Adaptive-acceleration data center TCP. IEEE Trans. Comput. **64**(6), 1522–1533 (2015)
10. K. Amin, G. von Laszewski, M. Hategan, N.J. Zaluzec, S. Hampton, A. Rossi, Gridant: a client-controllable grid work.ow system, in *HICSS '04: Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04)—Track 7* (2004)
11. M. Armbrust, A. Fox, R. Grifth, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, Above the clouds: a berkeley view ofcloud computing. Technical report, University of Californiaat Berkeley, February 2009
12. R. Buyya, S. Pandey, C. Vecchiola, Cloudbus toolkitfor market-oriented cloud computing, in *CloudCom'09: Proceedings of the 1st International Conference on Cloud Computing*, vol. 5931 of LNCS. (Springer,Germany, December 2009), pp. 24–44
13. J. Cao, S.A. Jarvis, S. Saini, G.R. Nudd, Gridflow: workflow management for grid computing, in *CCGRID'03: Proceedings of the 3rd International Symposium on Cluster Computing and the Grid*, Washington, DC, USA (2003), pp. 198–205
14. E. Deelman, G. Singh, M.-H. Su, J. Blythe, Y. Gil, C. Kesselman, G. Mehta, K. Vahi, G.B. Berriman, J. Good, A. Laity, J.C. Jacob, D.S. Katz, Pegasus: a framework for mapping complex scientific workflows onto distributed systems. Sci. Program. **13**(3), 219–237 (2005)
15. N. Furmento, W. Lee, A. Mayer, S. Newhouse, J. Darlington, ICENI: an open grid service architecture implementedwith Jini, in *Supercomputing '02: Proceedings ofthe 2002 ACM/IEEE Conference on Supercomputing* (2002)
16. A. Kumar, S.S.S.S. Reddy, V. Kulkarni, An object detection technique for blind people in real-time using deep neural network, in *2019 Fifth International Conference on Image Information Processing (ICIIP)*, Shimla, India (2019), pp. 292–297. https://doi.org/10.1109/ICIIP47207.2019.8985965
17. A. Kumar, A review on implementation of digital image watermarking techniques using LSB and DWT, in *Third International Conference on Information and Communication Technology for Sustainable Development (ICT4SD 2018),* held during 30–31 August 2018 at Hotel Vivanta by Taj, GOA, India
18. S.S.S. Reddy, A. Kumar, Edge detection and enhancement of color images based on bilateral filtering method using K-means clustering algorithm, in *ICT Systems and Sustainability. Advances in Intelligent Systems and Computing* ed. by M. Tuba, S. Akashe, A. Joshi, vol. 1077. (Springer, Singapore, 2020)
19. A. Kumar, S.S.S. Reddy (eds.), *Advancements in Security and Privacy Initiatives for Multimedia Images.* (IGI Global, 2021). https://doi.org/10.4018/978-1-7998-2795-5
20. A. Kumar, Design of secure image fusion technique using cloud for privacy-preserving and copyright protection. Int. J. Cloud Appl. Comput. (IJCAC) **9**(3), 22–36 (2019)

Detection of Insider Threat Based on Forensic Analysis of Windows



Kaushal Bhavsar and Bhushan Trivedi

Abstract Insider threats are security threats by actors having access to the organization's IT infrastructure like employees, contractors, etc. Conventional network security systems can fail in detecting insider threats as the malicious activity never crosses the endpoint. Most researchers focus on monitoring a user's activity on a host machine to detect threats. However, in the absence of a monitoring mechanism when responding to an insider threat attack, it is impossible to detect the threats. In our paper, we apply forensic analysis of a Windows machine to detect insider attacks.

Keywords Insider threat · Computer forensics · Windows registry · Cyber crime

1 Introduction

In cybersecurity, an entity having the potential to exploit a vulnerable system is known as a threat. Threats can be broadly categorized as:

1. **Outsider threat**–Any threat that emerges from outside the organization's IT infrastructure. Such threats need to identify a vulnerable entry point to breach the security before they execute their attack.
2. **Insider threat**–Any threat that emerges from within the organization's IT infrastructure. Such threats do not need to breach the security from outside, since they already have access to key IT resources of the organization.

Outsider threats can be thwarted by appropriate security mechanism like intrusion detection systems and firewalls that monitor each incoming network packet to filter out malicious traffic. However, since insider threats are already within the organization's infrastructure, they are not detected by the security mechanism unless exchange of data to external network is detected [1].

This makes detection of insider threats a challenging assignment. With the coronavirus pandemic affecting organizations globally, insider threats are on the rise [2].

K. Bhavsar (✉) · B. Trivedi
GLS University, Ahmedabad, Gujarat, India
e-mail: kaushal@pratikar.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_55

Several methods of detecting and preventing insider threats have been researched since the first mention of this issue. Most research involves continuous monitoring of the activities performed by the user [3] to identify anomalies in their pattern.

However, if a security incident happens before the monitoring system is deployed, it is extremely difficult to identify the threat. In the absence of any monitoring mechanism, we must rely on the forensic information stored in the computers. This information can help rebuild the sequence of events that have taken place on the computer from which we can determine the cause of the attack.

In this paper, we propose a technique to use forensic analysis for identifying insider threats when no security controls were present prior to the incident. Our approach is suitable for analysis of large-scale computer networks.

2 Literature Review

In the field of insider threat research, the Tim Llyod-Omega corporation is a textbook example where the threat actor Tim Lloyd sabotaged an entire organization by planting a malware [4]. While most of the evidence was designed to be deleted, a few removable media as well as the login/logout timings of the threat actor were main evidence in the trial by FBI.

In modern work environment, network access control can stop data leak or malicious data download to/from the extranet. However, removable media devices have limited control, and they are one of the key assets used by threat actors [5].

The CERT guide to insider threat suggests [6] that insider threat actors exhibit certain technical precursors before they perform a real attack. These precursors can be system activity that can be recorded in the operating system's internal logs. With appropriate technique [7], we can extract this information and use it for predicting [8] whether the user is a threat or a non-threat.

A significant research is done in proactive monitoring for insider threats over the years [9 ,10], but as mentioned above, in the absence of proactive monitoring controls it is not possible to predict or even detect insider threats with the present research. We wish to bridge the gap between proactive and reactive insider threat detection with this research.

3 System Architecture

As discussed above, our technique is suitable in a scenario of insider threat incident response when there is lack of proactive monitoring mechanism. We analyze forensic artifacts from the user's system to identify if the user is an insider threat. In this paper, we present the system for detection of insider threats based on forensic analysis of a Windows computer.

Figure 1 describes the architecture of our system:

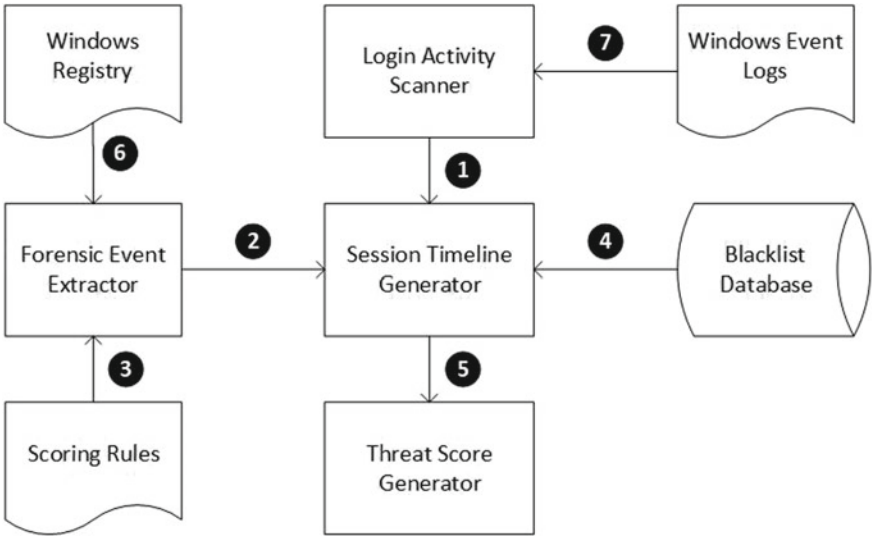


Fig. 1 Architecture of proposed system

1. The login activity scanner fetches the login information from the ACCESS logs.
2. The login activity scanner generates a collection of login sessions that have taken place. Each session is identified with a unique session ID that can be used for future reference.
3. The forensic event extractor collects forensic information from the Windows registry.
4. The forensic event extractor arranges the events sequentially according to the timestamp.
5. The session timeline generator takes the session information from the login activity scanner and identifies the events that have happened during the session with the above information from the forensic event extractor.
6. The session timeline generator identifies blacklisted events based on the blacklist database and associates those events with the session ID.
7. The threat score generator identifies the threat score for each session based on the scoring rules and the session event data generated by the session timeline generator.
8. The aggregate threat score is a cumulative calculation of each of the session, threats, course which have been identified.

3.1 Dataset Generation

CERT has made significant contribution to insider threat research by releasing a dataset [11]. However, this dataset simulates the insider threats based on the cases

Table 1 Windows registry reference for forensic information

List item	Location in registry
Applications accessed	HKCU\Software\Microsoft\Windows\CurrentVersion \Explorer\UserAssist
Removable media	HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR
	HKLM\SYSTEM\MountedDevices

they have analyzed in the past, and it is not collected from a real computer. Hence, we need to generate new data from real computer systems.

We aim to collect information about past events that have taken place on target systems with the purpose of identifying insider threats. This requires regenerating past events by collecting forensic evidence from all the systems in the network. Every operating system has a mechanism to collect forensic evidence for further investigation. On the Unix platform, this information is stored in log files, whereas on the Windows platform, it is stored in the Windows Event Logs and Windows Registry.

For this experiment, we have considered a Windows computer system as this is the most used business operating system. We stored the event information into a central data repository for ease of access. The data is stored in XML format for analysis and review. In our experiment, the data can be divided into the following parts:

1. **Session activity**–This includes the login/logout events that have been invoked by the user across a typical workday, along with their time stamps. This information is important for us to establish a link between the activities performed on the computer and the user logged on at the time of performing this activity.
2. **Application activity**–This includes the list of applications that have been executed on the computer. We associate this activity with the user whose login session was active during the timestamp of this activity.
3. **Removable media activity**–This includes the USB removable media connected/disconnected events. Just like application activity, we associate this one with the user whose login session was active during occurrence of this event.

The session activity is collected from the Windows Event logs. We collect them from "Security" section of the Event viewer application, by extracting as a CSV file. To get the application as well as removable media activity, we go to various sections of the Windows registry [7] as shown in Table 1.

3.2 Ontology

We devised a unique ontology to represent the forensic evidence captured, in form of events. This ontology is used to generate an XML file to store the event information. We used XML because it can be examined manually with a normal text editor, and it is easy to extract information from it programmatically, too (Fig. 2).

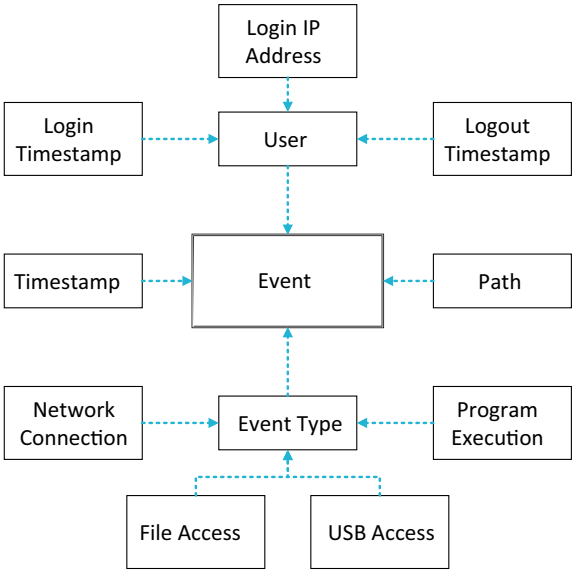


Fig. 2 Ontology for representation of events in a computer system

The fields in the ontology as explained as follows:

1. **Event**: The main event object.
2. **User**: The subject, i.e., the user whose session was active, while the event was invoked.
3. **Login time stamp**: Date/time when the user last logged in to the system before the event took place.
4. **Logout time stamp**: Date/time when the user logged out of the system after the event took place.
5. **Login IP**: IP address (INTRANET IP or INTERNET IP) of the user from which the login took place.
6. **Timestamp**: Date/time when the event occurred.
7. **Path**: Absolute path of the program/file/network connection accessed during the event.
8. **Event Type**: Type of the event which can be a Network Connection, i.e., connection to a network share, File Access, USB device connection or Program Execution.

3.3 Threat Score

The prime motive to introduce a threat score is that we want to convert qualitative output to a quantitative output. Most threat researchers classify a transaction into two categories viz. malicious vs. benign. That might hold for atomic activities like analysis of log files or network traffic. However, our topic involves the behavioral

Table 2 Windows registry reference for forensic information

Event	Score
Connected to a new network	10
Connected to an unrecognized network	75
Accessed network share	20
Accessed file	15
Executed program	15
Connected USB disk	50
Connected unregistered USB disk	75
Executed blacklisted program	100
Accessed file with confidential information	90
Logged in out of regular shift hours	80
Logged in remotely	60

analysis of a computer user and covers a broad spectrum of computing activity performed by heterogeneous groups of people. Introducing a threat score removes the effort of categorizing users and instead provides a qualitative, relative scale for further analysis by the administration. We have knowledge-engineered a threat score matrix which includes a threat score for various activity scenarios related to insider threats based on the DREAD framework, as shown in the following Table 2:

4 Experiment Implementation

After the user sessions have been identified, we can now go ahead and identify all the activities that have happened during those sessions. Once we have a list of all the activities, we correlate each activity with the user session to generate a session timeline. The session timeline represents a sequential list of all activities performed in the session. Here, each session is uniquely identified by a randomly generated session ID. However, we need to make sure that the activity data is relevant.

We have been provided with a list of blacklisted programs, sensitive, confidential keyword as well as serial numbers of the USB disks which are authorized to be used in the network. Our next step is to identify if each of the events belongs to either of the blacklists and to save relevant information. Once we have a list of events that are interesting to us, we try to identify the session ID to which the event belongs. We do that by getting the timestamp of the event and trying to find out what session was active during that timestamp. In some instances, it may be possible that there would be no active session when the timestamp of the event was recorded. In such a case, people try to ignore the event because such an event may be system generated and not user-generated, which is not the objective of our system (Fig. 3).

Since we already have the list of events that have taken place into a particular session, we can combine the threat scores of each event to calculate a total threat

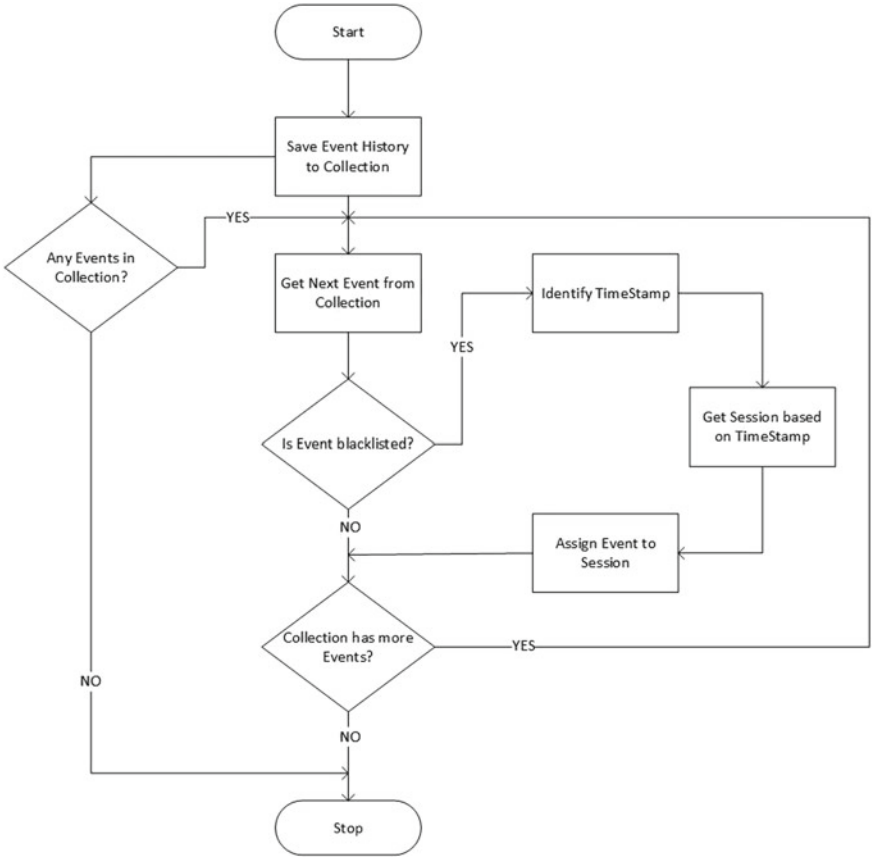


Fig. 3 Flowchart for generating session timeline

score of an individual session. Since a user can have multiple sessions across a period, we can calculate the aggregate threat score by combining the threat score of each session. A higher threat score denotes the higher possibility of an insider threat, and the security analyst can perform a further investigation in the incident.

5 Scenarios

We try to identify the usefulness of our system by applying it into some common scenarios:

Table 3 Threat score calculation for scenario 1

Event	Score
Logged in remotely	75
Accessed file with confidential information	90
Total	165

Table 4 Threat score calculation for scenario 2

Event	Score
Logged in remotely	80
Logged in out of regular shift hours	60
Total	140

5.1 Scenario 1–Exfiltration of Sensitive Data

In this scenario, an employee of the company is taking confidential company information into their private USB disk. Since we can identify the list of USB disks, which have been connected to the system as well as the timestamp of the file access, we are able to generate a threat score (Table 3).

5.2 Scenario 2–Remotely Accessing the Network from Home

In this scenario [12], an employee of the company is accessing the company network from home after office hours via remote desktop connectivity. Since we can identify the login IP address as well as a login attempt from a remote network, we are able to generate a threat score (Table 4):

6 Conclusion and Future Work

In this paper, we have scratched the surface of possibilities of detecting insider threats using forensic analysis. We presented the architecture as well as workflow for our system. In the absence of large-scale forensic data, we utilized a knowledge-engineered threat score and applied them on two different scenarios to generate a threat score. In our future work, we wish to apply our hypothesis on larger test dataset using machine learning techniques. We wish to test the accuracy of our generated threat score with proactive user behavior analysis systems [8] to identify the effectiveness of our research.

References

1. V. Visintine, in *An Introduction to Information Risk Assessment*, vol. 8 (SANS Institute, Citeseer, 2003), pp. 116
2. P. Chapman, Are your IT staff ready for the pandemic-driven insider threat? Netw. Secur. **2020**(4), 8–11 (2020)
3. K. Bhavsar, B. Trivedi, An insider cyber threat prediction mechanism based on behavioral analysis. in *Proceedings of International Conference on ICT for Sustainable Development* (Springer, Singapore, 2016)
4. S. Gaudin, Case study of insider sabotage: the Tim Lloyd/Omega case. Comput. Secur. J. **16**, 1–9 (2003)
5. G. Silowash, T. Lewellen, in *Insider Threat Control: Using Universal Serial Bus (USB) Device Auditing to Detect Possible Data Exfiltration by Malicious Insiders* (Software Engineering Institute, 2013)
6. D. Cappeli, A. Moore, R. Trzeciak, in *The CERT Guide to Insider Threats.* (Addison-Wesley, 2012)
7. H. Carvay, The windows registry as a forensic resource. Digit. Investig. **2**(3), 201–205 (2005)
8. K. Bhavsar, B. Trivedi, Predicting insider threats by behavioural analysis using deep learning. in *Proceedings of the 2018 International Conference on Security and Management* (2018)
9. C. Blackwell, A security architecture to protect against the insider threat from damage, fraud and theft. in *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies* (2009), pp. 45
10. M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, D. Gritzalis, An insider threat prediction model. in *Trust, privacy, and Security in Digital Business* (2010)
11. J.G.B. Lindauer, Bridging the gap: a pragmatic approach to generating insider threat data. in *2013 IEEE Security and Privacy Workshops* (2013)
12. L. O'Donnell, Threat Post, 23 June 2020. [Online]. Available https://threatpost.com/work-from-home-opens-new-remote-insider-threats/156841/

License Plate Recognition for Stolen Vehicles Using Optical Character Recognition

Armand Christopher Luna, Christian Trajano, John Paul So, Nicole John Pascua, Abraham Magpantay, and Shaneth Ambat

Abstract Optical character recognition (OCR) is the process of extracting the characters from a digital image. The concept behind OCR is to acquire a text in a video or image formats and extract the characters from that image and present it to the user in an editable format. In this study, a convolutional neural network (CNN) is applied, which is a mathematical representation of the functionality of the human brain, using back-propagation algorithm with test case files of English alphabets and numbers. The purpose of this study is to test systems capable of recognizing vehicle plate number English alphabets and numbers with different fonts, and to be familiar with CNN and digital image processing applied for character recognition. Scientific journals and reports were used to research the relevant information required for the thesis project. The chosen software was then trained and tested with both computer and video output files. The tests revealed that the OCR software can recognize both vehicular plate and computer alphabets and learns to do it better with each iteration. The study shows that although the system needs more training for vehicular plate characters than computerized fonts, and the use of CNN in OCR is of great benefit and allows for quicker and better character recognition.

Keywords Image processing · Signal processing · Computer vision · Optical character recognition (OCR) · Back-propagation algorithm · Convolutional neural network (CNN) · Mobile hybrid algorithm · Number plate detection · Mobile application · Android · Character extraction

A. C. Luna (✉) · C. Trajano · J. P. So · N. J. Pascua · A. Magpantay · S. Ambat
FEU Institute of Technology, Manila, Philippines

A. Magpantay
e-mail: atmagpantay@feutech.edu.ph

S. Ambat
e-mail: scambat@feutech.edu.ph

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_56

1 Introduction

Around the world, production of cars is continually increasing. According to CEIC Data Company Ltd. in (2018), the number of registered Motor vehicles in the Philippines was reported at 11,595,434 units in December 2018, a 10% increase from the previous year.

According to an open data platform called Knoema Company, private car theft rate in Philippines is 9 cases per 100,000 population. These numbers of cases in car theft increased in the year 2013−2016. With this number, this study aims to aid the police force maximize their operations through quick detection of license plates.

The current procedures of the police force are limited to documentation and application in check points. Documentation procedures are done by reported cars to be in the data of the police anti-carnapping units. Whereas application of the documents in checkpoints is to manually check the cars that pass through the area over radio communications. If the stolen vehicles have been identified by the spotter, it will be then apprehended by the authorities.

This study is a mobile application designed for image capture and pre-processing, verification of vehicles license plate number against a database simulating the national record of reported lost and stolen vehicles. This application will use optical character recognition to identify the license plate. After determining the character details of the license plate, this is then searched against a cloud database of car plates tagged as "hot cars." After that the user will be able to determine if the car is stolen or not. This application can be used in numerous police and other government checkpoints to minimize the rate of car theft in the country by having access to the country-wide database at the palm of the user's hands. This can be used to efficiently find the vehicles that are stolen by checkpoint identification and apprehending the driver. This would help the car owners and the authorities trace lost or stolen vehicles faster. This can help minimize the thousands of stolen cars reported in the police records.

2 Methodology

In this part, the step-by-step process on how the application works is discussed. Figure 1 shows overall use of the application.

The conceptual framework is the input, process, and output model that shows the stages of the project. First, the user will login in the application. The user can also create an account, and it will be verified by the administrator. If the account is does not exist, a message will be prompt that there is no account. After logging in, the user can scan the license plate through a video using the smartphone. The user can also choose to report new stolen vehicle with its licensed plate number. If the user chose to take a picture, the image will go through image processing and undergo the process of optical character recognition. After recognizing the character of the

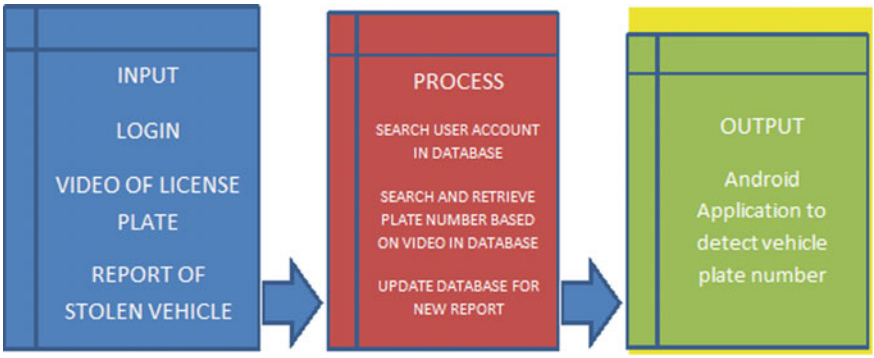


Fig. 1 Conceptual framework

licensed plate, the information about the vehicle will be shown in the screen of the smartphone, if it was stolen or not. On the other hand, if the user chose to report, the user will need to input the data needed. The system will automatically pop up a notification that there is a new hot stolen vehicle and will show the license plate.

During the process, Fig. 2 shows the flow starting with the input through the camera. The Mobile OCR algorithm has the following steps:

(1) **Image Detection.** Image detection is performed with a snap of an image is captured from the video output.

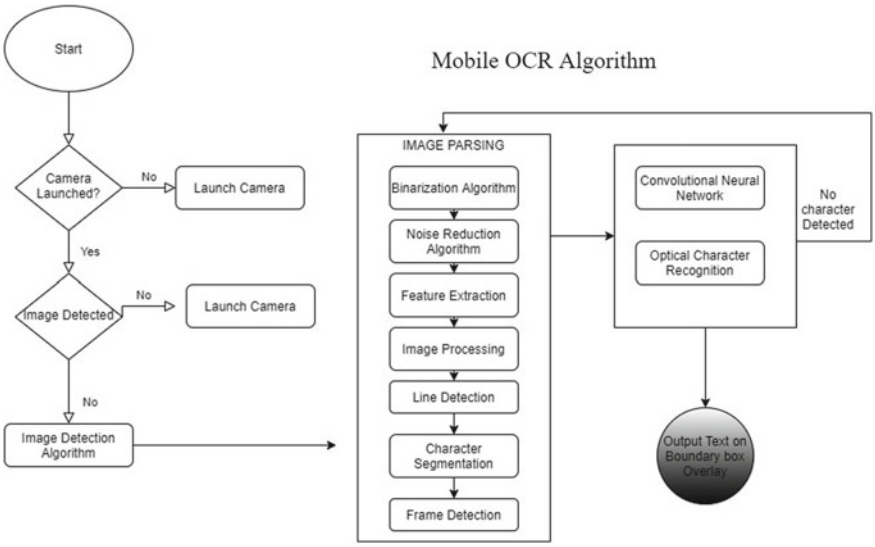


Fig. 2 OCR algorithm

(2) **Image Binarization.** Binarization is performed on the captured image. Performing the reduction of a grayscale image to a binary image. The algorithm assumes a foreground of black pixels and background of white pixels. It then checks the optimal threshold separating the two-pixel classes to a minimum variance between the two.

(3) **Noise Reduction**. Noise reduction is then performed to remove distortions in the image for a clearer copy.

(4) **Feature Extraction.** Feature extraction is performed to identify distinct features of the image highlighting lines that may represent characters in the image.

(5) **Frame Detection.** Frame detection is performed to detect the boundary of the identified lines in the image.

(6) **Line Detection**. The Line detection is performed identifying lines of text found and analyze finding the adjacent space between lines to analyze potential characters. A Y projection of the image binary finds location with a pixel count less than a specific threshold. Potential lines are identified and further analyzed to confirm.

(7) **Convolution Neural Network (CNN).** The convolutional neural network searches through the image and identifies pixels in the foreground. They are marked as "blobs" or potential character. After each character is found, CNN identifies similar characters and compares width to correct extraction of characters as shown in Fig. 3.

(8) **Word Recognition.** The word recognition starts after finding all of the possible character "blobs" in the document, Tesseract does word recognition word-by-word, on a line-by-line basis. Words are then passed through a contextual and syntactical analyzer which ensures accurate recognition.

(9) **Optical Character Recognition (OCR).** The OCR identifies characters through blobs and presents an output of the characters that is compared against the database.

(10) **Detected Characters**. An output of the detected characters is placed in a boundary box and is overlaid in the video output. This is placed close to the location of the detected text.

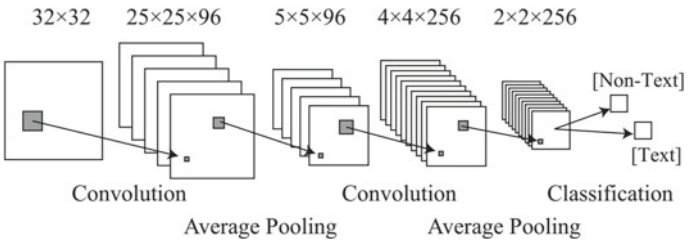


Fig. 3 Convolutional neural network character recognition

The combinations of the following algorithms create a dynamic and efficient performance for the application to run in mobile phones. It is both minimal in processes and refined in character detection. The equations used are as follows:

This mathematical formula explains the how the functions r and s process in CNN

$$(r * s)(g, h) = \sum_{d=-\infty}^{\infty} \sum_{c=-\infty}^{\infty} r(c, d)s(g - c, h - d) \tag{1}$$

Where "r" (XXY) represents image and "s" as the kernel which have a finite element number in points:

$$(r*s)(g, h) = \sum_{d=h-b}^{h+b} \sum_{c=g+y}^{g+y} r(c, d)s(g - c, h - d) \tag{2}$$

3 Results and Discussions

In this section, the findings of the research are discussed together with the obtained output from testing the application.

Figure 4 shows a screenshot of the application performing real-time plate number recognition with the vehicles.

The application has been determined to detect multiple cars concurrently. Out of 58 cars tested 50 cars were identified at a 100% accuracy rate at a distance of 3 m. 2% of the car plates was recognized at a distance of 3 m and 6 m. This dropped to further 2% of the cars were only recognized at a distance of 3.6 and 9 m. Some 2 percent of the cars were recognized at 2 m and the remaining 4% was not recognized at all by the application. This can be determined due to the condition and readability of the plate from distortion to dilapidation. See Fig. 5a.

Figure 5b indicates an average minimum of 4 s for typing a plate number manually and 2 s average to detect the plate number no matter the length of the plate. This indicates automatic plate identification having an edge over manual typing of the plates and factor of human error can be overridden by automatic detection with multiple queries with the database on all possible results. The advantage of concurrently detecting multiple plates and zooming into plate video to better detect the characters. According to Bessmeltsev [6], automatic OCR has a 100% accuracy and processing time depending on image quality is processed in milliseconds (Table 1).

The overall functionality of the application tallied a total average of 4.84 (96.8%) which shows an excellent remark and greatly reflects the ability of the application's functions. The application was easily learned and used after the demonstrations showed which resulted to an excellent remark with a total usability average of 4.65 (93.0%). The overall reliability of the application was evaluated as excellent having a

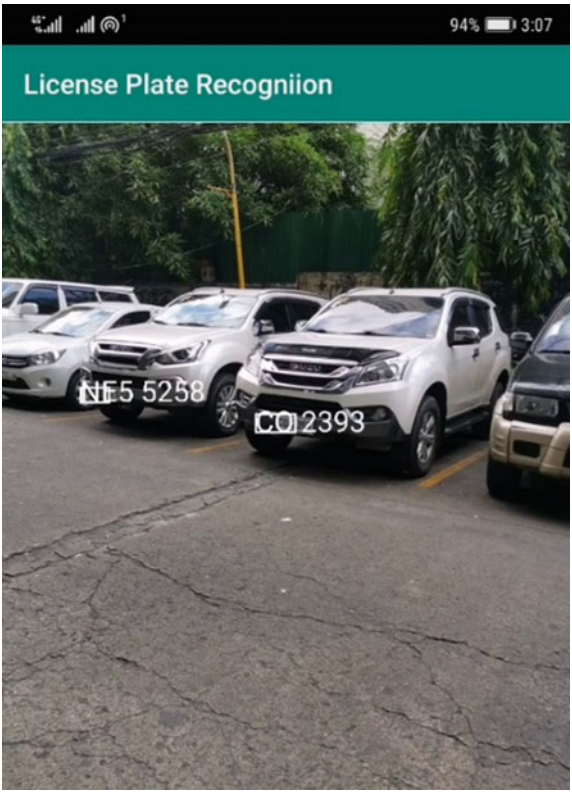


Fig. 4 License plate recognition application

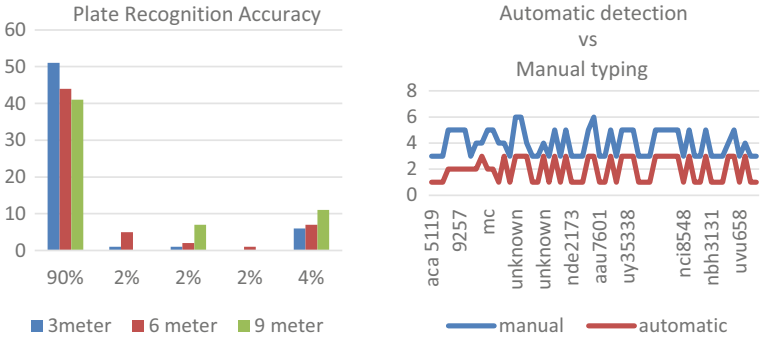


Fig. 5 Recognition accuracy (**a**) Automatic versus manual (**b**)

Table 1 Summary of findings

Category	Weighted mean	Interpretation
Functionality	4.84	Excellent
Usability	4.65	Excellent
Reliability	4.80	Excellent
Performance	4.71	Excellent
Supportability	4.77	Excellent
Total average	4.75	Excellent

weighted average of 4.80 (96.0%). This implies that the application performed consistently and shows efficient results. The performance of the application and its ability to give adequate results with the given workload was tested providing an average of 4.71 (94.2%) and shows an excellent remark. Finally, with a total average of 4.77 (95.4%), the supportability of the application gives an excellent remark. This depicts that the developers opened to enhance the application's supportability with open user-feedback and error-checking. Overall, the application for License Plate Recognition for Stolen Vehicles using Optical Character Recognition is considered by the Government Officials particularly mobile traffic officers and Far Eastern University–Institute of Technology Information Technology and Computer Science students to be an excellent application with a weighted average of 4.75 (95.0%). This shows that can the application can detect incoming licensed vehicles, shows if the vehicle is stolen, and report possible stolen cars white space above the section head.

4 Conclusion

Prior to the given project objectives, the researchers are successful in building and developing an anti-carnapping application using portable camera embedded in smartphones, specifically an application for Android users. This will greatly give assistance and support for police checkpoints to enhance and give speedily checking of cars. For the applications functionalities, the system applied the following concepts, tools, and algorithms. Firebase real-time database for database indexing algorithm, Binarization, Image Detection, Noise Reduction, Frame detection, Feature extraction, Line detection, Character Segmentation. The white or default color implies that the car in the camera has no violations and red for hot plates (carnapped unit). Users can easily detect car with violations with the color-coding function. Overall, the results of the assessment justify that the application is functional, usable, reliable, functional, and efficient. It successfully gives additional support to users with information and operation it provides.

5 Recommendation

The researchers recommend the following for the future users of this study: (a) to design and develop the application in different platforms and operating system like iOS version to expand the number of users and possibility to attain different results. This is to consider the effects of different modern technology with the same objective of the software. (b) The proponents also recommend improving the plate and character recognition algorithm, this is to obtain a more accurate result and faster performance. (c) To update the database by adding more licensed plates data, to cover a wide range of vehicle available for scanning. (d) To provide efficient lighting in the device that is used, this will greatly enhance the licensed plate recognition for rainy season and nighttime. (e) It is also recommended to add more cars in the live camera, and this will greatly enhance the detection rate. Since this application is only limited to detection one car at a time for checkpoints. With multiple detection, the application will not be limited to police checkpoints and can be applied to main roads and highways. (f) To update the camera features with current trends and innovations, this will help to improve the camera function and keeps the application up to date with the current trend, and lastly, (g) The researchers recommend adding statistics and forecasting models and modules to give and enable the users the ability to check summary of all the results and detect possible attacks of stolen vehicles. (h) To record all detected plates and store in a database for data collection and archiving for future reference and data-mining purposes. (i) To develop a server to store all detected and archived plate numbers as reference.

References

1. C.R. Albis, V.R. Bernardo, M.S. Wong, *Application of Artificial Neural Network* (De La Salle University, Manila, 2007)
2. C.-N. Anagnostopoulos, I. Anagnostopoulos, V. Loumos, E. Kayafas, A license plate-recognition algorithm for intelligent transportation system applications. IEEE Trans. Intell. Transp. Syst. **7**(3), 377–392 (2006)
3. Automatic vehicle license plate recognition with color component texture detection and template matching. (2013). Retrieved from Academia.edu: https://www.academia.edu/17307565/Automatic_vehicle_license_plate_recognition_with_color_component_texture_detection_and_template_matching
4. J. Belandres, X. Crisostomo, M. Estrada, I. Tilbe, *Techy Bartender: Augmented Reality* (FEU—Institute of Technology, Manila, 2019)
5. J.H. Bernil, D.L. Michael, G.H. Rivera, E.L. Sembrano, R.M. Yu, *A License Plate and Road Violations Recorder System for Buses in EDSA* (De La Salle University, Manila, 2015)
6. V. Bessmeltsev, E. Bulushev, N. Goloshevsky, High-speed OCR algorithm for portable passport readers. Graphicon **11**, 25–29 (2011)
7. S. Bhatia, A.P. Nagare, License plate character recognition system using neural network. Int. J. Comput. Appl. **25**(10) (2011). https://doi.org/10.5120/3147-4345
8. S.A. Binayug, E.O. De la Cruz, J.G. Raymundo, *License Plate Recognition with Skew Detection and Corrrection Method for New Plates in the Philippines* (Mapua Institute of Technology, Manila, 2016)

9. Buying a Car in Philippines: Comprehensive Guide for Smart Filipinos. (2018, June 20). Retrieved from Cashmart: Your Online Lending Partner: https://cashmart.ph/buying-car-in-philippines/
10. D.B. Carandang, *ITEXT: A Mobile Application for Converting Present Text in Images to Mobile Text Format Using Text Detection Algorithm* (Technological Institute of The Philippines, Manila, 2018)
11. J.S. Castillo, A.P. Tanjutco, A.C. Valdez, *LiPID: License Plate Identifier: A Motor Vehicle License Plate Recognition System Using Ant Colony Systems and Support Vector Machines* (University of The Philippines Diliman, Quezon City, 2005)
12. S. Ch, S. Mahna, N. Kashyap, Optical character recognition on handheld devices. Int. J. Comput. Appl. **115**(22), 10–13 (2015). Retrieved from semanticscholar.org
13. H.C. Chavez, F.P. Conag, L.C. Tamondong, *Citycop: Crime Reporting Android Application Utilizing Firebase Database System and Google API* (Technological Institute of The Philippines, Manila, 2018)
14. C. Cruz, How to Deal with Car Theft in the Philippines (2017, July 21). Retrieved from Carmudi Philippines: https://www.carmudi.com.ph/advice/general-car-advice/how-to-deal-with-car-theft-in-the-philippines/

A Meta-Analysis on Online Classes for Hotel Management Students at Chennai During Covid-19



T. Milton and H. M. Moyeenudin

Abstract Teaching in the hotel management courses involves both practical and theory classes, as this is a skill based professional and practical oriented course were teaching has to encompass 50% of practical lab classes to develop the skills and talents of the students and the remaining 50% for teaching theory, which imparts knowledge to understand the concepts, and ideas accordingly to operate in the departments of hotel industry. Since learning provides an opportunity to student on acquiring new knowledge and skill with a positive attitude that motivates them to work in hotel industry, due to the outbreak corona virus which has disrupted the classroom teaching and thrown into disarray of practical and theory classes along with exam schedules, in addition to force the students and teachers to stay in indoors. The purpose of this study is to recognize the best tools in handling online classes. Furthermore, to know their participation in online classes with comparison of offline classes. However, teaching and learning process have not been stopped with the latest technology to meet the drift by Covid-19 pandemic situation, social media application (SMA) acts as a right tool for teaching and learning process.

Keywords Impact of online classes · Paradigm · Learning · Teaching

1 Introduction

The current technology provided a powerful tools for teaching through online which works beyond the classroom walls, through teaching students at their homes and also by bringing a pattern shift in the teaching–learning process. The severe crisis exist through Covid-19, will eventually end; however, it is not clear how long this disruption is going to occur although every disruption teaches us to emerge stronger, sharper

T. Milton (✉)
Tourism and Hospitality Management, Bharath Institute of Higher Education and Research, Chennai, India

H. M. Moyeenudin
School of Hotel and Catering Management, Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_57

and more nimble, in addition to learn so much of skills with a deeper knowledge to understand. Due to Covid-19, the teaching through online classes has taken the place of regular classroom teaching, almost many universities and affiliated colleges in Chennai have adapted to this online teaching method by conducting classes in Google meet, Zoom, WebEx and Google class room modes to facilitate students to learn and participate from home [1]. The impact of online teaching for hotel and catering management students has a combination of results. Few have responded that this method is easy to understand, whereas others say face to face teaching can't be replaced with online classes especially in hotel and catering management because they need to have practical classes as this course is practical oriented, although it is a professional course where learning skills is a significant factor. Education provides new knowledge about the World. It enables every human being to live their life in a better manner, which offers a wisdom to understand the good and bad by giving us a new dimension of looking at life through a foundation stone for everyone that provides assistance in building opinions and has a various view about things in life and also enlarges our vision by makes us to come out with different inventions and discoveries [2]. Teachers must be spearheading this change and try their level best to divulge the knowledge to students [3].

1.1 Impact on Hotel Management Education

In view of hotel management education, it provides a professional career for students as an administrators, executives, chefs and also as entrepreneurs. In the educational sector, this had a great impact with teaching methodology that has to change from the traditional classroom teaching to virtual online teaching mode Can [4]. Nearly, all educational institutions are forced to close but they have great responsibility to teach the students and cope up with this situation [5]. Due to the Covid-19 pandemic, the students were not able to get proper learning from the teachers. Online classes were the only source of contacting students [6]. There are many online tools could be used for teaching in a better way, since it is essential that can help these students with both the information and practical knowledge.

2 Literature Review

Due to Covid-19 pandemic, there is no face-to-face interactions by individual education system switched to online education. Despite the fact that students have the opportunity to access the computers and free internet at their education institution, whereas there is a query on knowing the facilities of electronic gadgets and internet access at their home, as they belong to different background [7]. Due to the Covid-19 outbreak, many universities and education institutions have faced a rapid change in educating students. In spite of various difficulties experienced by educators in the

event of instructing and for students in learning on the web, a surprising update is an ambiguity leading to online classes. The students of education institution must realize the importance of studies and acts as a part of this system by cooperation with online classes for their better future endeavors [8]. The education institutions and government must guarantee the accessibility of internet to students with a specialized instruments, excellent computerized experience for students may keep them motivated, and by advancing through innovative empowered learning for students to connect the inconsistencies faced during COVID-19 calamity [9]. Further there are challenges with communication due to internet connectivity issues. Consequently, every one of these components ought to be thought of while building up an online course to make it more successful and profitable for the student. It's conceivable that once the COVID-19 pandemic settles down [10]. Notwithstanding the difficulties to the staff, existing exploration demonstrates that over 60% of students tend to have vague future aptitude and objectives, need dynamic education association that invest more energy in-class as student's participation is very less with online class contrasted with the time spent in regular classroom [11]. There is an anxiety and stress among students on attending online classes that could be reduced by mentoring in an effective way in order to make them participate in web based learning [12]. The online education has created an entire innovative phase for teachers and students of world due to Covid-19 outbreak. Online training expects educators to transform from the old pattern of teaching to new instructing techniques that likewise coordinates with recent upgrades of online. [13]. In addition, there is no favorable learning conditions at home, eventually they lost their interest through online education [14].

3 Methodology

A research is initiated with a quantitative questionnaire having the variables of online teaching. The questionnaire is circulated among the hotel management students of Chennai city, and it is prepared in the way of Google forms. Data were received from hotel management Students of various Institutes and universities of Chennai out 380 responses only 315 responses are valid and used for this analysis. To understand the students participation at online classes and to find out their desire with apps in comparison with a traditional teaching methods. A mean statistics is done to know their usage on social media applications (SMA) further a correlation is carried out to distinguish the relationship among variables of online classes, further a linear regression is carried out to recognize the strength of online class variables.

4 Results and Discussion

A comprehensive analysis is carried to know the hotel management student's curiosity on online application for studies and also to recognize their wish on learning

Table 1 Mean on social media application acceptance

Online class acceptance * SMA			
Online class acceptance			
SMA	Mean	N	Std. deviation
YouTube	3.8819	237	0.32346
WhatsApp	3.8462	78	0.36314
Total	3.8730	315	0.33348

with teaching methods in order to offer a precise as well as sophisticated teaching method. The mean statistics is done to classify the collection of data with the average numbers or value to know the probability with the entire data along with standard deviation for acceptance on SMA, online apps used for teaching in education institution further on knowing the preferred app. Thus, a correlation analysis is performed to know the relationship between the variables of online teaching with its acceptance. A regression is performed to know the association between the independent and dependent variable with offline classes, online classes, comfort on apps, comfort on online exam, time spent in online class, acceptance on online class.

4.1 Mean Statistics

The SMA's are used by individual interest and in this study, it is presenting the usage by hotel management students in Chennai. The mean on using SMA is displayed in Table 1. Though the students have a blend of choice on using the social media some of them are their favorite, in this juncture, the study focused to know the social media application (SMA) used by hotel management students. There is a mean value 3.8819 with a standard deviation 0.32346 for the usage of YouTube among social media app around 237 students opted from the total number of 315. However, some students also opted WhatsApp as a preferred social media app for studies with a mean value 3.8462, and a standard deviation of 0.36314.

4.2 Online Class Acceptance on APP

The mean statistics shows the preference of teaching faculties on teaching the subjects by using online tools for video conferencing in Table2 the outcome of the data collected from a quantitative questionnaire is favoring the Zoom application with a Mean value 3.9331 and Std. Deviation 0.35405, evidences the usage significantly for teaching, in addition Google Meet also used for the same purpose through a Mean value 3.3226 Std. Deviation 0.47519, here the maximum number say zoom 284 among 315 responses. Evidently proved as a best tool in teaching. Yet Google Meet is also a right tool for teaching through online. Here, the majority vary according to

Table 2 Mean online app used for teaching

Online class acceptance * Online app used			
Online class acceptance			
Online app used	Mean	N	Std. deviation
Zoom	3.9331	284	0.25029
Google Meet	3.3226	31	0.47519
Total	3.8730	315	0.33348
Total	3.8730	315	0.33348

the app preferences and flexibility in future. As there is no time limit for classes in Google meet, it can become a more predominant by adding some missing features in comparison with Zoom App.

4.3 Online Class Acceptance on Favorite APP

See Table3.

Hotel management course comes with a blend of subjects, which are been as departments in hotel, thus each department is thought as subjects in this course, as all it requires a practical exposure in this course. It is designed in such a way to impart practical skill along with theory. This is the reason YouTube videos are having a Mean value 3.8538 and a Std. Deviation 0.35405 with number of preference 253 out of 315 there is no doubt that YouTube becomes as their choice in learning. Thus, the recorded practical videos will support them well in learning process. Especially for the students of hotel management course this online tool is a prime SMA than any other. Since the hotel management course deals with practical oriented subjects. There are various decision and plans are taken to prevent the spread of the novel corona with the forms of education structure that are changing with online training turning into the essential methods for guidance to colleges and education institutions already to meet the demands of education. The investigations are showing that greater part of the students manifested an uplifting perspective toward online classes during

Table 3 Mean on favorite app used by students

Online class acceptance * Favorite app			
Online class acceptance			
Favorite App	Mean	N	Std. deviation
YouTube	3.8538	253	0.35405
WhatsApp	3.9516	62	0.21633
Total	3.8730	315	0.33348

Table 4 Correlation between the variables of online education

Correlations						
		Offline class	Online class accp	Time spent online	Online exam	Like practical
Offline class	P. Correlation	1	−0.535**	−0.050	0.278**	0.571**
	Sig. (2-tailed)		0.000	0.378	0.000	0.000
	N	315	315	315	315	315
Online class acceptance	P. Correlation	−0.535**	1	−0.326**	−0.340**	−0.230**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000
	N	315	315	315	315	315
Time spent online	P. Correlation	−0.050	−0.326**	1	0.426**	−0.097
	Sig. (2-tailed)	0.378	0.000		0.000	0.086
	N	315	315	315	315	315
Online exam	P. Correlation	0.278**	−0.340**	0.426**	1	0.018
	Sig. (2-tailed)	0.000	0.000	0.000		0.754
	N	315	315	315	315	315
Like practical	P. Correlation	0.571**	−0.230**	−0.097	0.018	1
	Sig. (2-tailed)	0.000	0.000	0.086	0.754	
	N	315	315	315	315	315

** Correlation is significant at the 0.01 level (2-tailed)

this pandemic period. Despite fact in Hotel and Catering management education, the outcomes are favoring in practical classes. In Table 4.

4.4 Correlation Analysis on Variables of Online Classes

The investigations are showing that greater part of the students manifested an uplifting perspective toward online classes during this pandemic period. Despite fact in Hotel and Catering management education, the outcomes are favoring in practical classes. In Table 5, the variables of online education are negatively associated with interest of students, whereas there is greater significance for practical class with offline class with a stronger correlation value $r = 0.571^{**}$ and a significant value $p = 0.000$. This

Table 5 Summary of predictors

Model summary	
R square	Adjusted R square
0.169	0.158

a Predictors: (Constant), Issues By Online Class, Time Spent Online, App Comfort, Online Exam

study results also shows a strong correlation value $r = -0.340^{**}$ with a significant value $p = 0.000$ for variable online exams and online class acceptance. The time spent on attending online classes shows a sturdier correlation value $r = -0.326^{**}$ and significant value $p = 0.000$ for a negative association. Similarly, there is a negative association for attending practical through online with a good correlation value $r = -0.230^{**}$ and a significant value $p = 0.000$. This evidences that the hotel management students are not satisfied with the online education in regard with practical. However, there is a resilient correlation value $r = 0.426^{**}$ with a significant value $p = 0.000$. Which signifies a positive relationship on time spent on online to attend their exams.

4.5 Linear Regression

Online education is the best way to handle classes of higher education, due to some inadequate facilities like paid internet, availability of electronic gadgets with an android facility has become a challenge for the students of low income groups in India, Table 5. Indicates the *R* Square 0.169 proves that there is a difficulty with the access of online classes as the predictors are issue from online class, time spent online, app comfort and online exam.

4.6 Anova Test

The variables of online education are the time spent during online classes to identify their participation at online classes, then App Comfort, Online Exam and Issues in Online Classes. Table 6 represents the relationships between the variables, there is a significant association between the dependent variable as the F value is 15.745 with

Table 6 Coefficients of online class acceptance

Coefficients[a]						
model		Unstandardized coefficients		Standardized coefficients	t	Sig
		B	Std. Error	beta		
1	(Constant)	45.501	4.310		10.558	0.000
	Time spent online	−0.188	0.050	−0.217	−3.790	0.000
	Online exam	0.199	0.051	−0.226	−3.866	0.000
	App comfort	0.123	0.058	0.113	2.127	0.034
	Issues in online class	−0.413	0.625	−0.034	−0.661	0.509

[a] Dependent Variable: Online Class Acceptance

Table 7 Anova test with the variables of online classes

ANOVA[a]						
Model		Sum of squares	df	Mean square	F	Sig
1	Regression	2802.012	4	700.503	15.745	0.000[b]
	Residual	13,792.451	310	44.492		
	Total	16,594.463	314			

[a]Dependent Variable: Online Class Acceptance
[b]Predictors: (Constant), Issues In Online Class, Time Spent Online, App Comfort, Online Exam

a lesser p value = 0.000b. Here, the independent variables can predict the dependent variable online class acceptance. There is a strong association observed among these coefficients like Time Spent Online, Online Exam, App comfort and the Online Issues with a dependent variable online class acceptance.

Table 7 denotes the coefficients value with the dependent variable as ($b = -0.188$, $p = 0.000$) for time spent by students of Hotel and Catering management which is little negatively associated online class acceptance proves that some students cannot able to participate completely, in addition to their participation in online exams has a value ($b = -0.199$, $p = 0.000$) signifies a minimum difficulty in participation further the coefficient app comfort is positively associated with a value ($b = 0.123$, $p = 0.034$), as Google meet and Zoom app are comfortable in online classes. To know the issues faced by the students a coefficient issue in online class is negatively associated with the acceptance of online class with a value ($b = -0.413$, $p = 0.509$). The outcome of regression shows a clear evidence on issues faced by students by online classes.

The offline classes are favorable for the practical used to be conducted further there is an interest on learning with online classes also noticed. However, students have started to adapt the change in teaching there are some controversies in regard with practical classes, which shown in Fig. 1. A group of students showing their interest in learning practical subjects through offline classes by a regression curve displays the plots to closer and above 90% on learning through online. Traditional teaching is mostly applied in Indian education Industry, further this system need to be more advanced that could provide an opportunity to students in participation of online classes [14]. Acceptance of online classes among students can be achieved with a blend teaching using suitable applications [15]. The time spent during online term exams shows a significant results between the participation of students in Fig. 2. But the time taken to complete their exams are lesser that the normal time taken when they participate in traditional term exams with the regression curve, it is proved that the maximum time taken is not above 60% and many have completed their exams early than the time taken to complete, and there is an opportunity to cheat during online exam as many go out of the camera [16]. There is a decrease in time spent at online classes, which is evidenced by a scattered plots of a regression curve in Fig. 3. Students have varied choices when they use electronic gadgets as there are many options for students to get engaged with SMA, although many have participated

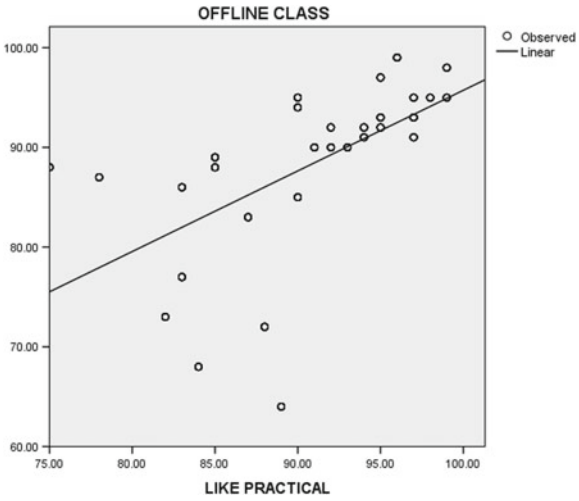


Fig. 1 Acceptance of offline

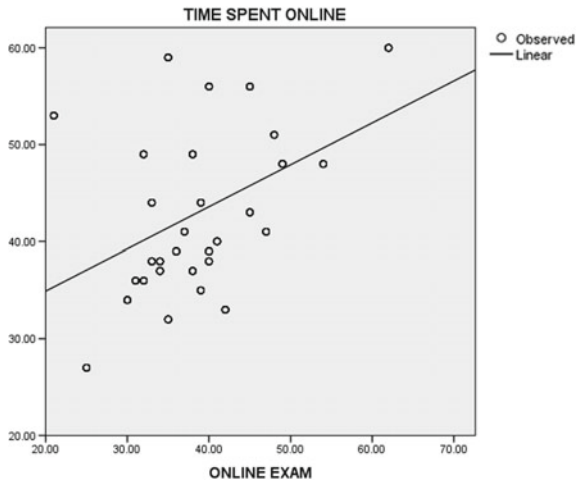


Fig. 2 Time spent on online exam practical classes with a regression curve

in online classes with the apps like Google meet and Zoom App, there may be the negligence due to their family responsibilities. Representation from Fig. 4, on participation of students in online classes with the time spent shows a lesser time span this may be, due to the work load given by their family as many students are involved in household jobs during their online classes, which makes their lesser participation eventually that will also reduce their time spent on online classes [17].

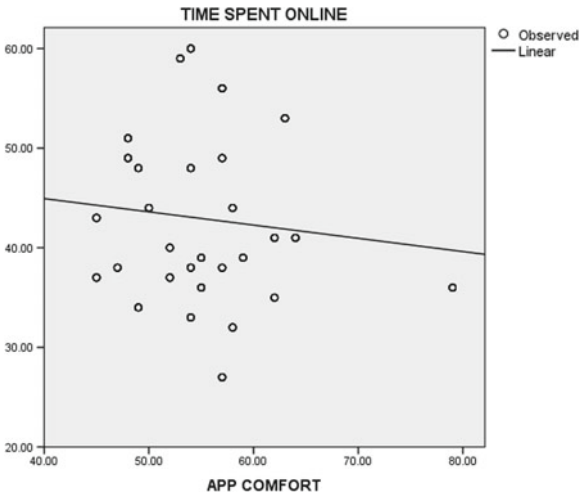


Fig. 3 Time spent on online classes

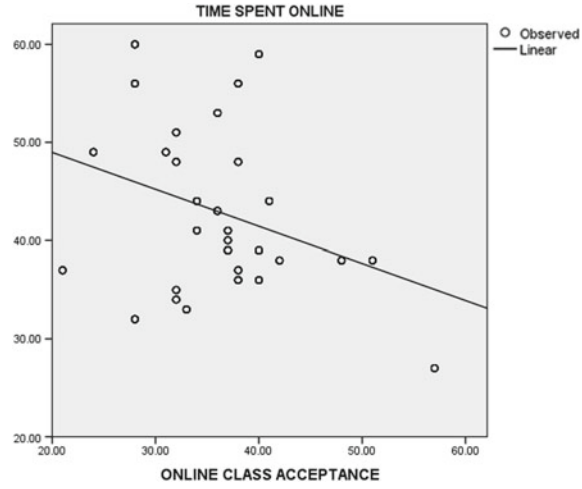


Fig. 4 Time spent on online classes with the app comfort

5 A Discussion on Teaching and Learning

An online discussion is carried to know the difficulties of teaching and learning with selective faculties and students, in light of perceptions toward internet education for Hotel and Catering management students. Online education with teaching faculties have fewer command and control over students as the class connected with internet, and students are bound to "avoid the class." Consequently, the advancement of web based instructing and its learning adequacy generally rely upon the quality or interest of an individual student, whereas in traditional classes the student can be controlled in front. There are some reasons make them disconnected like lacking orientation

study and readiness toward online materials, a little amount of contribution in class conversations, rather than in traditional classroom an elaborate discussions are made, in online deficient conversation profundity, also, those issues ought not be ignored in web based instructing. To take care of such issues that is based on education through online, teaching faculties ought to make the instructions in various segments, the disconnected stage on making assignments and next in presenting their work through online. In the disconnected segment, students are needed to peruse the course-specific writing and submit short papers dependent on their perusing of key materials before the class. Teaching faculties ought to give input on their performances and tasks, I order to assure the students about their learning intellectual degrees [18]. Along these lines, faculties also can share the teaching content before the class which will aid in understanding about the subject. During the online class, faculties should utilize a conversation segment and most importantly providing their recorded teaching content will help those who have internet connectivity issues.

6 Conclusion

There are various views on online education especially during the contagion Covid-19 situation, although this is a best tool for educating students at their home, which also motivate them for a better prospect, rather than being idle with stress and anxiety by thinking about their education and future. There are some barriers identified through the outcome of this meta-analysis which indicates the impact of online classes for hotel management students of Chennai. Nevertheless, teachers and students are not fully accustomed to the online mode of classes. Students are focused toward learning subject through practical classes as they belong to hotel management course. In addition, they have their higher participation toward YouTube videos, so the recorded practical videos will be a better option to educate as the time spent in online classes shows ($b = -0.188$, $p = 0.000$). The teachers have to be taught about the various ways to conduct the hotel management subjects in an interesting and innovative way. They should be given proper orientation and training in this skill. In addition, students need to be informed about the facilities and utilization. The students should learn how to attend the classes in online mode and should respond in a proper way with their difficulties in attending classes with online connectivity or inadequacy of gadgets.

Limitations of this Study

The results are obtained from the students of Hotel and Catering Management Institutes of Chennai, and there may be chances of varied opinion with other specialization like engineering, science and commerce. In addition, this study carried only in Chennai, students from suburban areas or villages are not included.

References

1. F. Pucciarelli et al., Competition and strategy in higher education: managing complexity and uncertainty. Bus. Horiz. **59**(3), 311–320 (2016)
2. E. Andrew et al., Compensating for academic loss: online learning and student performance during the COVID-19 pandemic. China Econom. Rev. **68** (2021)
3. C. Rapanta et al., Online university teaching during and after the Covid-19 crisis: refocusing teacher presence and learning activity. Postdigit. Sci. Educ. **2**, 923–945 (2020)
4. C. Doruk et al., Understandability, and quality of online education materials for vocal fold nodules. J. Voice **34**(2), 302.e15-302.e20 (2020)
5. Y. Huang, N. Zhao, Generalized anxiety disorder, depressive symptoms and sleep quality during COVID-19 outbreak in China: a web-based cross-sectional survey. Psychiatry Res **288** (2020)
6. D. Ibrahim et al., Understanding the most important facilitators and barriers for online education during COVID-19 through online photovoice methodology. Int. J. Higher Educ. **10**(1), 166–190 (2021)
7. A. Qazi, K. Naseer, J. Qazi, H. AlSalman, U. Naseem, S. Yang, G. Hardaker, A. Gumaei, Conventional to online education during COVID-19 pandemic: do develop and underdeveloped nations cope alike. Children Youth Serv Rev **119** (2020)
8. L. Mishra, T. Gupta, A. Shree, Online teaching-learning in higher education during lockdown period of COVID-19 pandemic. Int. J. Educ. Res. Open **1** (2020)
9. T. Muthuprasad, S. Aiswarya, K.S. Aditya, Girish K. Jha, Students' perception and preference for online education in India during COVID-19 pandemic. Soc. Sci. Humanit. Open **3**(1) (2021)
10. A.E.E. Sobaih, A.M. Hasanein, A.E. Abu Elnasr, Responses to COVID-19 in higher education: social media usage for sustaining formal academic communication in developing countries. Sustainability **12**(16), 6520 (2020)
11. W. Bao, COVID-19 and online teaching in higher education: a case study of Peking University. Human Behav. Emerg. Technol. **2**(2), 113–115 (2020)
12. D.S. Lorico, An effective blended online teaching and learning strategy during the COVID-19 pandemic. Educ. Chem. Eng. **35**, 116–131 (2021)
13. N. Kapasia et al., Impact of lockdown on learning status of undergraduate and postgraduate students during COVID-19 pandemic in West Bengal, India. Children Youth Serv. Rev. **116** (2020)
14. M. Adnan, K. Anwar, Online learning amid the COVID-19 pandemic: students' perspectives. J. Pedagogical Sociol. Psychol. **2**(nmber1), p45-51 (2020)
15. S.K. Mathivanan, P. Jayagopal, S. Ahmed et al., Adoption of E-learning during lockdown in India. Int. J. Syst. Assur. Eng. Manag. (2021)
16. A. Jabbar, C.G. Gauci, C.A. Anstead, Parasitology education before and after the COVID-19 pandemic. Trends Parasitol. **37**(1), 3–6 (2021)
17. E. Bilen, A. Matros, Online cheating amid COVID-19. J. Econ. Behav. Organ. **182**, 196–211 (2021)
18. I. Asanov et al., Remote-learning, time-use, and mental health of Ecuadorian high-school students during the COVID-19 quarantine. World Developm. **138** (2021)

Traveling Salesman Problem Solution Using Plate Tectonics Based Neighborhood Search Optimization



Lavika Goel

Abstract Traveling salesman problem (TSP) is one of the most fundamental constraint satisfaction and optimization problem in computer science and engineering. In this paper, we have adapted the plate tectonics based neighborhood search optimization technique on this problem. This theory explains and describes the large scale motions of Earth's lithosphere. This actually motivates the application of plate tectonics and create a new paradigm, i.e., plate tectonics based neighborhood search optimization. PBO search technique find solutions for the traveling salesman problem (TSP) which depend very much on the way the initialization part is handled. We have used biogeography based optimization BBO for it and also tried many crossover operators in it. As the movements along the paths in solving TSP problem are continual and happen to be very stable, it naturally induces optimized solution of a function by choosing the most stable position. The proposed algorithm can exploit the local information available from the gradients of the function, while also allowing for exploration to scout for better solutions throughout the search space. This allows the algorithm to improve the known solution in each iteration and locate the global minimum efficient. Our results are comparable to ACO and PSO. For the dataset Att48, the number of cities are 48, and the optimal cost is 33522. The cost using ACO and PSO are 33,514.1 and 33,534.2, respectively, whereas the cost using PBO is 33, 537.1. For this case, the cost by PBO lies between ACO and PSO. The cost is better than ACO. Comparable results of many datasets are discussed in the paper.

Keywords Optimization · Evolutionary algorithms · Plate tectonics · Restricted neighborhood search · TSP

1 Introduction

Optimization problems are indispensable in most fields of science, engineering, and technology. However, finding the global optimum (or a good approximation) of a

L. Goel (✉)
Department of Computer Science and Engineering, Malaviya National Institute of Technology, Jaipur, India
e-mail: lavika.cse@mnit.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_58

multivariate function is a challenge as the variables that define the function can be continuous or discrete and, in many cases, need to satisfy certain constraints. It is well known that these problems belong to the class of NP-Hard problems. TSP is one of them. Given a set of cities, the traveling salesman problem is to find a route of cities with some constraint such as each city should be visited exactly once and the salesman has to come back to the starting city. We have to find the minimized tour. The traveling salesman problem can be discussed as follows: Given a set of cities which can be represented as nodes of the graph. The cost to travel from one city to another is weight represented on edge of the graph. The problem is to find a route of cities with constraint such as each city should be visited exactly once, and the salesman has to come back to the starting city and this route should be the one with minimum cost. The basic and known to be exact solution is to iterate all the tours and then find the cost of each of them and solution will be the minimum cost. This approach is easy but with large number of cities will become impossible to solve in finite amount of time. As the time to solve with, this approach is exponential.

2 Literature Review

The traveling salesman problem has been studied since the eighteenth century; however, evolutionary algorithms have been recently very popular as they are very easily able to solve this problem. Sarit Wagner analyzed the standard traveling salesman problem and proposed ant colony-based approaches [1, 2]. İsmail Babaoğlu suggested an improved particle swarm optimization (PSO) [3]. ShowkatGani gave an algorithm for traveling salesman problem with cycle crossover operator [4, 5]. Julius BeneoluchiOdili solved the traveling salesman's problem using the African buffalo optimization (ABO) using reform operators. At the latest, Kerschke, Pascal gave an automated algorithm selection for TSP. Kotthoff, Lars and Bossek in 2018 provided a leveraging TSP Solver through machine learning. Marie-Eléonore proposed a learning and intelligent optimization (LION) for TSP on latest algorithms. In 2019, Aneta and Wagner evolved diverse TSP instances by means of novel creative mutation operators. The latest discoveries are shown in Table 1.

3 Plate Tectonics Based Optimization–Intuition and Discussion

PBO falls under the category of nature inspired algorithms and is inspired by the theory of tectonic plate. PBO neighborhood search has the potential to outperform many algorithms because of the balanced amalgamation of both exploration as well as exploitation. Gradient based algorithm uses the information available in the gradient of the function but lacks exploration. In evolutionary algorithms, candidate solutions

Table 1 Latest discovery or research in the field of TSP

Year	Author	Description
2016	Pascal	Gives an automated algorithm selection for TSP
2015	Sarit Wagner	Analyzed the standard TSP problem and proposed ant colony-based approaches
2016	Julius Beneoluchi Odili	Solved the traveling salesman problem using the African buffalo optimization (ABO) using reform operators
2017	Showkat Gani	Genetic algorithm for TSP with modified cycle crossover operator
2017	Marie-Eléonore	Proposed a learning and intelligent optimization (LION) for TSP on latest algorithms

evolve toward global optimum with every iteration but gradient based information is not utilized. PBO uses both the concept of exploration as well as exploitation. It explores the search space as well as utilizes the information about the function.

The theory of plate tectonics suggests to see all formations in lithosphere as relativistic movements of tectonic plates. However, movements must occur only to increase the stability of the plate's arrangement, and thus, the idea of an optimization algorithm based on this phenomenon. The continuous movements of tectonic plates to achieve minimum energy, especially in certain localized formations, inspire an optimization algorithm that does so along the same lines [6, 7]. We now present some definitions from plate tectonics as a first step toward formalizing PBO to find global minimum of arbitrary d-dimensional functions.

Candidate Solutions. The candidate solutions represent feasible solutions to the problem and are analogous to the coordinates on a d-dimensional plate.

Global Optimum. To each of the 'n' coordinates, we associate a temperature T. Mathematically, we associate this temperature to the value of the objective function at ci. Therefore, the problem optimization problem is akin to finding the coordinates on the plate where temperature is the lowest.

Weights. Each decision variable in each of the candidate solutions is assigned a separate weight. Each can be seen as the component to displacement in the direction resulting from accumulative effect of plate tectonic forces acting on point. These weights are adjusted to allow for exploration to find a local minimum.

Equilibrium State. A point on the plate will be in equilibrium if the net force acting on it is zero. By extension, one can see that the net displacement, and hence, each of its components would reduce to 0. An equilibrium point can also be identified by finding the coordinates where the potential energy of the system is the minimum.

Plate Mobility Index (PMI). PMI is analogous to the system's potential energy at a coordinate. Borrowing from descent optimization algorithms, we abstract the potential energy at a point using the gradient of the objective function.

Hybrid Initialization using BBO: In the proposed PBO, we used BBO for initialization of candidate solutions. PBO can yield results much faster if the initial population is seeded in promising regions where the probability of finding the optimal solution

is more. To obtain seeded candidate solutions for PBO, we allow BBO to divide an initially random population into habitats.

Roulette Wheel based Relocation of Candidate Solution: PBO identifies candidate solutions that are stuck by checking if they moved in the previous iteration. Once a solution is identified as being stuck, PBO relocates them by defining two sets, one for probable solutions (PS) and one for candidates for relocation (CR). Both PS and CR are initialized as empty sets during PBO's initialization. PS is used to store the current best candidate solution in PBO in case it stops moving and needs to be re-initialized. This allows PBO to keep track of the best solutions in case relocation yields worse results. The set CR is for candidates for relocation and contains points that need to be relocated.

Effect of stability on neighborhood: Since the number of local probes performed by each candidate point remain constant, more stable candidate solutions aggressively search their smaller neighborhoods to find a local minimum while the less stable solutions sample over a larger hyper-ellipse to find more optimal solutions that will make them more stable, effectively allowing for exploration over the search space. To ensure this, PBO restricts the weight probing procedure to only sample from the outer half of the hyper-elliptical neighborhood by volume.

Randomized Neighborhood Search: For each point, PBO performs a randomized local search to find a better candidate solution than the point in question. Since the axes of the hyper-elliptical neighborhood centered around each point are determined by the limit, instead of adding the computational overhead of modeling the drag pull and the ridge push forces on the plate in d-dimensions, we search each neighborhood for the most optimal solution by randomly sampling points within them. Thus, PBO selects p samples from all possible values constrained within the hyper-elliptical neighborhood.

4 Proposed Methodology for Solving TSP Using PBO Search

In this section, the definitions of all the terms and concepts used in the approach to solve TSP are explained which will be needed after this section to understand all the steps in the solution.

Initialization of variables: The initial population is selected using selective techniques using heuristics operation. The fitness, PMI index, stability are calculated for each tour to find how each tour is well suited for the problem and whether it is optimum tour or not. We will use evaluation function such as evaluate chances and evaluate fitness to find how good the tour is. The fitness and other variable will then be used to decide which tour should be considered to pass to the next iteration without any change. The function to evaluate is inspired from the given problem.

The cost is used to compare among graphs and to find the optimized one which can be passed to next generation using other techniques which are explained below.

Roulette wheel Selection for selecting tours: In this technique, an individual is selected depending upon the probability of a fitness value. The size of the individual slice of the roulette wheel will have fitness value which will be inversely proportional to their indices as 0 is considered as best fitness in this technique. Once the slices have been determined each slice will be assigned a number at random. Randomly, a number will be generated and the selected slice will be chosen. The pseudocode is discussed below in Fig. 1.

Tournament Selection for selecting tours: In the selection technique, individuals are selected at random and are paired with each other. The fitness value of each pair is calculated. The winner of them is passed to next generation while the loser is sent back to initial collection. This continues until the number of winners demanded is satisfied which is equal to the number of tours demanded. The pseudocode is discussed below in Fig. 2.

```
void roulette_wheel (num of tours, Population)
high = 0
`       for tour in Population:
        if (fitness of tour is greater than high)
               high is assigned fitness of tour;
        create vector equal to size of Population;
for (0 <= i< size of population)
        for (0 <= j < high)
        update fitness of element i
add i to vector of integers;
tours.add (element at i) ;
```

Fig. 1 Pseudocode for roulette wheel

```
void tournament_tours (num of tours, Population)
create an empty set for population;
add 0 to last member of Population;
create vectors equal to size of Population;
if (size of Population. <= num of tours)
       tours = Population;
else
       for (0 <= i< /2)
              Compare   element   at   I   of   population   and
              Size_of_Population - i
              The one which wins i.e. with max fitness is added
              to temporary set.
tournament_tours (num_of_tours, temporary population)
```

Fig. 2 Pseudocode for roulette wheel

Crossover: The fitness or the cost of each tour is used to find the individual's probability of crossover. The crossover technique has a constraint that cities should not be repeated during creating child tours from parent tours. In our approach, we select some cities from parent and copy them as same in child, while producing permutation for remaining cities and then follow some convention in creating new tours.

Mutation: The mutation will modify the tours and swap some cities from one portion to another to generate new tours so that the search algorithm does not get stuck on local minima.

4.1 Steps of Algorithm

In this section, all the steps of algorithm are explained in detail. Figure 3 presents the algorithm for solving TSP problem using PBO search technique.

Step 1. Initialization: Given the number of cities and their coordinates in the form of $(x_1, x_2, \ldots x_d)$ for each city. These features can be anything related to each city such as x-coordinate, y-coordinate, population of each city, transport at each city, weather, traffic, culture, food-habits and various other properties which can affect the function which calculates closeness of adjacent cities. Here, adjacent cities are those which are connected by an edge. Calculate the closeness of each city with other cities based on weights of different features (dimensions) and save it to the relation matrix. Initialize the number of random salesman in the search space, i.e., select some cities randomly and place a salesman there showing the start city using BBO techniques used in PBO for initialization and append memory with each salesman to remember the best tour and cost till now, the iteration times (Maximum Iterations) and a global tour remembering best tour found till now by checking the cost of all tours of the salesmen at different cities. In this objective function, elite function, migration, bound check, and replace habitat functions are being used.

Step 2. Calculate the distance of each salesman tour based on the above relation matrix and the tour associated with them.

Step 3. Start iteration: For each salesman define a boundary (range) based on the weights of each candidate solution so that they each have a defined neighborhood within which to search for a local optimum in each iteration, where it can find the best next city for its tour and once he found the best next city it will be appended to current tour and salesman will jump to this location now and will found the next best city from the current node which is not visited till now. Once all the cities are done, this process will stop. Evaluate fitness for each tour of the population. Evaluate chances for each tour to get passed on the next iteration. Calculate PMI index for each and initialize random weights which will be used to generate next iteration. Select two tours from a population according to their fitness or cost and better the fitness, the bigger chance to be selected using roulette wheel selection. Crossover is performed on the selected tours to produce a new tour. Mutation is performed on some selected tours and mutation percentage is passed. Place all produced tours

```
def main
       import data
       get distance between cities
       Initialize the population and divide it into regions
       PBO_init
              Calculate the immigration, emigration, evolution
              and extinction rates based on their suitability
              Objective function is initialized.
                     for i in range (PopSize):
                            calculate objective fn value
              Define the elite function and initialize the
              collection of tours
                     for j in range (PopSize):
                            define_EliteSolution
                            define_EliteCost
              Perform migrate function to initialized tours
              Perform bound check on variables so that the
              selected cities are in search space
                     for i in range (PopSize):
                            Check bound for defined variable
              Replace habitat function for removing wrong tours
              Remove duplicate function which removes duplicate
              tours
Initialize random weights
Find all routes between cities and initialize salesman at each
city and initialize tours
for individual in population
       Find fitness of each tour
Evaluate chances of each tour to get selected in roulette wheel
       For var in pop:
              chance = fitness / summed_fitness // Evaluate
              chance matrix
Find PMI Index //Absolute value of gradient is calculated
for iteration in range (Number of iterations):
       for i in range (Population Size):
              Select individuals using roulette wheel selection
              while rand > 0:
                     Select random tours to be modified next
              Perform crossover technique to generate new tours
              Append new tours to the collection of the tours
              generated
              Perform mutation
              Mutate on tours to calculate few more tours
              Append these tours to the collection
       for individual in population
              Find fitness of each tour
       Evaluate each tour's chances of selection in roulette
       wheel
       best = find best tour till now
       update all variable before iterating again
```

Fig. 3 Pseudocode for complete algorithm

in a new generation. Use the new generated population for further iterations. Each salesman's tour will be independent of other salesmen's tours in most cases.

Step 4. Update best tour and cost for each salesman if found. Find the cost of the present tour for each salesman, i.e., evaluate fitness for each tour in the population and check if the fitness of the present best tour is less than the global tour. If it is less, update the best global tour and cost of it for each salesman.

Step 5. After updating the best route for all salesman, find best tours out of them and update the global tour variable.

Step 6. Judge the termination criterion. If the current iteration > maximum number of iterations, or if it has crossed the optimum solution which was already given then go to step 7 else repeat the process from step 3.

Step 7. Output the global best tour and cost.

5 Results

We accomplish various results based on different datasets using python version 3.7 on windows10 core i7 8th generation with 16 GB ram. We calculate optimal cost for every tour applying number of iterations 50,100, 500,1000,2000,5000. The important parameters for this problem are population size, mutation percentage, number of iterations whose values are 120, 0.35, 2000, respectively, for the example of rat99.tsp. We have used the available datasets which are standard for TSP and tried several of them for a range of cities using our proposed solution (results shown in Table 2).

From the results, it can be seen that PBO performs well on almost all the TSP instances, and its cost is comparable with the optimum cost value. As the number of city increases to a very high value, the value of PBO cost becomes more than optimum cost.

Table 2 Results with optimum cost and PBO cost

Data	Cities	Optimum	TSP using PBO
Ulysses16	16	6859	6862.4
Ulysees22	22	7013	7014.4
Swiss42	42	1273	1276.5
St70	70	675	671.9
Rd100	100	7910	7914.5
Rat99	99	1211	1204.6
Pr76	76	1081	1085.8
Lin105	105	14,379	14,385.3
Hk48	48	11,461	11,452.1
Gr24	24	1272	1274.4
Eil101	101	629	631.1
Eil125	125	3261	3271.1

Table 3 Comparative experimental results

Problem	Optimal	ACO	PSO	PBO
Att48	33,522	33,541.1	33,534.2	33,537.1
St70	675	675.7	681.2	678.4
Eil76	538	550.7	532.3	535.1
Eil 101	629	678.04	640.1	635.1
Ch150	6528	6648.51	6641.2	6710.4

The above Table 3 shows the comparable results of various other algorithms compared to optimization technique proposed in this paper, i.e., plate tectonics based optimization. From the results, it is proven that the solution by PBO technique is very much comparable to ACO and PSO. For various cases, it is far way better than both algorithms. As soon as number of city increases, the cost by PBO is near equal to PSO and is better than ACO.

6 Conclusion and Future Work

The proposed algorithm can exploit the local information available from the gradients of the function, while also allowing for exploration to scout for better solutions throughout the search space. This allows the algorithm to improve the known solution in each iteration and locate the global minimum efficiently. PBO search technique for the traveling salesman problem (TSP) which depend on the way the initialization part is handled. We have used biogeography based optimization (BBO) for it. It depends upon the encoding function, selection technique, crossover technique and mutation methods. From the results, it is observed that the solution by PBO technique is very much comparable to ACO and PSO. For various cases, it is far way better than both algorithms. For different number of iterations and different size of population, the cost varies with increasing number of cities. Thus, we see that as the number of cities increase, the cost by PBO is near equal to PSO and is better than ACO and therefore PBO needs further optimization in the search strategy to handle large number of cities.

We suggest to increase the dimension of the problem to more than 2 which will act as features for each city and will affect the closeness function. We also suggest a modified algorithm which can work on a dynamic traveling salesman problem. Here, the number of cities will change in number as well as they can change their locations as well.

References

1. D.B. Fogel, An evolutionary approach to the traveling salesman problem. Biol. Cybern. **60**, 139–144 (1988)
2. M. Dorigo, M. Birattari, *Ant Colony Optimization* (Springer, 2010)
3. R. Eberhart, J. Kennedy, A new optimizer using particle swarm theory. in *Proceedings of the Sixth International Symposium on Micro Machine and Human Science*. MHS'95, (IEEE, 1995), pp. 39–43
4. J.H. Holland, Genetic algorithms. Sci. Am. **267**(1), 66–73 (1992)
5. N. Kumar, Karambir, R. Kumar, A genetic algorithm approach to study travelling salesman problem. J. Global Res. Comput. Sci. **12**(3) (2012)
6. J.C. Briggs, in *Biogeography and Plate Tectonics*. vol. 10 (Elsevier, 1987)
7. D. Bercovici, Y. Ricard, M.A. Richards, The relation between mantle dynamics and plate tectonics: A primer. Geophysical Monograph, American Geophysical Union **121**, 5–46 (2000)

An Optimistic Approach for Managing the Handover Latency by Using Dynamic Data in Software Defined Networks (SDN)



Krishna Shah and Kishor Kolhe

Abstract The access point (AP) assignment of IEEE 802.11 standards is a universal network challenge. It can be smartphones, Wi-Fi, etc., in terms of network equipment. Two methods may be carried out depending on the flow-type or the frequency of the RSSI signal for the globally assigned Software defined network (SDN) AP. The flow style AP assignment is performed in this article. As a researcher studying various algorithms that are helpful to SDN AP assignments and also various feature types that are useful to make current work more accurate. This paper discusses the mobile connectivity AP assignment algorithm using SDN architecture.

Keywords SDN · Mobile communication networks · Optimization · Latency · Handover · QoS parameter · Fitness Function

1 Introduction

The idea of programming is the basis for the most accurate definition of what is SDN: technology that distinguishes network appliance control plane management from the underlying data plane, which promotes network traffic. If a particular controller carries too much load, then an inefficient performance problem of the controller will occur. Due to this problem, the network is inefficient in providing services [1]. The control and data planes are decoupled in the SDN architecture, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications [2].

Key issue is what we can understand by the term 'Optimize.' If multiple communication paths are available, which path is best for best results, or which result is optimal for the best result. A literature has addressed extensively the problem of finding an optimal connection of terminals to wireless apps [3–6]. Most approaches, as stated

K. Shah (✉) · K. Kolhe
School of Computer Science and Technology, Dr. Vishwanath Karad MIT World Peace University, Pune, India

K. Kolhe
e-mail: kishor.kolhe@mitwpu.edu.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_59

here [7], try to allocate the best AP for every terminal in one performance metric, like RSSI, bandwidth efficiency or replacement throughput. However, because traffic monitoring information from the terminals may be unavailable for reasons of privacy, network decision algorithms must rely on user traffic class estimates at access points.

The handover is vertical and horizontal with two different forms. When a system transfers within a certain kind of network infrastructure to one operator, a horizontal transfer happens. For example, by going in and out of a range of towers, a smartphone user moves through the network of their provider. When a system has to swap technologies or technicians, vertical handover happens. For example, an application changing wireless coverage from IEEE 802.11 to 4G shows a technology transition. A provider roaming on the 4G network, e.g., between Rogers and Telus shows vertical handover across operators under a single technology. Author demonstrated with existing tendency in vertical handover mostly with the authentication, latency and packet loss issues [8]. Network selection and handoff timing issues can be resolved with novel vertical handoff scheme specially for heterogeneous wireless networks [9].

The rest of this paper systematized as follows: Sect. 2 discusses a literature survey of recent developments which are based on SDN which reduce handover. Section 3 describes the dataset used in this study. Section 4 gives information about what kind of experiments are done on topology and also in mobile communication networks. Section 5 explains about experimental setup and the performance of all the operations which we have performed.

2 Literature Survey

When it comes to IEEE 802.11 networks, it is often thought that resources are scarce, and as a result, many customers are expecting next-generation systems such as 5G networks or ultra-dense networks (UDN) [10]. Another intriguing part of our research [11] is that we use real-world evidence to test our methodology. The first example was created using data gathered in a massive Wi-Fi campus network of actual users from the publicly accessible LiveLab data collection. However, we suggest a second speculative 5G ultra-dense network scenario based on this dataset. Wireless networks that are ultra-dense in the traditional sense are they are used as a supplement to cellular networks and are deployed in limited areas, such as airports as well as indoor and hotspot scenarios [12]. In both cases, we demonstrate the presence of a fast centralized prediction algorithm. In an IEEE 802.11 access network, wireless stations (WSs) compete for the aggregate bandwidth provided by access points (APs) [13].

Increasing demand for traffic around the world is being met, with the rapid proliferation of mobile devices, tablets and other handheld devices. This dramatic increase in demand for cellular networks has driven the development of small, pico and nano BSs from the use of macro base stations (BSs) [14]. The 5G evolution for mobile networks, for example, dictates that one thousand fold capacity will improve, and that

will be achieved in an evolutionary and heterogeneous phase of network densification [15].

One of the most crucial aspects of wireless communications is the mobility performance [16]. Mobility is also key requirement together with latency and reliability [17]. In the same geographical region, deploying more BSs reduces each BS' footprint, increasing spectral efficiency and increasing capacity. The expected network densification capacities gains are, however, at the cost of higher transfer (HO) rates. Usually, such a significant adverse effect of BS densification (i.e., HO ratio) is ignored [18]. The HO procedure interrupts the data flow to the user in addition to the overhead signaling system because of a connection with the BS service and the connection to the BS goal. Higher HO rates increase the frequency of such unwanted interruptions and the associated overhead signal which may decrease or can even nullify the predicted capacity gain for network densification. As smart phones, laptops and other handheld devices are rapidly proliferating, the World's traffic demand is growing.

This dramatically increased demand for cellular networks has led to the evolution of the deployment of mini, pico or even nano BSs from macro base stations (BSs). For example, the 5G developments for mobile networks determine 1000 times that the evolutions of the heterogeneous networks density are required to achieve. The implementation of further BSs within the same geographical area reduces each BS' footprint, increasing spatial spectral efficiency and providing greater capacity.

In an area served by multiple access points, a STA (station) usually chooses to connect to one of the APs based on a set of selection criteria. In standard IEEE 802.11 protocols, the obtained signal intensity indicator (RSSI) is the only parameter used in AP collection [11]. This enables the STA to connect to the AP with the highest signal strength after scanning the channel, regardless of the AP's load.The variable channel-width technology has recently been proposed to improve the fairness and capacity of WLAN [19].

SDN is at the heart of 5G transport network design, allowing for automatic network reconfiguration and network slicing. In this paper, they show OpenFlow approach to implement control plane area. They analyse network slicing at the network edge. Here, they tried to achieve how to recover from single-link failures without delays and packet drops. All this kind of architecture is named as the 5G XHaul project. Main purpose of this paper is, what kind of challenges facing while designing a 5G XHaul architecture and they tried to solve it. Here, they mentioned virtual data plane concept and that dataplane contains three types of nodes. ETN (edge transport node), IATN (inter area transport node), T N (transport node).

Big MIMO antennas are built into BSs in cellular 5G networks where hundreds of antennas are used for wireless transmission [20]. When 5G BS is restricted to the same amount of 4G BS transmission capacity, the transmission power of each antenna at 5G BS must be 10–20 times lower than at 4G BS for each antenna. Consequently, in view of the reduction of transmitting power at each antenna, the 5G BS radius should be reduced by one magnito.

3 Datasets

The LiveLabdataset includes real data from 24 iPhone 3GS mobile terminals that were tracked on Rice's Wi-Ficampus network [21]. The programs running in the terminals, accelerometer readings, and the collection of active Wi-Fi APs to each terminal at various times are all included in the data set. When the data set was released, the campus network had 834 APs serving an area of 700,500 m2.

4 Proposed System

In this paper, we propose an architecture for handling handover scenarios in mobile communication and Wi-Fi networks using software defined networks (SDN) (Fig. 1).

The above figure shows model architecture with various layers of SDN framework. The architecture is divided into three main parts. The first one is data plane then second is control plane, and third one is application plane. A packet arrives at a network switch in a traditional SDN case, and rules built into the switch's proprietary

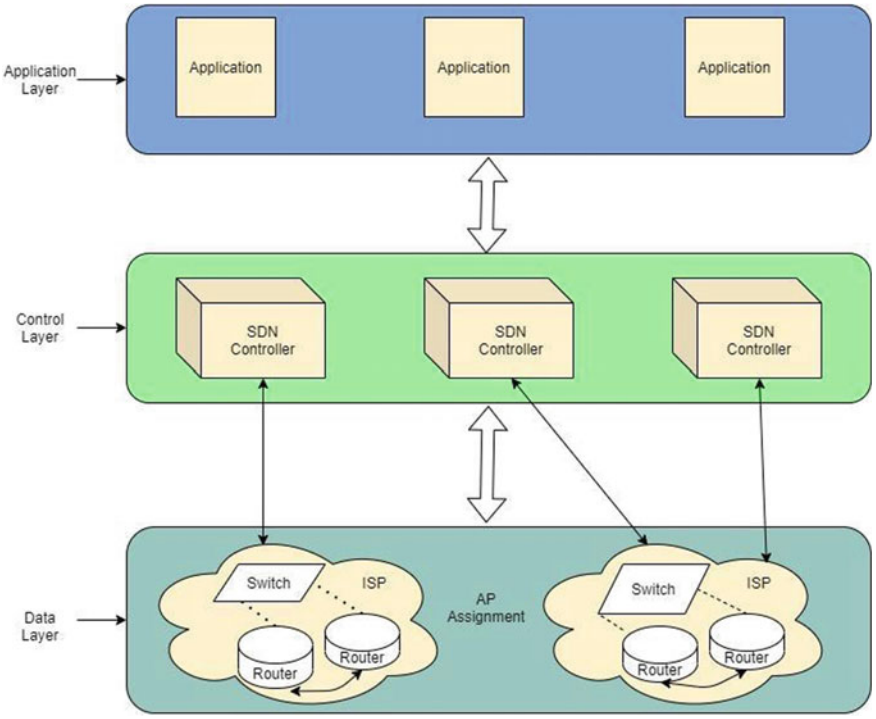


Fig.1 Proposed model architecture

firmware instruct it where to forward it. The unified controller sends these packet-handling rules to the switch. The turn, also known as a data plane computer, requests input from the controller as required and provides information about the traffic it handles to the controller. Each packet going to the same destination is sent down the same route by the switch, and all packets are treated the same way.

HO is the method of modifying the association of versatility between user gear (UE) and mobility in order to choose the best serving BS. The obtained signal intensity (RSS) level is a popular and easy rule for deciding the best serving BS. That is, if another BS offers a higher RSS than the BSA, the UE switches its association and the customer moves from the BS to another. Increased cellular network heterogeneity creates many other conditions for the selection of the right service BS that may include load balance, latency and performance measurements. In terms of mobile devices communication or between mobile network communication these terms as BS, BSS all are required to understand first (Fig. 2).

The SDN controller is implemented as a network feature. The controller will connect an AP to the terminal using the NorthBound API (Network API), which receives traffic flow information provided by the terminals. As a result, current SDN-enabled switches and routers flow tracking is beneficial to us. The SDN controller manages the routing tables of these different network elements. This feature can be used to associate a certain AP with a terminal and to maintain terminal session compatibility even though routes are changed (due to changes in service of APs or other path changes).

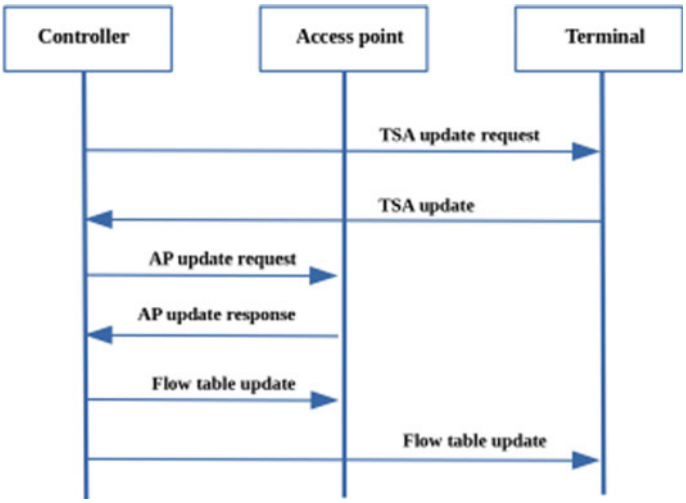


Fig. 2 Periodic TSA signaling

5 Experiments

We built a network based upon proposed architecture in a mininet simulator using Ryu controller. All experiments related to handover done on mininet with controller. For multipath topology designing, we used the Miniedit tool and for showing output virtually we used Mininet-Wi-Fi Graph with json file. Whole scripting done in Python Language.

For handling handover, we tried to get every AP data so that we can understand their SSID, bandwidth and latency too. As we wanted to get updates dynamically so we imported Mininet-Wi-Fi based on that traffic getting changed periodically. By this operation, we came to know about how much the packet gets delayed, and how many packets are totally sent throughout the communication channel.

For the solution of the shortest path among all paths, we gave weight to each and every link. At the end of code, we used fitness function rule so that we get optimal output of that.

- Creating a network based on various requirements.
- Ping all nodes in a network..
- Add as many as no. of nodes in a topology for getting a deep idea on that.
- Try to implement a 5G network scenario for handover.
- For handover assigning APs and servers to the network and creating a live virtual environment with Mininet-Wi-Fi.

6 Results

We created a network by using a mininet simulator which is going to help us for measuring QoS parameters of a network like latency, bandwidth, frequency also based upon our requirements it helps us to calculate the shortest path among all paths in multipath topology (Figs. 3, 4, 5, 6, 7, and 8).

With the help of Mininet simulator we created a network for experimental purposes.

As above showed the results after creating the network using mininet we got round trip time and calculated path from each and every node and at the end we calculated the shortest path among all paths in multipath topology. For the optimal solution of the shortest path, we used a fitness function in script (Figs. 9 and 10).

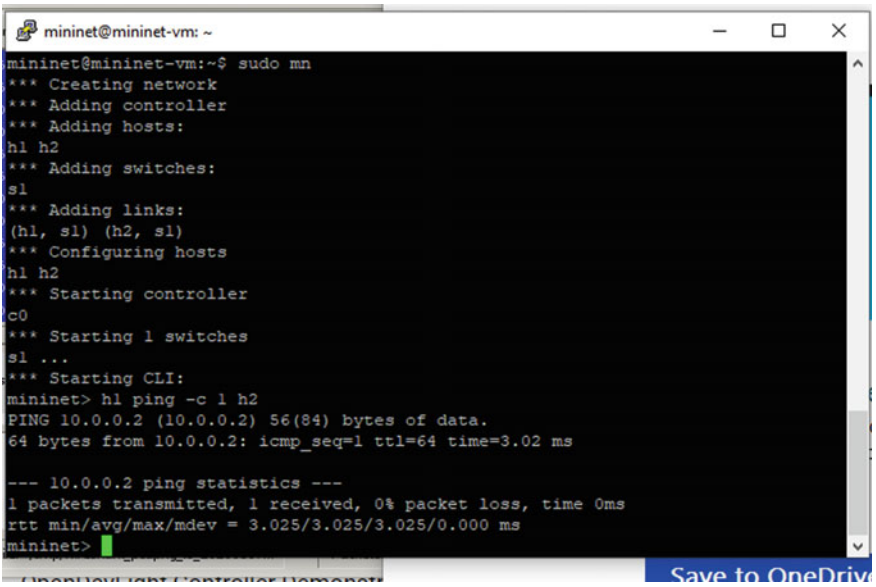


Fig. 3 Creating network using mininet

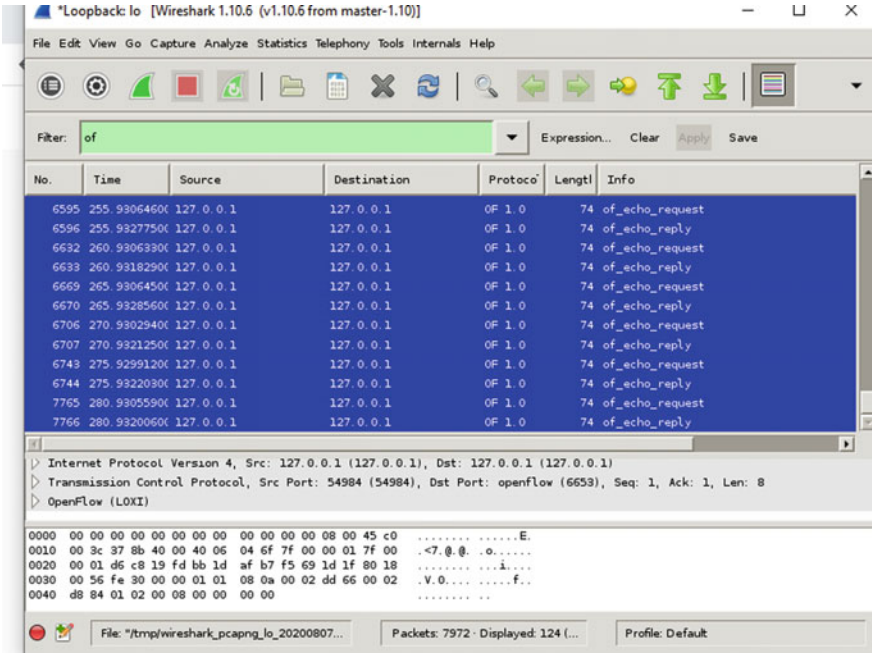


Fig.4 RTT observation during packet forwarding using wireshark

```
*** Starting CLI:
mininet> h1 ping -c 1 h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=3.02 ms

--- 10.0.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.025/3.025/3.025/0.000 ms
mininet>
```

Fig.5 Ping operation

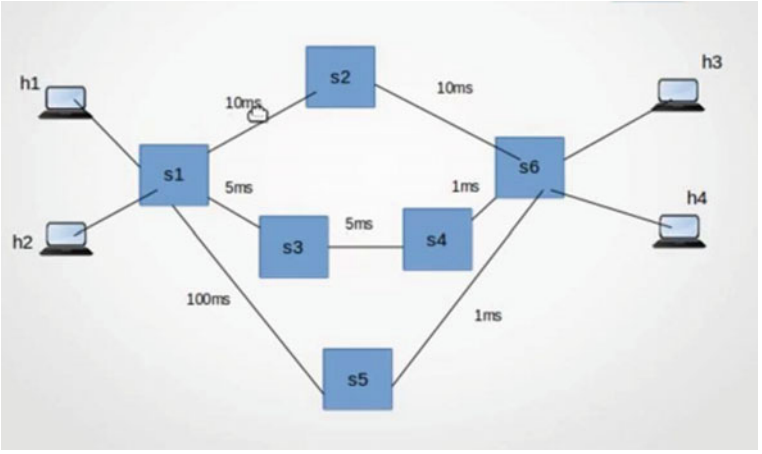


Fig.6 Multipath topology

```
rt': 2, 'weight': 1}), (6, 5, {'port': 3, 'weight': 1}), (3, 1, {'port': 1, 'weight': 1}), (4, 3, {'port': 1
, 'weight': 1}), (1, 3, {'port': 2, 'weight': 1}), (6, 4, {'port': 2, 'weight': 1}), (1, 2, {'port': 1, 'wei
ght': 1}), (5, 1, {'port': 1, 'weight': 1}), (2, 1, {'port': 1, 'weight': 1})]  Hosts [('00:00:00:00:00:03',
 6, {'port': 4}), ('00:00:00:00:00:02', 1, {'port': 5}), ('00:00:00:00:00:01', 1, {'port': 4}), ('00:00:00:0
0:00:04', 6, {'port': 5})]
Monitoring Link Latency....
Monitoring Link Latency....
Shortest path calcaulation 00:00:00:00:00:01 to 00:00:00:00:00:03
all paths [[1, 2, 6], [1, 3, 4, 6], [1, 5, 6]]
path  [1, 2, 6] , total_latency 22.9433774948
path  [1, 3, 4, 6] , total_latency 16.0254240036
path  [1, 5, 6] , total_latency 103.785037994
 Selected Path is [1, 3, 4, 6]
Shortest path calcaulation 00:00:00:00:00:03 to 00:00:00:00:00:01
all paths [[6, 2, 1], [6, 4, 3, 1], [6, 5, 1]]
path  [6, 2, 1] , total_latency 23.5104560852
path  [6, 4, 3, 1] , total_latency 16.118645668
path  [6, 5, 1] , total_latency 104.832530022
 Selected Path is [6, 4, 3, 1]
```

Fig.7 Calculating latency for all links

```
Shortest path calcaulation 00:00:00:00:00:01 to 00:00:00:00:00:03
all paths [[1, 2, 6], [1, 3, 4, 6], [1, 5, 6]]
path  [1, 2, 6] , total_latency 22.9433774948
path  [1, 3, 4, 6] , total_latency 16.0254240036
path  [1, 5, 6] , total_latency 103.785037994
 Selected Path is [1, 3, 4, 6]
Shortest path calcaulation 00:00:00:00:00:03 to 00:00:00:00:00:01
all paths [[6, 2, 1], [6, 4, 3, 1], [6, 5, 1]]
path  [6, 2, 1] , total_latency 23.5104560852
path  [6, 4, 3, 1] , total_latency 16.118645668
path  [6, 5, 1] , total_latency 104.832530022
 Selected Path is [6, 4, 3, 1]
```

Fig. 8 Shortest path calculation

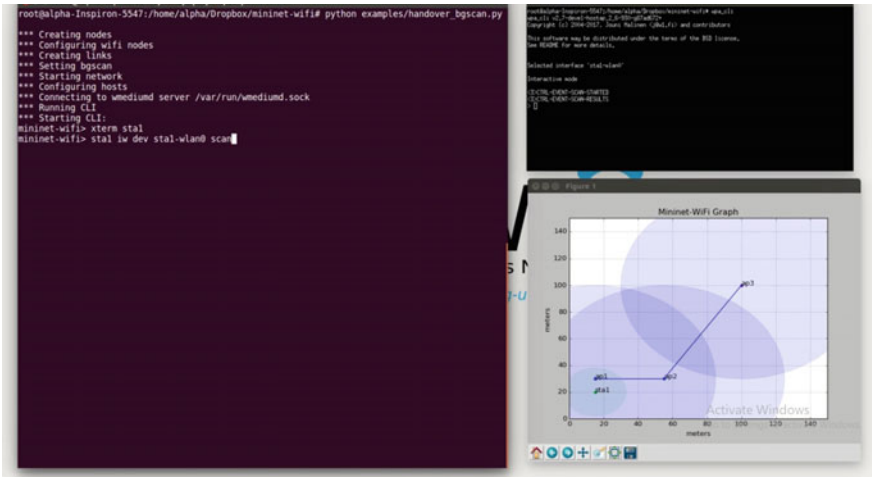


Fig. 9 Creation of another network for handover

7 Conclusion

Next-generation ultra-dense wireless networks would have enough bandwidth capacity for existing implementations, but would necessitate more regular data transfers to user computers. For these modern situations, low-handover latency is a critical condition for success. In 5G networks, for example, transfers require the gNBs involved in exchanging control messages and user data transfers may be blocked, thus optimizing transfers through the decrease in signal load and time (as these could even result in interruptions in the data stream and reduced mobile user performance). As a result, in this article, we recommend a new AP solution that makes fast decisions based solely on previous usage experience. We looked at the traditional AP system and addressed the issues with the RSSI-based AP system in this article. With the above drawbacks, our TPR could make the APs picked more sensible and effective by the new AP selection mechanism, called TPR, in the SDN-enabled WLAN to

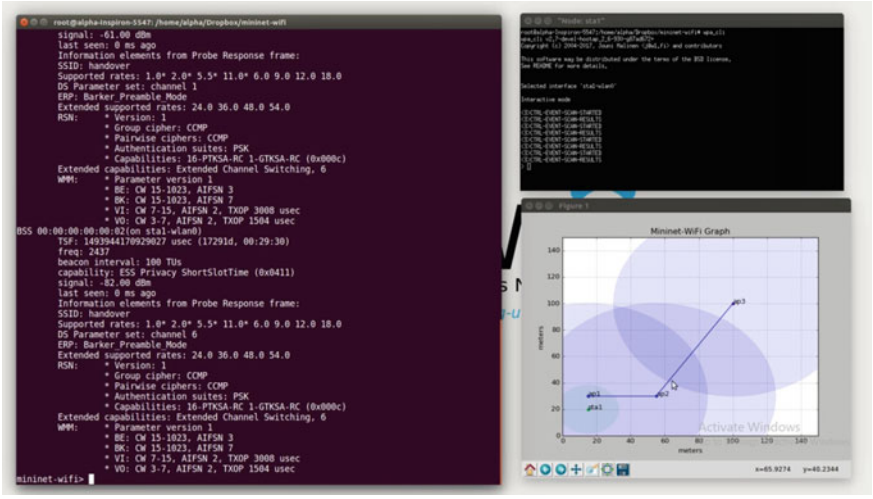


Fig. 10 Output of handover

reduce AP costs by adding a centralized control from the SDN controller. Furthermore, by using the OpenFlow protocol on AP computers, the metric used for handoff determination could be obtained effectively.

References

1. P. Dely, A. Kassler, N. Bayer, OpenFlow for wireless mesh networks. in *2011 Proceedings of 20th International Conference on Computer Communications and Networks* (ICCCN), Lahaina, HI, USA (2011), pp. 1–6. https://doi.org/10.1109/ICCCN.2011.6006100
2. S. Sezer et al., Are we ready for SDN? implementation challenges for software-defined networks. IEEE Commun. Magazine **51**(7), 36–43 (2013). https://doi.org/10.1109/MCOM.20136553676
3. L. Yen, J. Li, C. Lin, Stability and fairness of AP selection games in IEEE 802.11 access networks. IEEE Trans. Veh. Technol. **60**(3), 1150–1160 (2011). https://doi.org/10.1109/TVT.2010.2104167
4. X. Chen, W. Yuan, W. Cheng, W. Liu, H. Leung, Access point selection under QoS requirements in variable channel-width WLANs. IEEE Wireless Commun. Lett. **2**(1), 114–117 (2013). https://doi.org/10.1109/WCL.2012.120312.120741
5. J.B. Ernst, S. Kremer, J.J.P.C. Rodrigues, A utility based access point selection method for IEEE 802.11 wireless networks with enhanced quality of experience. in *2014 IEEE International Conference on Communications* (ICC), Sydney, NSW, Australia, (2014), pp. 2363–2368. https://doi.org/10.1109/ICC.2014.6883676
6. A. Antonopoulos, J. Alonso-Zarate, E. Kartsakli, L. Alonso, C.´Verikouki, Cross layer access point selection mechanisms for a distributed queuing MAC protocol. Telecommun. Syst. **53**(3), 329–342 (2013)
7. A. Raschellà, F. Bouhafs, M. Seyedebrahimi, M. Mackay, Q. Shi, Quality of service oriented access point selection framework for large wi-fi networks. IEEE Trans. Netw. Serv. Manage. **14**(2), 441–455 (2017). https://doi.org/10.1109/TNSM.2017.2678021

8. http://dx.doi.org/https://doi.org/10.14569/IJACSA.2012.030114
9. Q. Li. L. Jie. J. Yusheng, H. Changcheng, A novel software-defined networking approach for vertical handoff in heterogeneous wireless networks: a demonstration of the wireless communications and mobile computing class file. Wireless Commun. Mobile Comput. **16** (2016). https://doi.org/10.1002/wcm.2690
10. C. Shepard, A. Rahmati, C. Tossell, L. Zhong, P. Kortum, LiveLab: measuring wireless networks and smartphone users in the field. SIGMETRICS Perform. Eval. Rev. **38**(3), 15–20 (2011). https://doi.org/10.1145/1925019.1925023
11. P. Fondo-Ferreiro, S. Mhiri, C. López-Bravo, F.J. González-Castaño, F. Gil-Castiñeira, Fast decision algorithms for efficient access point assignment in SDN-controlled wireless access networks. IEEE Trans. Netw. Serv. Manage. **16**(3), 1059–1070 (2019). https://doi.org/10.1109/TNSM.2019.2925506
12. J.G. Andrews et al., What will 5G Be? IEEE J. Sel. Areas Commun. **32**(6), 1065–1082 (2014). https://doi.org/10.1109/JSAC.2014.2328098
13. S. Jamali, A. Badirzadeh, M.S. Siapoush, On the use of the genetic programming for balanced load distribution in software-defined networks. Digital Commun. Netw. **5**(4), 288–296 (2019). ISSN 2352–8648 https://doi.org/10.1016/j.dcan.2019.10.002
14. R. Arshad, H. Elsawy, S. Sorour, T.Y. Al-Naffouri, M. Alouini, Handover management in 5G and beyond: a topology aware skipping approach. IEEE Access **4**, 9073–9081 (2016).https://doi.org/10.1109/ACCESS.2016.2642538
15. https://onlinelibrary.wiley.com/doi/abs/https://doi.org/10.1002/dac.4510
16. T. Bilen, B. Canberk, K.R. Chowdhury, Handover management in software-defined ultra-dense 5G networks. IEEE Netw. **31**(4), 49–55 (2017). https://doi.org/10.1109/MNET.2017.1600301
17. H. Park, Y. Lee, T. Kim, B. Kim, J. Lee, Handover mechanism in NR for ultra-reliable low-latency communications. IEEE Netw. **32**(2), 41–47 (2018). https://doi.org/10.1109/MNET.2018.1700235
18. M. Faisal, M.N. Khan, An enhanced scheme for reducing vertical handover latency. Int. J. Adv. Comput. Sci. Appl. (IJACSA) **3**(1), (2012)
19. J. Galán-Jiménez, Minimization of energy consumption in IP/SDN hybrid networks using genetic algorithms. in *2017 Sustainable Internet and ICT for Sustainability* (SustainIT), Funchal, (2017), pp. 1–5.https://doi.org/10.23919/SustainIT.2017.8379802
20. X. Ge, S. Tu, G. Mao, C. Wang, T. Han, 5G Ultra-dense cellular networks. IEEE Wirel. Commun. **23**(1), 72–79 (2016). https://doi.org/10.1109/MWC.2016.7422408
21. C. Shepard, A. Rahmati, C. Tossell, L. Zhong, P. Kortum, LiveLab: measuring wireless networks and smartphone users in the field. SIGMETRICS Perform. Eval. Rev. **38**, 15–20 (2010). https://doi.org/10.1145/1925019.1925023
22. J. Orlosky, K. Kiyokawa, H. Takemura, Virtual and augmented reality on the 5G highway. J. Inform. Process. **25**, 133–141 (2017)
23. C. Giraldo-Rodríguez, J. Fontenla-González, C. Pérez-Garrido, S. Mhiri, F. Gil-Castiñeira, F.J. González-Castaño, TSA, an SDN architecture including end terminals. in *2016 13th IEEE Annual Consumer Communications and Networking Conference* (CCNC), Las Vegas, NV, USA, (2016), pp. 250–251.https://doi.org/10.1109/CCNC.2016.7444765
24. N. Bhomia, K. Kolhe, Anti-theft hybrid solution for tracking & locating mobile devices with data security. Int. J. Recent Technol. Eng. (IJRTE) **8**(2S3), 696–699 (2019). ISSN: 2277–3878. 10.35940/ijrte.B1129.0782S319, Jul 2019, URL:https://www.ijrte.org/wp-content/uploads/papers/v8i2S3/B11290782S319.pdf

The 3D Facemask Recognition: Minimization for Spreading COVID-19 and Enhance Security

Ashish Sharma, Ara Miran, and Zanyar Rzgar Ahmed

Abstract Nowadays, the world suffers from a terrible problem with COVID-19. Some researchers worked for a facemask detection biometric system by using Residual Networks such as Resnet50 or Resnet100. This research focuses on depreciating the transmission of Corona Virus Disease (COVID) from person to person. To wear a facemask plays an excellent role in not spreading COVID to the community. Moreover, to enhance social life, automatic facemask detection and facemask recognition systems are needed. Additionally, this system is helpful for security enhancement through face recognition. Here, the research for developing and implementing a biometric system for banks, offices, universities, and other public areas. This system helps in detecting the facemask for wearing by the human With Artificial Intelligence (AI), Deep Learning (DL), and Digital Image Processing technologies, this system allows the person to enter inside or stay outside because of not wearing a facemask. Besides designing and implementing a new model, the authors will discuss pre-defined the VGG16 deep learning model of CNN (Convolution Neural Network). Further, conclude the performance of both CNN models. This paper proposes a Facemask Detection model for solving the problem of manual care. This proposed model is a combination of most trending technologies such as AI, DL, and Image processing. In the future, describe this newly implemented model by appending Gaussian noise with images and make the system more reliable for actual use.

The original version of this chapter was revised: The affiliations of authors "Ashish Sharma, Ara Miran, Zanyar Rzgar Ahmed" has been updated. The correction to this chapter is available at https://doi.org/10.1007/978-981-16-5655-2_91

A. Sharma (✉) · Z. R. Ahmed
Department of Information Technology, Lebanese French University, Erbil, Kurdistan, Iraq
e-mail: ashish.sharma@lfu.edu.krd

Z. R. Ahmed
e-mail: zanyar.ahmed@lfu.edu.krd

A. Sharma · A. Miran · Z. R. Ahmed
College of Engineering and Computer Science, Lebanese French University, Erbil, Kurdistan, Iraq

A. Miran
Department of Computer Networking, Lebanese French University, Erbil, Kurdistan, Iraq
e-mail: ara.zozan@lfu.edu.krd

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022, corrected publication 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_60

Keywords COVID-19 · Facemask · Face detection · Biometric system · Artificial Intelligence (AI)

1 Introduction

The World Health Organization (WHO) declared that coronavirus (COVID-19) is an epidemic virus [1]. The world is suffering from a pandemic disease COVID-19 and following the new COVID-Strain as COVID-20. As per the news, in the previous months of 2020, most countries started to lockdown public gathering places such as schools, colleges, universities, and offices. These are the exercises to be followed only, not to spread the virus to the nation. Lockdown is not an explication of the problem for a long time. Due to the lockdown, countries are suffering from the economic, financial crisis too much. Human life is not suitable everyday for working, studying, and relationships. The researchers identified that the virus spreads through social gatherings, close connections, congested and overpopulated regions [1].

Accordingly, to avoid the extent of infection to the inhabitants of the nation. The facemask to be worn by the people plays a significant role in not spreading the virus to the community. Here, this Facemask Detection System (FDS) is profitable to avoid human effort. The FDS detects the facemask on people's faces implicitly. Some of the people are not wearing the facemask while going outside to the crowded areas. The FDS identifies the people not wearing a facemask and is against issue a warning.

As the reverse facility of the same research is enhancing the public security. It is the opposite utility of the same system. According to train the model for the training dataset, FDS will provide results. If the train system recognizes the face without a mask and allows the individual to enter inside any building, then as per training, it will perform and manage the security for the region. Vice versa, if the trained model recognizes the face with mask to allow any person inside the building, it will perform and minimize the spreading of Corona Virus among the public.

This research is an implementation of the FDS model. The FDS is a hybrid model that consists of AI deep learning (DL) concepts. The DL algorithms help train the system (or hardware) for working artificially intelligently.

2 Previous Studies

Generally, in the past months, within the spread of pandemic Covid-19 worldwide, many researchers conducted publications on the pandemic and the technology of detecting face masks. In this study, the focus is more on developing and implementing a biometric system for humans. Researchers and scientists have demonstrated that wearing face masks helps reduce the spreading rate of COVID-19.

In [1], the authors proposed models that consist of two modules. The first module has been designed for feature removal using Resnet50. Moreover, the second module

has designed the face masks classification process using decision trees, Support Vector Machine (SVM), and ensemble algorithm. For the investigations and detections, three faces masked in the database have been selecting for further analysis. The Three datasets are the Real-World Masked Face Dataset (RMFD), the Simulated Masked Face Dataset (SMFD), and the Labeled Faces in the Wild (LFW). The SVM classifier reached 99.64% testing precision in RMFD. In SMFD, it reached 99.49%, while in LFW, it achieved 100% testing precision.

Meanwhile, in [2], the authors have usurped the layout matching method, face shapes signified from the passageway picture adequately. A picture-based face mask produces to get a format face picture. The format face mask evaluates the fundamental and fruitful strategy to specify a face from the entrance picture. Although light, contrast, complex foundation, skin shading contrasts controls for face mask technique has operated effectively. The template face mask and face image from the entrance picture must be roughly 10% of error. In this event, the face picture size is more notable than the face mask size or more noticeable than the face picture size, and out of 10% error, regulating execution was lowered.

In [3], it proposes that deep learning detects persons who are not wearing the mask. Here the deep learning has been built by using transfer learning of InceptionV3. In this work picture, growth procedures utilize to upgrade the model's execution, as they increment the variety of the preparation information. The proposed transfer learning model accomplished exactness and explicitness of 99.92%, 99.9% during preparing, and 100%, during testing on the SMFD dataset (Fig. 1).

In [4], they introduced a face mask detection model based on the face recognition algorithm: pyramid box, which is very suitable for the current situation in

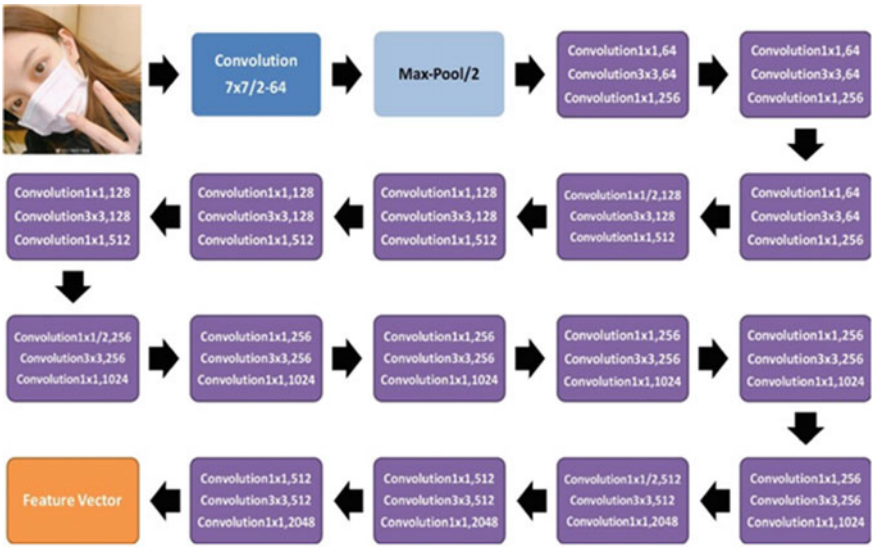


Fig. 1 ResNet-50 as the feature extractor [1]

the environment for the rapid rise of the virus. The pyramid box, mask recognition calculation results have accomplished the common objective. They can utilize the pyramid box of the mask recognition model and distinguish whether the face in the image is wearing a mask rapidly and can give the precision of judgment. The actual acknowledgment achievement rate is over 90% in the nearby scene, which shows the pyramid box. The face identification calculation is incredible, demonstrating that deep learning is a great help to human beings. The week's point is that the model's accuracy needs to be improved, especially when there are more faces in public places.

In [5] the paper with the fast sprayed of Covid-19, they successfully built a detection module for detecting masks and faces. The primary purpose of this research is to create an application and used it on the door of malls. Once the door opens, it can catch either the person wear or not the mask—the research scope is based on classification models in Machine Learning. Besides boosting techniques and the operation of neural networks in Deep Learning, it recognizes if the individual is wearing a mask.

In [6], they were able to generate accurate face mask detection from RGB frequency images comprising local objects. They demonstrate their results on Multi Human Parsing Dataset having the Mean accuracy of pixel level. Additionally, false expectations have been explaining, and an appropriate bounding box has been drawing around the fragmented district. The strategy can discover applications in advanced tasks, for example, facial part recognition.

In [7], they observed 9 COVID-19 deep learning applications according to the pathogen's fast analysis. Since clinical IoT devices frequently focus on malware, they planned to consider static and dynamic malware as annoyances and commotion vectors to produce ill-disposed models. They have utilized industry-standard devices, for example, IBM ART, to assess and shield their calculations against ill-disposed dangers. They have recognized that the current DL applications are helpless against AE assaults, requiring further examination, consideration, and usage of suitable protector instruments, shields, and controls before these applications utilize, all things considered, medical services offices.

Furthermore [8] in the research, a *G*-Mask technique suggests face recognition and division. The methodology can extricate includes ResNet-101, create ROIs by RPN, protect the exact spatial situation by RoIAlign, and produce paired masks through the entire convolutional network (FCN). The research structure can recognize faces accurately. While also definitely fragmenting each expression in an image, exploratory outcomes with self-manufactured expression datasets just as openly accessible datasets have confirmed that the proposed *G*-Mask strategy accomplishes promising execution.

The research article [9] presented two different profitable FRS to custom 3*D* silicone face masks. They have a certain new dataset based on eight different themes. For individual subjects, a custom silicone mask has been created. Their experiments specify the remaining detection truth of the LBP-SVM method with D-EER = 0%, BPCER = 0% @ APCER = 10 and 5%.

Finally, in [10], the paper briefly explained the image process operations for 3*D* images. The three significant tasks chose for execution are improvement partition

and obscure. This paper discussed the details of the product utilized for usages in MATLAB and the outputs of calculations. Beforehand their activities were done consumed 2*D* pictures, and now the proposed work measures 3*D* graphics.

3 Methodology

This methodology represents a new CNN deep learning Facemask recognition model. This research focuses on two models such as 1. Design and implements a new user-defined model; 2. Discussion about pre-defined VGG16 model.

3.1 Design and Implements a New User-Defined Model

Firstly, for a new user-defined model, write all algorithm steps to develop a practical and worthy system. This system is entirely base on AI technology. It is comprehending the actions of the deep learning CNN model for a different facemask detection system. The steps are as follows:

Algorithm for User-defined Facemask Detection Model.

Step-1. *Initiate a model.*
Step-2. *To import all the required inbuilt libraries, such as:*
TensorFlow, Keras, NumPy, Matplotlib, Confusion matrix
Step-3.*To prepare data for training the model, validating the model, and testing the model.*
→ *Set path for image data collection*
→ *Classify the image data into two classes, such as with_mask and without_mask.*
→ *Divide image data into distinct batches, i.e., train_batches, valid_batches, and test_batches.*
Step-4.*Display images.*

→ *Plot images in the form of a grid of one (01) row and ten (10) columns.*

Step-5.*Build a new facemask detection model by CNN.*

→ *Design a sequential model with convolution 2D filters, kernel-size, activation function 'relu,' and padding function 'same'; maximum pooling size of 2D images; add a dense layer with activation function 'softmax.'*

→ *Summarize the model.*

Step-6. *Compile a new facemask detection model.*
Step-7. *Train a new facemask detection model as per collected image data.*
→ *Plot a graph to show the 'Training and Validation Accuracy' and 'Training and Validation Loss.'*



Fig. 2 Show image data in one row and ten columns for user-defined FDS

Step-8. *Predict the model as per test_batches collected image data.*
→ *To show the results as an array of 0 and 1 to classify the object without_mask and with_mask, respectively.*
→ *To round-off the prediction array values of the above step by using NumPy inbuilt library.*
Step-9. *Create a Confusion matrix without normalization to represent the accuracy of a new facemask detection model for adapting.*
Step-10. *End.*

An explanation of a user-defined FDS imitates the system with collected data for training, validating, and testing the model. For training, validating, and testing purposes, here 1315 image data, 142 image data, and 194 image data respectively use. This whole image data is classifying into two categories, with_mask, and without_mask. This data has been taken from the kaggle.com website (https://www.kaggle.com/datasets). During the source code execution to make the training_batches, validation_batches, and testing_batches for image data with two classes. Then, plot the images in one row and ten columns with each figure-size 20 × 20 pixels setting.

See Fig. 2. This result clearly shows an array of binary digits zero (0) and one (1). Here, 1 represents an image with_mask, and 0 illustrates an image without_mask. According to the same, it defines the result to classify whole image data into two forms.

Figure 3 illustrates the user-defined FDS model by using the CNN technique to decide on the object is with_mask or without_mask as output. In detail indicates that the Convolution layer with activation layer 'ReLu,' the Pooling layer for input and intermediate steps, and output layer activation 'SoftMax' function. After the Input layer to Flatten layer is known as Feature Maps. The feature map includes the filtration process of a layer and provides the output. Then this previous layer output is an input for the next layer and continuing the same process till it finishes all layers in between with the given images' dataset. Combining the Input dataset (or input layer) with feature maps up to flatten layer is termed Feature Extraction. The subsequent flatten layer to get output data in an image with_mask, or without_mask is called Fully Connected Layer. During this process, from flattening layer to output layer

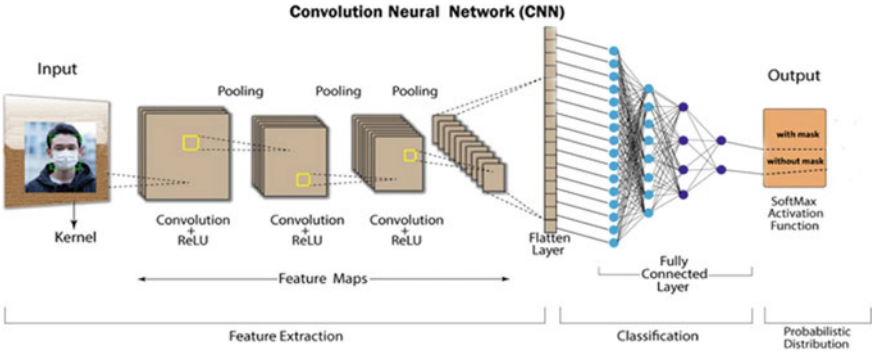


Fig. 3 User-defined facemask detection system

```
Model: "User-defined Sequential"
_________________________________________________________________
Total params: 775,778
Trainable params: 775,778
Non-trainable params: 0
_________________________________________________________________
```

Fig. 4 Summary of user-defined model

categories, the images in two classes are acknowledged as Classification. After the following method of the user-defined model will determine Probabilistic Distribution with two types of images with_mask or without_mask. Here, after building a user-defined FDS model, look at the summary part of a model. It describes its features nicely.

This summary shows in Fig. 4, sequential model architecture is a combination of seven convolution 2*D* (Conv2D), seven max-pooling 2*D* (MaxPooling2), one flattens (Flatten), and one dense (Dense) layer. As a result, it represents all of the parameters (params) that the system has trained, such as **Total params:** 775,778; **Trainable params:** 775,778, and; **Non-trainable params:** 0.

Further, compile the user-defined FDS model using compile function with Adam optimizers from Tensorflow and Keras library.

Furthermore, train the user-defined FDS model as per algorithm for building a user-defined FDS model. The system trains with fit function and store result to anyone variable. It uses five epochs or iterations processes to train a model for further optimal use.

See Fig. 5. It represents the results after five iterations process completed by the user-defined FDS model. Here for prediction, 100% accuracy, 3.37% minimum losses for training, and 97.89% accuracy, 0.07% minimum losses for validation. According to the actual results, data visualizes in Fig. 6 for Training and Validation Accuracy and Fig. 7 for Training and Validation Losses after five Epochs of User-

```
Epoch 1/5
132/132 - 178s - loss: 0.0352 - accuracy: 0.9894 - val_loss: 0.0391 - val_accuracy: 0.9859
Epoch 2/5
132/132 - 178s - loss: 0.0100 - accuracy: 0.9962 - val_loss: 0.0702 - val_accuracy: 0.9789
Epoch 3/5
132/132 - 178s - loss: 0.0020 - accuracy: 1.0000 - val_loss: 0.0761 - val_accuracy: 0.9789
Epoch 4/5
132/132 - 178s - loss: 4.7582e-04 - accuracy: 1.0000 - val_loss: 0.0766 - val_accuracy: 0.9789
Epoch 5/5
132/132 - 182s - loss: 3.3719e-04 - accuracy: 1.0000 - val_loss: 0.0779 - val_accuracy: 0.9789
```

Fig. 5 Result after five epochs to train the user-defined FDS

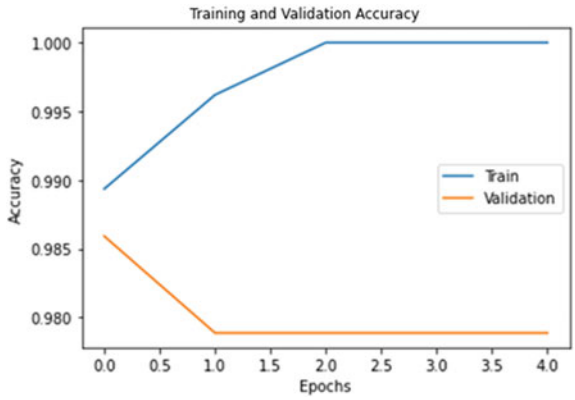


Fig. 6 Training and validation accuracy after five epochs of user-defined FDS

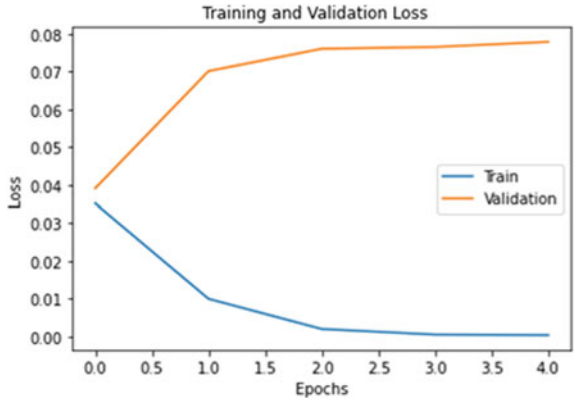


Fig. 7 Training and validation loss after five epochs of user-defined FDS

defined FDS. The total execution time for training a user-defined FDS model is 894 s, i.e., approximately 15 min, mentions in Fig. 5.

Now, it is showing that user-defined FDS is ready for the act of predicting by reasoning about future utilization. This will provide the outcome as per training the model in the previous step.

It is very much evident by seeing the actual result of the user-defined FDS model after prediction. It is exactly matching to the expected outcome of the system. Here, at work, all the faces are covered with masks. So, the predicting array is [1, 0] only for all one row and ten columns, as shown in Fig. 8.

See Fig. 9. This confusion matrix shows the result regarding the adaptation of the user-defined FDS model for natural use. It presents the predictions result in real-time,



Fig. 8 After prediction step for user-defined FDS

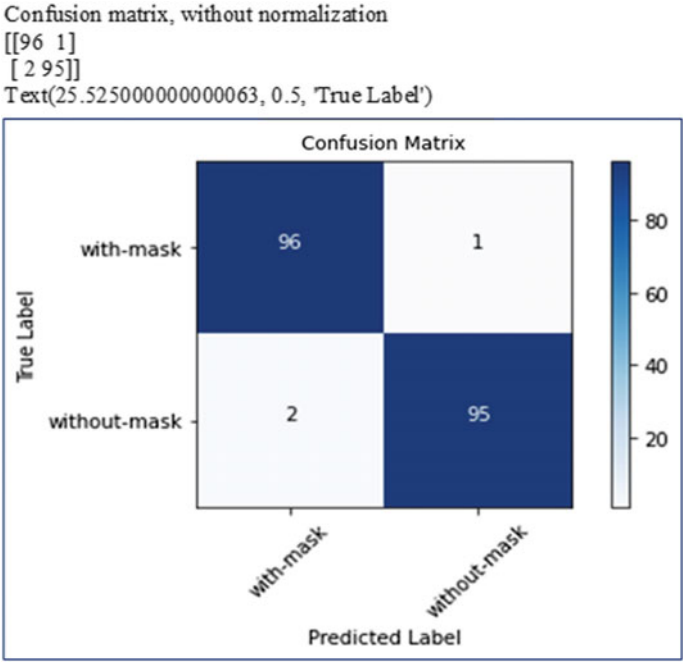


Fig. 9 Confusion matrix of user-defined FDS

i.e., detects 96% age precision for with_mask to with_mask and 95%age correct for without_mask to without_mask.

3.2 Discussion About Pre-Defined VGG16 Model

Secondly, for a pre-defined (or system-defined) model, the internet is the primary resource to access the VGG16 inbuilt model. It should be download first, then make it worthwhile.

Algorithm for Pre-defined Facemask Detection Model.

Step-1. *Initiate an inbuilt VGG16 model. Internet connection is needed.*
Step-2. *Download the VGG16 model, follow the link (*https://storage.googleapis.com/tensorflow/keras-applications/vgg16/vgg16_weights_tf_dim_ordering_tf_kernels.h5*)*
Step-3. *From inbuilt VGG16 model:*
→ *Remove the last layer such as* ***predictions(Dense)*** *layer*
→ *Add a new last layer such as* ***dense_1(Dense)*** *layer*
Step-4. *Compile the VGG16 inbuilt model.*
Step-5. *Train and validate the VGG16 model with collected image data of train_batches and valid_batches.*
→ *Plot a graph to show the 'VGG16 Model: Training and Validation Accuracy' and 'VGG16 Model: Training and Validation Loss'.*
Step-6. *Predict using fine-tuned VGG16 model as per test_batches collected images data.*
→ *To show the result as plotting images with an array of 0 and 1 to classify the object without_mask and with_mask, respectively.*
Step-7. *Create a Confusion matrix without normalization for the VGG16 model to represent a facemask detection model's accuracy for adapting.*
Step-8. *End.*

Figure 10 demonstrates the VGG16 pre-defined FDS model. According to the above algorithm, this architecture has been designing. It is an accurate model with a substantial layered architecture. This VGG16 FDS model takes more time to execute

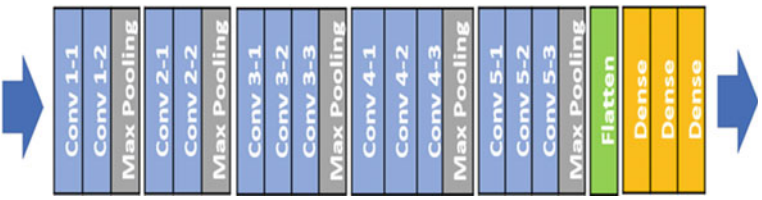


Fig. 10 Pre-defined VGG16 facemask detection system

```
Model: "System-defined Sequential"
_________________________________________________________________
Total params: 134,268,738
Trainable params: 8,194
Non-trainable params: 134,260,544
_________________________________________________________________
```

Fig. 11 Summary of system-defined VGG16 model

```
Epoch 1/5
132/132 - 954s - loss: 0.0125 - accuracy: 0.9992 - val_loss: 0.0085 - val_accuracy: 1.0000
Epoch 2/5
132/132 - 819s - loss: 0.0096 - accuracy: 0.9992 - val_loss: 0.0079 - val_accuracy: 1.0000
Epoch 3/5
132/132 - 754s - loss: 0.0077 - accuracy: 1.0000 - val_loss: 0.0068 - val_accuracy: 1.0000
Epoch 4/5
132/132 - 753s - loss: 0.0064 - accuracy: 1.0000 - val_loss: 0.0059 - val_accuracy: 1.0000
Epoch 5/5
132/132 - 753s - loss: 0.0054 - accuracy: 1.0000 - val_loss: 0.0057 - val_accuracy: 1.0000
```

Fig. 12 Result after five epochs to train the pre-defined VGG16 FDS

the same number of repetitive steps than user-defined FDS model architecture with the same system configuration. To verify the same, see Figs. 5 and 12.

This algorithm is showing clearly modifications regarding the last layers of the VGG16 pre-defined model. In Step-3, remove the predictions (Dense) layer and add a new dense_1 (Dense) layer. After these modifications, the summary of the pre-defined VGG16 model manifested in Fig. 11.

See Fig. 11 summary shows, sequential model architecture is a combination of two convolution 2D (Conv2D), one max-pooling 2D (MaxPooling2), two convolution 2D (Conv2D), one max-pooling 2D (MaxPooling2), three convolution 2D (Conv2D), one max-pooling 2D (MaxPooling2), three convolution 2D (Conv2D), one max-pooling 2D (MaxPooling2), three convolution 2D (Conv2D), one max-pooling 2D (MaxPooling2), one flattens (Flatten), two dense and one extra added dense (Dense) layer. As a result, it represents all of the parameters (params) that the system has trained, such as **Total params:** 134,268,738; **Trainable params:** 8194, and; **Non-trainable params:** 134,260,544.

After this, compiles the pre-defined VGG16 FDS model using compile function with Adam optimizers from Tensorflow and Keras library. Furthermore, train the pre-defined VGG16 FDS model as per algorithm for built a pre-defined VGG16 FDS model. The system trains with fit function and store result to anyone variable. It uses five epochs or iterations processes to train a model for further optimal use.

See Fig. 12. It represents the results after five iterations process completed by the pre-defined VGG16 FDS model. Here for prediction, 100% accuracy, 0.00% losses for training, and 100% accuracy, 0.00% losses for validation.

According to the actual results, data visualizes in Fig. 13 for Training and Vali-

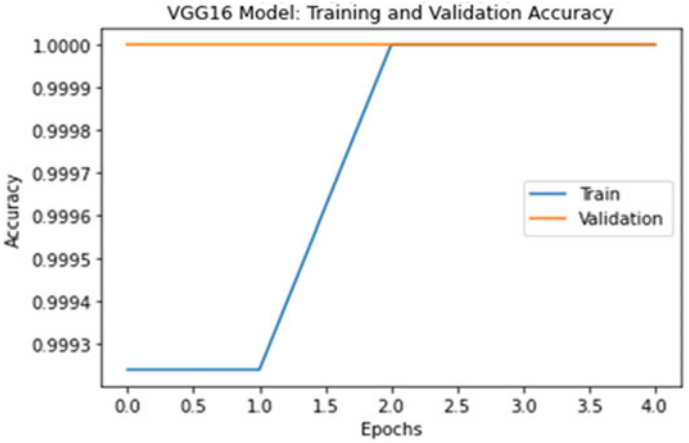


Fig. 13 Training and validation accuracy after five epochs of pre-defined FDS

dation Accuracy and Fig. 14 for Training and Validation Losses after five Epochs of Pre-defined FDS. The total execution time for training a pre-defined FDS model is 4,033 s, i.e., approximately 1 h and 7 min, mentions in Fig. 12.

Now, it is showing that pre-defined VGG16 FDS is ready for the act of predicting by reasoning about the future utilization. This will provide the outcome as per training the model in the previous step.

Figure 15, it is very much evident by seeing the actual result of the pre-defined VGG16 FDS model after prediction. It is exactly matching to the expected outcome of the system. Here, at work, all the faces are covered with masks. So, the predicting array is [1, 0] only for all one row and ten columns.

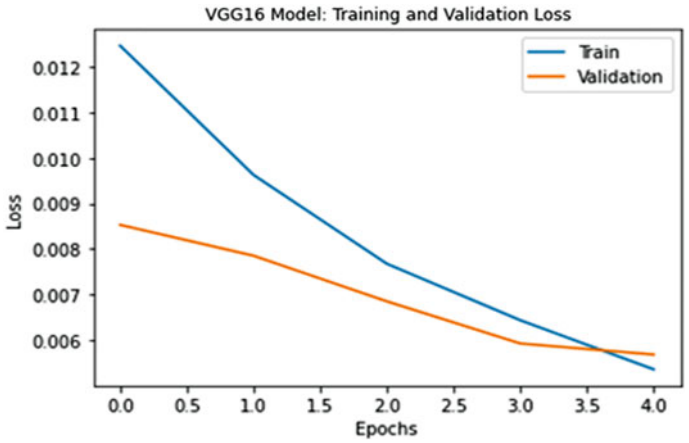


Fig. 14 Training and validation loss after five epochs of pre-defined FDS



Fig. 15 After prediction steps for pre-defined VGG16 FDS

See Fig. 16. This confusion matrix shows the result regarding the adaptation of the pre-defined VGG16 FDS model for general use. It presents the predictions result in real-time, i.e., detects 96% age precision for with_mask to with_mask and 96% age correct for without_mask to without_mask. Here, it clearly shows that results are not much different from the user-defined FDS model confusion matrix, as shown in Fig. 9.

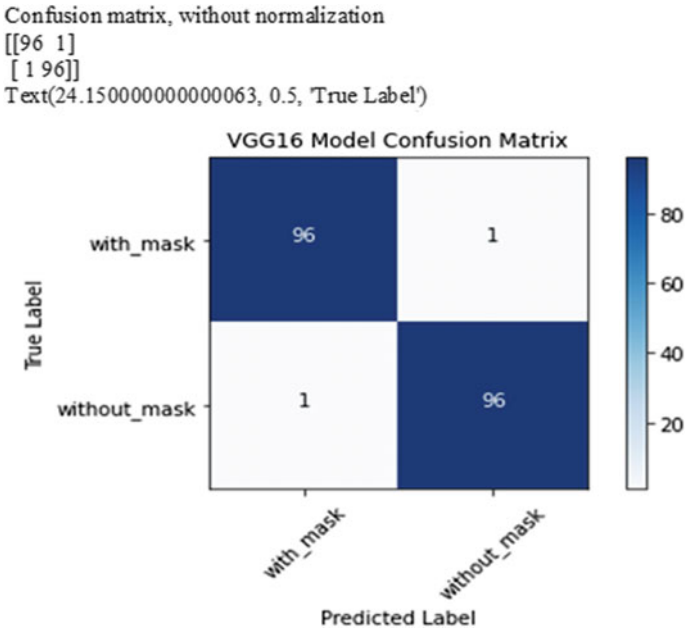


Fig. 16 Confusion matrix of pre-defined FDS

3.3 Discussion About Adding Gaussian Noise to the Image Dataset

By adding Gaussian noise to the image dataset, the prediction should be extra realistic. If the object is behind a glass door, the FDS also eligible to detect the facemask and provide the best results. Gaussian noise is adding over the image, see the result in Fig. 17.

Then uses a bilateral filter on Gaussian noise added over the image. The bilateral filters are helpful to denoise the image. After completing this process, try to differentiate between the original image and the denoised image with an edge detector. The result in Fig. 18.

Further, to verify the differences between using Edge detector for Original Image and Filtered Image. Then see Figs. 19 and 20 make sure the actual results. In Fig. 19, it is after applying an edge detector on the original image. The actual result is having much of the noise and not clear to detect the object's facemask.

As compared to Fig. 19, see Fig. 20 is more and more clear to detect the facemask after applying an edge detector on the denoised image. The actual result is pretty satisfactory after using a bilateral filter on the original image.

4 Discussion About FDS Model

Here, this is an engineered discourse to circumvent manual care challenges for detecting face masks and the security system. FDS presents the safety-catch innovation to the COVID-19. It serves to detect the facemask in real-time and lead to the alert to avoid spreading disease. Moreover, reverse advantage enhances the public security in any building to detect the person who wears the mask. The same FDS is usable for both conditions; train the model as per the requirements. The FDS consists of CNN's profound innovation and image processing learning concept for its technical design and implementation. It is discussed here about user-defined and pre-defined FDS models. Both systems provide 100% age accuracy with minimum losses or no losses regarding training and validation as per actual results. For the pre-defined VGG16 FDS model, internet services should be available to utilize this system in the natural environment. Whereas, for the user-defined FDS model, internet services are not mandatory for the same environment. The pre-defined VGG16 FDS model takes five times the time for training compared to the user-defined FDS model. See Figs. 12 and 5, respectively.

Figs. 9 and 16 both define the confusion matrices of user-defined and pre-defined FDS models sequentially. These matrices results are very near each other, i.e., 96%, to prefer any models. Furthermore, to get more accuracy with results for train models, applied Gaussian noise with datasets. It facilitates to provides better accuracy at the edges of the image. So, it precise the tangible result for further forecasts and finds more on more sharpness.

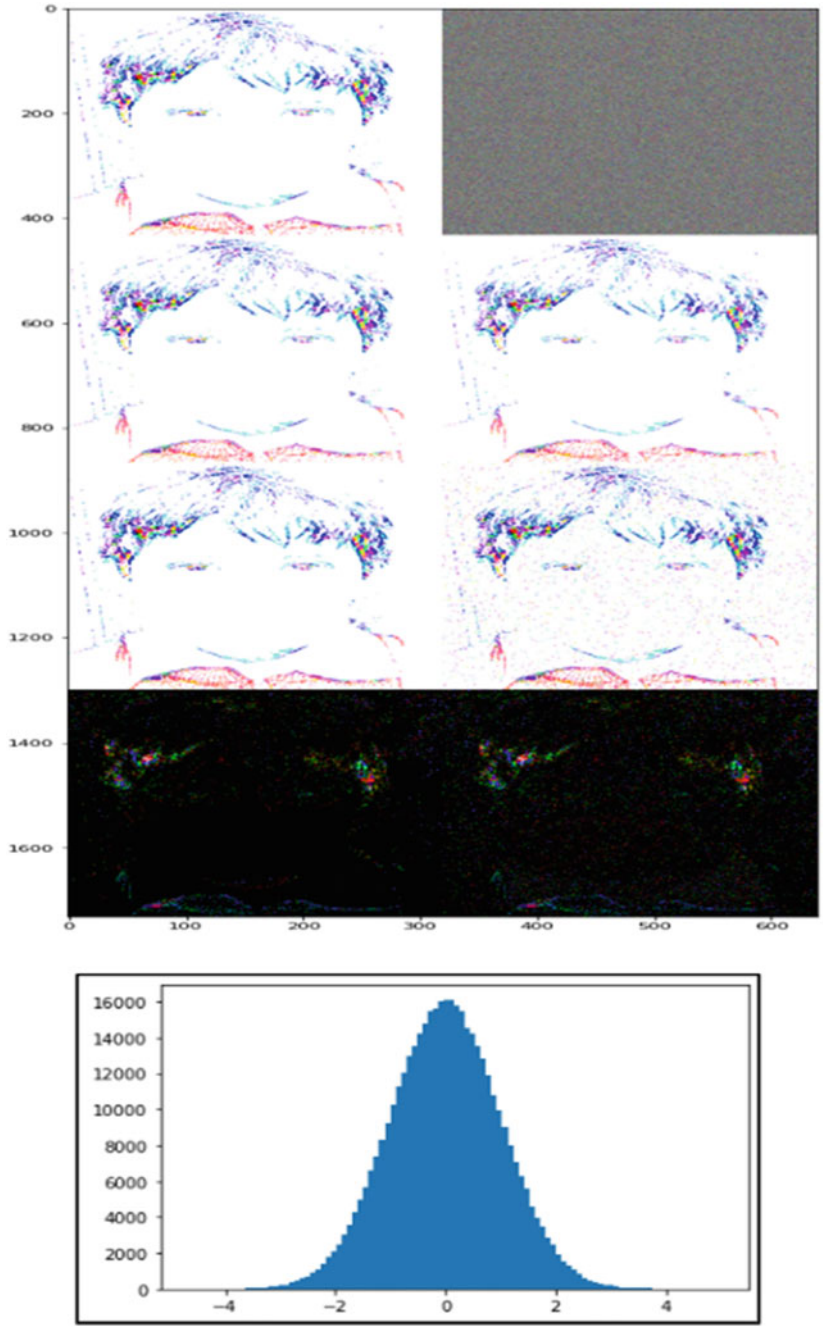


Fig. 17 After adding Gaussian noise to the image



Fig. 18 After using bilateral filter on Gaussian noise added image

5 Conclusion

After exercising with both user-defined and pre-defined FDS models, the user-defined model is succeeding. This model works in real-time without using internet services. It runs directly on a local server. It takes significantly less time to train and predict the

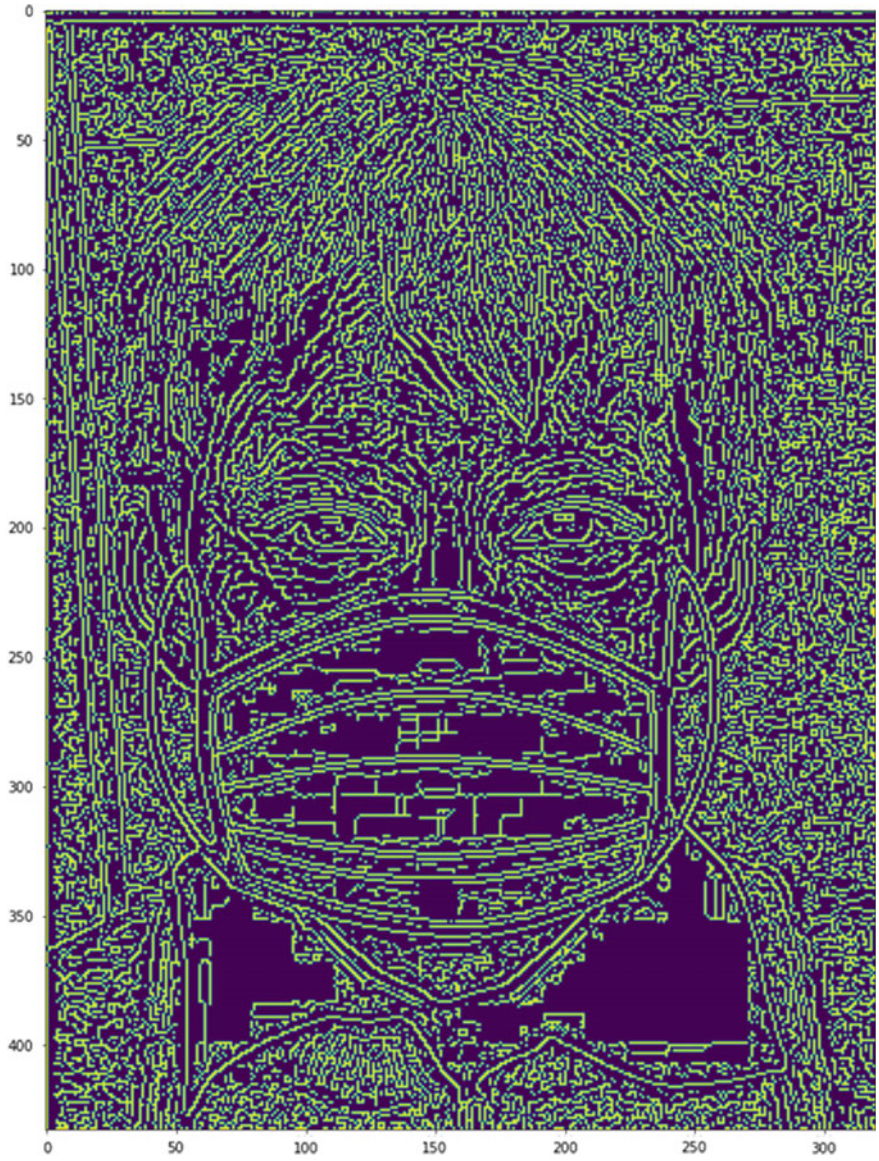


Fig. 19 After using edge detector for original image on Gaussian noise added image

model compared to the pre-defined VGG16 FDS model. Even the exact results are very similar after functioning with both FDS models. It concludes that it is preferable to use the user-defined FDS model to save time for training, predicting, and detecting the facemasks in real-time. This system is beneficial for maintaining the safety to

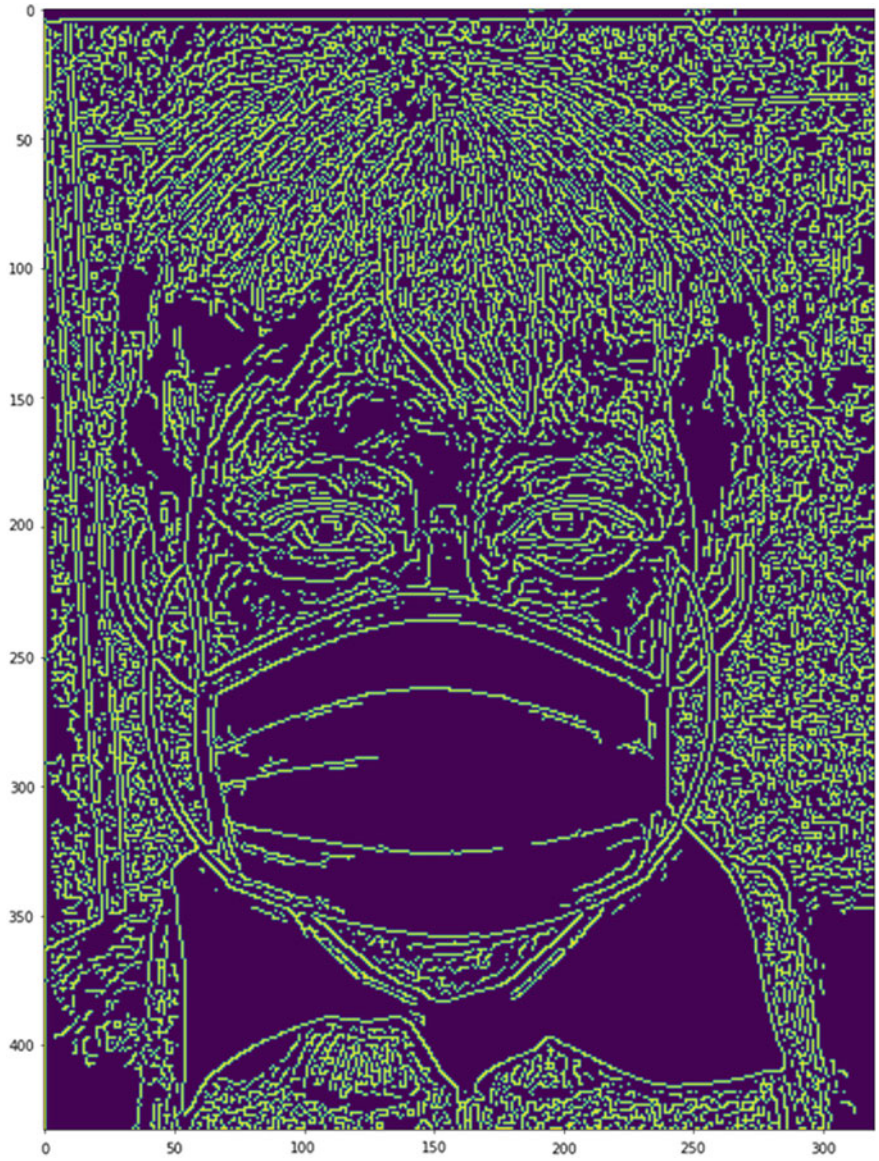


Fig. 20 After using edge detector for filtered image on Gaussian noise added image

observe the object with masks and without masks. It depends on training the model in a particular way. Then the model will give the results accordingly.

The limitation of the proposed deep learning FDS user-defined model is that training is highly precious due to complicated data patterns. Additionally, it demands

high-priced fancy graphics processing units (GPUs) and hundreds of machines, making it costly.

References

1. M. Loey, G. Manogaran, M. Taha, N. Khalifa, A hybrid deep transfer learning model with machine learning methods for face mask detection in the era of the COVID-19 pandemic. Measur. J. Int. Measur. Confederation **167**, 108288 (2021). https://doi.org/10.1016/j.measurement.2020.108288
2. S.Yilmaz, M. Salhmuhsn, Face detection using template face mask. J. Multimedia Process. Technol. **4**(4) (2013). https://www.dline.info/jmpt/fulltext/v4n4/3.pdf
3. G. Jignesh Chowdary, N.S. Punn, S.K. Sonbhadra, S. Agarwal, Face mask detection using transfer learning of inceptionV3 in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12581, Springer Science and Business Media Deutschland GmbH, (LNCS, 2020), pp. 81–90. https://doi.org/10.1007/978-3-030-66665-1_6
4. Y. Liu, J. Liu, K. Chen, Mask detection algorithm based on pyramid box. J. Image Process. Theory Appli. **3**, 11–19 (2020). https://doi.org/10.23977/jipta.2020.31002
5. T. Venkat Narayana Rao, G. Vishal Sai, M. Chenna, M. Sahas Reddy, An application for the detection of COVID-19 face mask using OpenCV. **26**(7) (2020). https://doi.org/10.37896/HTL26.07/1394
6. T. Meenpal, A. Balakrishnan, A. Verma, Facial mask detection using semantic segmentation, in *2019 4th International Conference on Computing, Communications and Security, ICCCS 2019*. Institute of Electrical and Electronics Engineers Inc. (2019). https://doi.org/10.1109/CCCS.2019.8888092
7. A. Rahman, M.S. Hossain, N.A. Alrajeh, F. Alsolami, Adversarial examples—security threats to COVID-19 deep learning systems in medical IoT devices. IEEE Internet Things J. 1–1. (2020). https://doi.org/10.1109/jiot.2020.3013710
8. K. Lin, H. Zhao, J. Lv, C. Li, X. Liu, R. Chen, Z. Wang, Face detection and segmentation based on improved mask R-CNN. Discrete Dynamics in Nature and Society, 2020 (2020). https://doi.org/10.1155/2020/9242917
9. R. Ramachandra, S. Venkatesh, K.B. Raja, S. Bhattacharjee, P. Wasnik, S. Marcel, C. Busch, Custom silicone face masks: Vulnerability of commercial face recognition systems & presentation attack detection, in *2019 7th International Workshop on Biometrics and Forensics, IWBF 2019*. Institute of Electrical and Electronics Engineers Inc. (2019). https://doi.org/10.1109/IWBF.2019.8739236
10. A. Padmapriya, S. Vigneshnarthi, Image processing operations for 3d image. Int. J. Sci. Res. **2**(6), 1–6 (2012)

ICT Enabled Cloud Cafeteria of Corporate Companies with a Customized App for Employee's Expediency

H. M. Moyeenudin, S. Chandrachud, and A. Mohammed Faisal

Abstract The growth of multinational enterprises has created a platform for Cloud cafeteria by digitizing their workplaces through mobile application assisted by ICT (Information and Communication Technology) and IoT (Internet of Things), for making their food preferences before their meal by placing their order through mobile app from workstation and visiting the counter once their food is ready to serve. This lessens the turnaround time for the decided food choice and furthermore decreases the heap on the cafeteria particularly during top long periods especially for dining, some of the multinational enterprises provides access to WIFI and furthermore as another option to utilize this facility on contract. This innovation stage of interface facilitates the Corporate Employees to communicate with food vendors and the Company Administration continuously, through a personalized application for employees of corporate companies. The aim of this research is to identify the part of mobile app on providing the convenience for corporate employees during their lunch and dinner sessions and secondly focused on the association of ICT with this mobile app.

Keywords Cloud cafeteria · Digital café · Mobile app · ICT

1 Introduction

The ICT has an association with Cloud cafeterias through Internet and electronic gadgets particularly by mobile phones [1], tabs as these gadgets comes with android facility, many mobile apps are generated for android, and simultaneously for desktop and laptops, these apps are enabled with windows and mackintosh systems. The food vendors have an arrangement of serving Breakfast, Lunch and dinner by setting them on discrete preparation on requirement with food orders placed by employees of corporate companies using mobile app nevertheless these Cloud cafeterias are located at the companies. The employees can collect food and beverages from food counter and move toward their table to take as a lot of nourishment as they wish.

H. M. Moyeenudin (✉) · S. Chandrachud · A. Mohammed Faisal
Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai, India
e-mail: moyeenudin@velsuniv.org

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_61

The center process of Cloud cafeteria is through connecting the food vendors with a mobile application that innovates and assumes a focal job in offering some enticement by an interface to every one of the partners. There are many food and beverage outlets comprised to form a food court at a multinational corporate companies with the foods from various cuisines. Numerous specialty restaurants use this framework for productivity and ease of serving at large enterprises which consist thousands of employees. At present, this concept is also applied at multiplex, shopping malls with the aid of mobile app for placing orders and making payments with Cloud wallet and the menus are designed with the pictures of dishes as like in online food delivery apps to satisfy the users [2], the commercial mobile apps helps Cloud cafeteria that has positioned their operations in corporate companies for the employees convenience at work, likewise it gives highlights like customized suggestions to employees through its Artificial Intelligence (AI) driven innovation arrangement, by comfort mode for the workforces at their work and so forth, among different highlights and different contributions of Cloud cafeteria, made to integrate as a completely agreeable cafeteria for the corporate companies, while curating food business for the corporate. It was a time consumption and burdensome procedure for the employees of corporate companies to get their food during busy hours and work schedules without any technology like this, thus organization can also assert the information with these applications for their employees and this cafeteria also disseminates offers and discounts of food and beverage outlets to their customers dependent on their necessities. For instance, in a corporate company this Cloud cafeteria convey the wishes to the employee on their birthday and give them free nourishment to commend their day. At that point at their customers' command, they have propelled the idea of 'Eat now, Pay later' in which clients can take care of their nourishment tabs whenever they wish. They additionally give information to the staffs of corporate company while some F&B outlets are getting high volumes to keep them informed and to prompting longer hold up time and numbers of available seats. As these Cloud cafeterias are tied up with many food and beverage outlets it will be easy for employees to opt foods from these outlets [3].

1.1 ICT with Cloud Computing

The ICT has become a main source for smooth functioning of restaurant industry with the help of cloud computing, by making mobile applications related to food ordering and delivery, thus Cloud cafeterias are able to receive the food orders and prepare the food before the client arrives to their table and this also assists in numerous areas like receiving feedbacks from clients instantly to build a rapport and client satisfaction [4]. The restaurants of Cloud café have an ease in providing the food and beverages to clients and also can guarantee that they have the correct item in the ideal spot at the ideal time to their clients or corporate employees, with the aid of IoT in association with cloud computing [5]. The mobile interface supports employees of organizations and continuously assists in providing nourishment with the cooking specialist of

various cuisines and F&B outlets, the cloud computing framework with ICT makes this process successful with a solitary eatery in their system [6]. This would be troublesome without the cloud computing support. The restaurateurs can make instant advancements at any time using cloud computing to support the Cloud cafeteria according to the organization types, rules and regulations. ICT comprised together with IoT, mobile phones and computer network mostly in multinational organizations to control remotely. It likewise integrates with the advanced network connected with android phones, mobile applications, Internet devices and Web sites. This technology keeps on modernizing the user capabilities from computer to contemporary mobile apps with the various transactions [7].

1.2 Network Authentication with ICT

The blend of locally smart gadgets with Cloud-based application giving out its offering that ascend to another segment of superiority through the network formed by cloud computing, it offers innovative utilization prototypes, and however, there are some increased capability of different vulnerabilities with probability of boundless computer-generated risks, will be controlled by an additionally available authentications [8]. There are extra worries of client troubles if suppliers are not observing the ability of computers systems and guidelines with advanced electronic gadgets for the restrictive digital arrangements. There were some added disputes of client information security and legitimate setting previously, due to the quick advancement of ICT with edge figuring boundaries of cloud-based arrangements these disputes are resolved [9]. This approach requires a Cloud cafeteria organizations system to be communicated regularly with the Cloud specialist for upgrading their application through cloud computing and staying away from any lawful entanglements. The ICT-based Cloud administration can resolve the security issues raised with the devices connected with Internet over the foundation of reliance, and safety in a cooperative cloud technology [10]. Ultimately, the modern themes of programming patches and utilizing AI for security enhancements are introduced through some patterns that are probably going to proceed as systems will turn out to be quicker and machines will turn out to be increasingly wise to perceive examples of information to decide. Thus advancement of ICT in network security has become imperative to create the network connected with computer and software or registering gadgets are on the edge to meet the servers guarantee a level in network performance [11].

2 Materials and Methods

A quantitative research is done to analyze the performance of Cloud cafeteria at an International Corporate Company of Chennai, with a set of questions to the employees are created in Google forms and disseminated at their social media

groups, in regard to the convenience on utilizing Cloud cafeteria, the sample size was measured about 250, out of that only 240 were used to complete this study. The correlation is carried out with SPSS version 21, to identify the variables relationship, a linear regression was also done to establish the significance of correlation coefficient.

3 Results and Discussion

The outcome of this study is based on the feedback given by the employees of multinational company, and the data is processed to know the relationship between the variable of the Cloud cafeteria by means of statistical association between variables. A correlation study is performed to identify the strength between the quantitative variables with its direct association on comfort on using Cloud cafeteria with network security, mode of food ordered by accessing mobile application or Web site using Mobile phone, Desktop or laptop and on the features of tracking their food delivery with its accuracy, making amendments and cancellation of food orders with their convenience. A well-planned cafeteria space must be adaptable, with the correct innovation set up to address a wide range of purposes and circumstances without any problem. The skilful, multi-reason innovation of cafeteria space can be a focal headquarters inside the structure and an exhibit piece for someone visiting the office, all with negligible venture.

3.1 Correlations

Table 1 indicates a stronger relationship for comfort from Cloud cafeteria with the variable order from mobile app by having value $r = 0.952^{**}$ and a significant value $p = 0.000$, the relationship between the variables like comfort from Cloud cafeteria with network security has worthy relationship with a correlation coefficient $r = 0.780^{**}$ and a significant value $p = 0.000$, which proves that the users of Cloud cafeteria are comfortable with network security. The relationship between orders from Desk with Food order from mobile app is having a good relationship with a correlation coefficient $r = 0.839^{**}$ and a significant value $p = 0.000$, thus there is a greater significance between food order from work desk using a mobile app. The employees of corporate companies are also convenient in cancelling their food orders using mobile app which is substantiated by significant value $p = 0.000$ with a coefficient value $r = 0.648^{**}$, this demonstrates that there is a strong association between these variables, cancelling these food orders using mobile app found to be comfortable with Cloud cafeteria as the correlation results displays a positive association for the variables comfort from Cloud cafeteria with food order cancellation with a significant value $p = 0.000$ with a correlation coefficient $r = 0.705^{**}$. It is also

Table 1 Correlation between the variables of Cloud cafeteria

Correlations							
		Comfort	Network security	Order from app	Food order cancellation	Accuracy	Order from desk
Comfort on Cafeteria service	P. Correlation	1	0.780**	0.952**	0.705**	0.869**	0.837**
	Sig.(2-tailed)		0.000	0.000	0.000	0.000	0.000
	N	240	240	240	240	240	240
Network security	P. Correlation	0.780**	1	0.800**	0.530**	0.697**	0.720**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000	0.000
	N	240	240	240	240	240	240
Order from app	P. Correlation	0.952**	0.800**	1	0.648**	0.853**	0.839**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000	0.000
	N	240	240	240	240	240	240
Food order cancellation	P. Correlation	0.705**	0.530**	0.648**	1	0.642**	0.607**
	Sig. (2-tailed)	0.000	0.000	0.000		0.000	0.000
	N	240	240	240	240	240	240
Food order accuracy	P. Correlation	0.869**	0.697**	0.853**	0.642**	1	0.818**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		0.000
	N	240	240	240	240	240	240
Order from desk	P. Correlation	0.837**	0.720**	0.839**	0.607**	0.818**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	
	N	240	240	240	240	240	240

**Correlation is significant at the 0.01 level (2-tailed)

observed from this study that the food from app has a greater accuracy with a significant value $p = 0.000$ and $r = 0.671$** evidences the good relationships between these variables. The outcome of this correlation has given a positive association with the usage of mobile app for Cloud cafeteria.

3.2 Regression Outcome

A linear regression is prepared to establish the strength of linear relationship between the independent and dependent variable. The variables have shown a minimal error

Table 2 Prediction of *R* Square

Model summary				
Model	*R*	*R* Square	Adjusted *R* Square	Std. error of the estimate
1	0.963[a]	0.928	0.926	2.382

[a]Predictors: (Constant), Food Order Accuracy, Food Order Cancellation, Network Security, Order From Desk, Order from App

and great relationship between each for providing the comfort through a mobile app used to order food.

Table 2 denotes the independent variables are statistically significant with the dependent variable comfort from Cloud cafeteria with an *R* Square Value 0.659, with adjusted *R* Square 0.928, as the proportion of variance obtained by independent variables, the predictors are food order cancellation, network security, food order accuracy, order from app and the food ordering from work desk.

Table 3 exhibits the *F* value 599.078, attained by mean square 3399.251 through regression is significant with a *p* value 0.000[b]. Indicates a stronger association between the dependent and independent variables and these independent variables are like food order cancellation, network security, food order, accuracy order from app and order from work desk are reliably predict the dependent variable comfort on Cafeteria Service. Since the group of independent variables or predictors are significant with dependent variable, this outcome substantiates that Cloud cafeteria of corporate companies is providing a comfort zone at workplace using android mobile app, laptop, desktop, WIFI campus with network security. The communication from employees to food vendors proved to be significant for convenience with the independent variables of this study. Furthermore, the possibilities of a food ordering mobile app of Cloud cafeteria has reduced the inconvenience during their duty routines.

The values obtained from regression equation exhibits in Table 4. Signifies the strength of each independent variable with dependent variable. As the outcome of this study is significant with the dependent variable comfort from Cloud cafeteria with predictors like food order cancellation, food accuracy, network security, order from app and results have been varied with each. For instance, the network security is not much related to comfort on Cloud cafeteria with the value ($b = 0.036$, $p =$

Table 3 Overall significance of regression

ANOVA[a]						
Model		Sum of squares	df	Mean square	*F*	Sig
1	Regression	16,996.253	5	3399.251	599.078	0.000[b]
	Residual	1327.747	234	5.674		
	Total	18,324.000	239			

[a]Dependent Variable: Comfort on Cafeteria Service
[b]Predictors: (Constant), Food Order Accuracy, Food Order Cancellation, Network Security, Order From Desk, Order from App

Table 4 Coefficients of cloud cafeteria

Coefficients[a]						
Model		Unstandardized coefficients		Standardized coefficients	*t*	Sig
		B	Std. error	Beta		
1	(Constant)	−6.446	2.021		−3.190	0.002
	Network security	0.036	0.030	0.036	1.214	0.226
	Order from app	0.759	0.049	0.679	15.552	0.000
	Food order cancellation	0.163	0.031	0.123	5.185	0.000
	Order from desk	0.051	0.039	0.045	1.282	0.201
	Food order accuracy	0.176	0.044	0.148	4.009	0.000

[a]Dependent Variable: Comfort on Cafeteria Service

0.226) this represents a variance on association. But there is a stronger significance for order from app with comfort from Cloud cafeteria through the value ($b = 0.759$, $p = 0.000$) proves that the food ordering by mobile apps to Cloud cafeteria are making the employees of corporate companies more comfortable and also indicates the convenience on cancellation of food order with the value ($b = 0.163$, $p = 0.000$). There is a noticeable variance for order from desk to Cloud cafeteria by ($b = 0.051$, $p = 0.201$) this determines the employee could place his order before reaching the company or from cafeteria. Users of Cloud cafeteria are also comfortable with accuracy of food received that is ordered by mobile app by a value ($b = 176$, $p = 0.000$).

3.2.1 Regression Curve on Food Order

Linear regression results are favorable on using a mobile app to order food by employees of corporate companies. This signifies the ICT usage, to communicate to more integrated devices in various segments, which is compatible with mobile phone, PC and computerized advancements than IT. The values from order from app with food order accuracy have shown a good association.

In Fig. 1. There is a stronger association between these two variables order from app and food order accuracy as the X and Y axis, the users of mobile app has shown a greater satisfaction on the accuracy of food received, as the mean values are distributed evenly on a straight line based on the percentage of using mobile app with the percentage on Accuracy of food. Fig. 2. Shows a gradual association of variables with usage of mobile app, nevertheless the users have various provisions

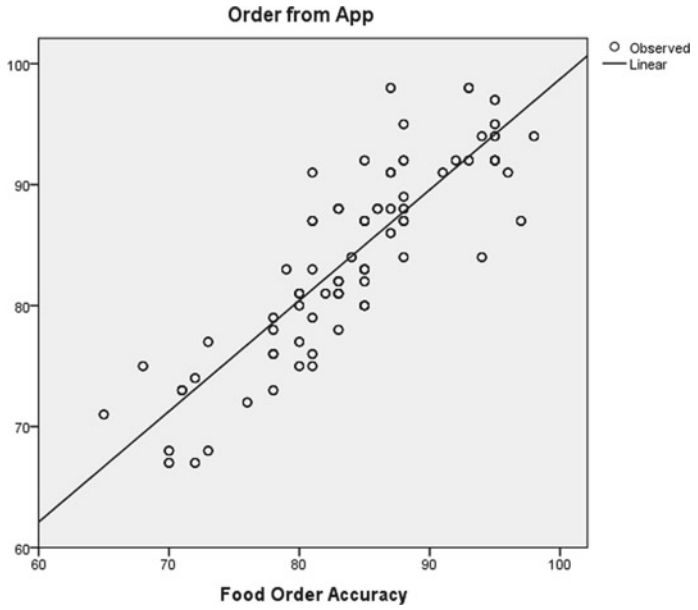


Fig. 1 Comparison of association between orders from app with food order accuracy

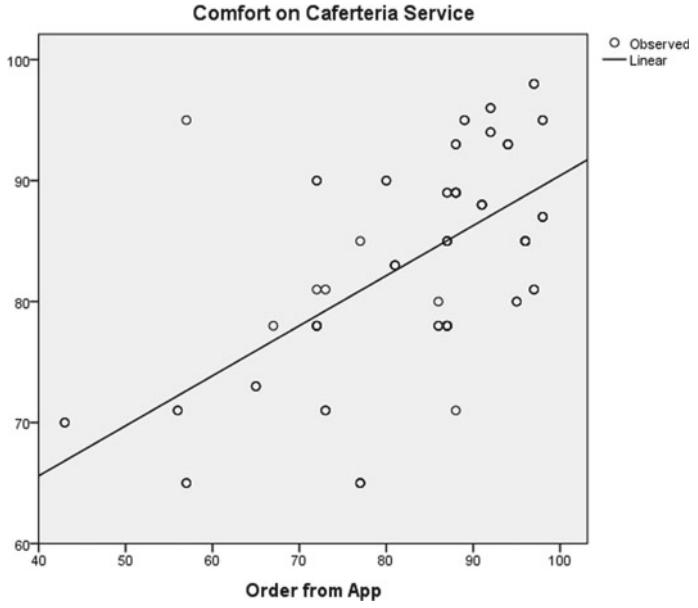


Fig. 2 Comparison of association between comforts on cloud cafeteria with order from app

for their food intake at their workplace, there was a good relationship observed for the comfort on using Cloud cafeteria service through food ordered from Mobile App. The mean values are distributed with the percentage of using mobile app with the percentage of comfort attained through Cloud cafeteria.

4 Conclusion

This research substantiates a positive role of ICT in corporate companies with the practice of Cloud cafeteria using mobile app. It is observed that the comfort from Cloud cafeteria is obtained through the usage of mobile app with a stronger relationship between these two variable through a coefficient $r = 0.952^{**}$ and the correlation is significant with the variables of Cloud cafeteria at 0.01 level. The linear regression results evidences the users have ease on cancelling their food orders. In addition to the accuracy of food received with order placed by mobile app in a contemporary scenario. Thus this outcome reveals a greater significance on practicing an android mobile phone, laptops and desktop to access Cloud cafeteria app at an international corporate company. In future, Cloud cafeteria will be a best source for providing food and safer environment at workplaces by reducing the gathering especially during pandemic situation.

References

1. Z. Cao, J. Lin, C. Wan, Y. Song, Y. Zhang, X. Wang, Optimal cloud computing resource allocation for demand side management in smart grid. IEEE Trans. Smart Grid **8**(4), 1943–1955 (2017)
2. S. Hussain, J.H. Bang, M. Han, M.I. Ahmed, M.B. Amin, S. Lee, C. Nugent, S. McClean, B. Scotney, G. Parr, Behavior life style analysis for mobile sensory data in cloud computing through map reduce. Sensors **14** (2014)
3. J. Lee, J. Jung, S. Yeoum, J. Bum, T.B. Dang, H. Choo, Cloud media DJ platform: functional perspective, in (eds) *Future Data and Security Engineering. FDSE 2018*, vol. 11251, eds. by T. Dang, J. Küng, R. Wagner, N. Thoai, M. Takizawa Lecture Notes in Computer Science (Springer, Cham, 2018)
4. A. Hameed, A. Khoshkbarforoushha, R. Ranjan et al., A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems. Computing **98**, 751–774 (2016)
5. C. Stergiou, et al., Secure integration of IoT and cloud computing, future generation computer systems, vol. 78, part 3, pp. 964–975 (2018)
6. M. Altamimi, K. Naik, The concept of a mobile cloud computing to reduce energy cost of smartphones and ICT systems, in *Information and Communication on Technology for the Fight against Global Warming*. ICT-GLOW 2011. Lecture Notes in Computer Science, vol. 6868, eds. by D. Kranzlmüller, A.M. Toja (Springer, Berlin, Heidelberg, 2011)
7. A.K. Pathan, M.M.Z.E. Mohammed, building customer trust in cloud computing with an ICT-enabled global regulatory body. Wireless Pers. Commun. **85**, 77–99 (2015)
8. I. Butun, M. Erol-Kantarci, B. Kantarci, H. Song, Cloud-centric multi-level authentication as a service for secure public safety device networks. IEEE Commun. Mag. **54**(4), 47–53 (2016)

9. Z. Siddiqui, A.H. Abdullah, M.K. Khan et al., Smart environment as a service: three factor cloud based user authentication for telecare medical information system. J Med Syst **38**, 9997 (2014)
10. N.K. Sehgal, P.C.P. Bhatt, J.M. Acken, Future trends in cloud computing, in *Cloud Computing with Security* (Springer, Cham, 2020)
11. E. Gelenbe et al., Security for smart mobile networks: The NEMESYS approach, in *2013 International Conference on Privacy and Security in Mobile Systems (PRISMS)* (Atlantic City, NJ, 2013), pp. 1–8

Influence of Probing Action Costs on Adversarial Decision-Making in a Deception Game



Harsh Katakwar, Palvi Aggarwal, Zahid Maqbool, and Varun Dutt

Abstract Deception, an act of misleading into false belief, has been proven to be an effective method to counter cyber-attacks. Although prior research in deception in cybersecurity has focused on the network size and the proportion of honeypots in games, there has been little research on the influence of probing action costs on adversarial decisions. In this research, using a deception game (DG), we investigate the impact of different cost functions in the probe stage on adversarial decisions. The DG involved a game DG (n, k, γ), where n was the number of webservers, k was the number of honeypot webservers in the network, and γ was the number of probes an adversary could make before choosing to attack the network. In an experiment, three between-subject conditions that differed in the cost of probing actions included: increasing-cost (40 participants), constant-cost (40 participants), and no-cost (40 participants). In increasing-cost, the cost for probing honeypots increased linearly over trials. However, in constant-cost, the cost for probing a honeypot webserver remained constant. In no-cost, probing a webserver did not cost the adversary. Results revealed that the probing cost did not influence the probe and attack actions and that there was a significant interaction between different cost conditions and the regular webserver probe actions over blocks. The main implication of the research is that the probing action costs may not influence adversarial decisions.

Keywords Honeypot · Cyber-attack · Behavioral cybersecurity · Deception · Probe · Attack · Adversary

1 Introduction

The increase in usage of the digital infrastructure has led to a rise in the rate of cyber-attacks. The growth of these threatening attacks has increased exponentially in the past decade [1, 2]. The major kinds of cyber-attacks in 2020 were ransomware

H. Katakwar (✉) · Z. Maqbool · V. Dutt
Applied Cognitive Science Laboratory, Indian Institute of Technology Mandi, Mandi, India

P. Aggarwal
Dynamic Decision-Making Laboratory, Carnegie Mellon University, Pittsburgh, USA

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_62

and social engineering, and these attacks were meant to steal data [3]. Although the current security solutions have provided relief from the cyber-attacks, these solutions may not work for the modern cyber-attacks. The increase in cyber-attacks and lack of security solutions has motivated the research community to develop security solutions to counter these modern cyber-attacks [4].

Some of the security solutions that have proved useful in defending against cyber-attacks are intrusion detection systems (IDSs) and the filtering strategy [5]. IDSs monitor the network traffic and send alerts to the defenders about the unusual behavior on the network. IDSs are robust, but they may possess some inaccuracies leading to false warnings [6, 7]. These false alarms may result in a loss of revenues. Another solution that has proven effective against cyber-attacks is the filtering strategy [5, 8]. The filtering strategy helps to screen out malicious activities and helps to ensure safe access. This strategy may make the non-rational network agents achieve consensus behavior [5].

In addition to the security solutions listed above, the deception technique has also proved successful in combating cyber-attacks. Deception, an act of making someone believe in incorrect information, may help provide real-time solutions to counter cyber threats. Deception has been utilized in computer networks with the help of honeypots, where honeypots are webservers that pretends to be real to detect, counter, and prevent cyber-attacks [9–11]. Deception via honeypots is a prevalent technique for finding, preventing, protecting, and combating cyber-attacks [11–14].

Researchers have studied deception in cybersecurity mathematically as well as through non-cooperative games [15–17]. But recently research community has given more focus on the human factors concerning adversarial decisions. For example, Aggarwal et al. [13] developed a cybersecurity tool, HackIT, where the tool could help understand human factors influencing adversarial decisions in cyber situations involving deception. Similarly, Katakwar et al. [18] investigated the effect of different network sizes on adversarial decisions in a deception-based game involving honeypot webservers.

Human factors in cybersecurity may be studied from cognitive theories like Instance-based Learning (IBL), which rely on recency and frequency of available information to derive its predictions [19, 20]. Researchers in the cybersecurity domain have shown that IBL theory has accounted for human decisions in situations where hackers and defenders play games against each other [21]. Thus, this theory may help derive expectations about the decisions of adversaries in scenarios involving cyber-attacks.

Although prior research has investigated several factors that influence adversary's decisions in cyber-attack situations [22–24], research has yet to investigate how different costs of probing actions influence the adversary's decision in cyber environments. Such probing actions may help adversaries collect information in the network before waging a cyber-attack. The repeated probes, along with the presence of deception, may make the adversary take uncertain decisions leading to the revealing of their identities. As a result, repeated probes could prove more costly to the adversary. So, the primary objective of this research is to understand how different cost for the probing actions influences the adversary's decision in deception game

involving honeypots. We develop a deception game with the different costs for the probing actions for investigating our hypotheses.

In what follows, first, a deception game is detailed. Second, an experiment is detailed where the cost of probes on a network in the deception game was varied. Lastly, results from the experiment are presented and discussed.

2 Deception Game

The deception game (DG) is a sequential, single-player, incomplete information web-based game, i.e., a game between adversary and the network [18]. The game is denoted as DG (n, k, γ), where n is the number of webservers in the network, k is the number of honeypot webservers in the network, and γ is the number of probes an adversary makes before making the final attack [17, 18]. There are two types of webservers in the network, regular webservers, and honeypots. Regular webservers are the real webservers; whereas, the honeypots are the fake webservers that pretend to be real. The game has two stages: probe and attack.

In the probe stage, an adversary can probe a certain number of webservers or decide not to probe the network. Probing a webserver in the DG means clicking on the button denoting a particular webserver in the user interface. On probing the webserver, the adversary gets a response from the system based on her actions. If deception is used in a particular round, then the adversary receives an incorrect response for her actions. However, if deception is absent, the adversary receives the true information from the network.

In the attack stage, the adversary can attack only one of the network's webservers or decide not to attack. Attacking a webserver means clicking the button denoting a particular webserver in the user interface. Based upon his actions, the adversary is awarded positive or negative points.

3 Influence of Different Probe Action Costs on Adversary's Decisions

There were three different cost conditions in the deception game. The following were the conditions of DG: increasing-cost probe, no-cost probe, and constant-cost probe. As per IBL theory, human decisions may be influenced by maximizing the positive outcomes and minimizing the negative outcomes. The outcomes are stored in the form of instances in the memory. These instances are retrieved based on the likelihood of their retrieval, which is a function of their activations. The activation of instances depends upon the recurrence and frequency of the outcomes. The instances retrieved are blended based on the likelihood of the retrieval and the outcomes accumulated in them. When the adversary probes/attacks the honeypot

webserver in a cost-associated condition (increasing-cost and constant-cost), the adversary experiences the negative outcomes that would minimize the blended value of honeypot probe decision/honeypot attack decision. However, for the no-cost condition, probing/attacking the network may not cause the adversary to experience negative outcomes. Thus, based upon the positive payoffs for regular webserver attacks and maximization of these positive payoffs, we expect the regular probe actions to be influenced by different cost conditions. In addition, as adversaries would learn about honeypots with negative payoffs over rounds and participants would tend to minimize negative payoffs, we expect a decrease in the proportion of regular webserver probes across all conditions. As the attack phase followed the probe phase and the cost was associated with probing, we do not expect any differences in the proportion of actions during the attack phase across different cost conditions.

4 Methods

4.1 Experiment Design

Participants performing the role of "adversary" were randomly assigned one of the three between-subject conditions: no-cost probe (40 participants), constant-cost probe (40 participants), and increasing-cost probe (40 participants). Each of these conditions had the same number of webservers, and the proportion of honeypot webservers in the network was constant across all the conditions (50%). These conditions differed by the cost for their action against the honeypot webserver in the probe stage. Each condition had four webservers. Out of the four webservers, 2 of them were honeypot webservers, while the other 2 were regular webservers. In no-cost condition, the adversary had no cost for their probe actions on honeypot webservers in the probe stage of DG. In constant-cost conditions, the honeypot webserver probe cost remained constant with the repeated probe attempts on honeypots in a particular round. In increasing-cost conditions, the honeypot webserver probe's cost increased linearly with the repeated probe attempts in a particular round. Across all the conditions, each of the rounds had a probe stage followed by the attack stage. Each of the three conditions had 29 trials, out of which 14 of them were randomly assigned as deception rounds, while the rest of the rounds had no deception. The participants were informed about the presence of deception in a DG, but they did not know which round belonged to the deception/non-deception condition. In the attack stage, the adversary decided to attack one of the webservers in the network or did not attack the network. In each condition, six dependent proportions were used: three actions of the probe stage (regular webserver probe, honeypot webserver probe, and no webserver probe) and three actions of the attack stage (regular web server attack, honeypot webserver attack, and no webserver attack). The probe decisions and the attack decisions over the 29 rounds were clubbed into blocks of 5 rounds each. Thus, 29 rounds translated to 6 blocks.

4.2 Stimuli

Figure 1a shows the interface presented to participants in the probe stage of DG in the increasing-cost condition of DG. A similar interface was shown in all the conditions of DG. Participants were informed about their objective in the form of brief instructions. In the probe stage, participants could probe the webservers by clicking the buttons depicting the webserver number. Based on her actions, the adversary got to the response from the system (see Fig. 1b). Adversaries may probe the network multiple times before the attack stage. Adversaries also had the option to click on "Do not probe the Network" and proceed to the attack stage. In the attack stage, adversaries had the option to attack one of the webservers by clicking the button

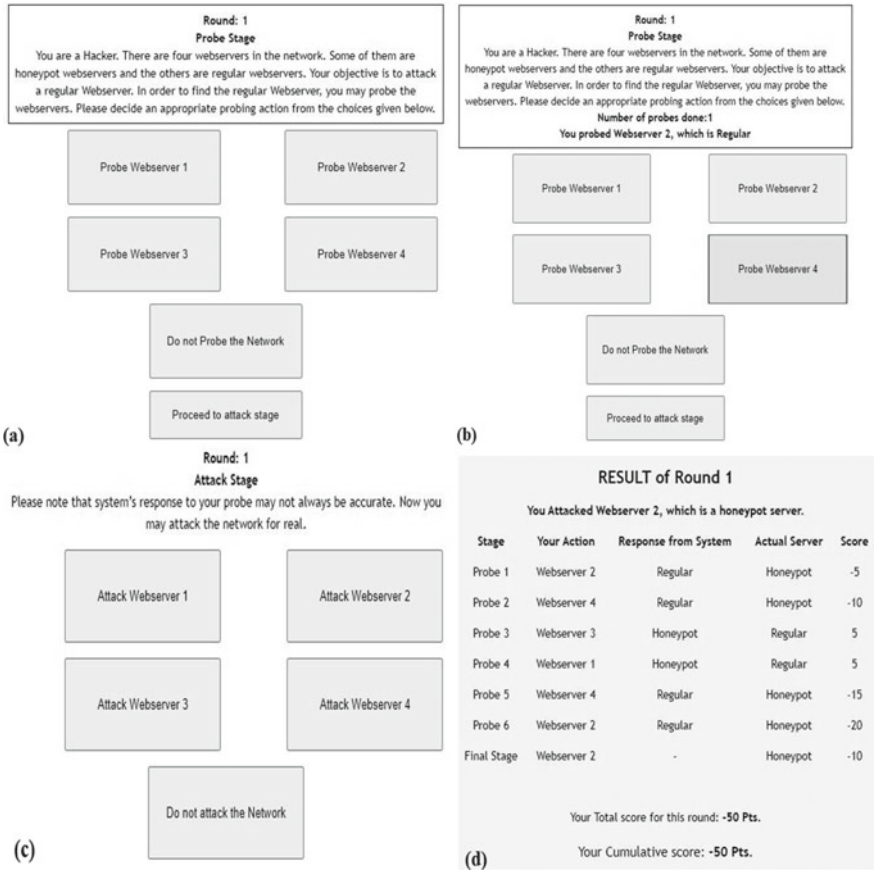


Fig. 1 **a** Probe stage of DG in increasing-cost condition. **b** Response received from the system in the probe stage of DG. **c** The attack stage in DG. **d** Complete result of the round in the increasing-cost condition at the end of a round in DG

depicting the webserver (see Fig. 1c). After the attack stage, the adversaries learned about their payoffs based on their actions in probe and attack stages (see Fig. 1d).

4.3 Participants

The study was conducted after approval from the ethics committee of the Indian Institute of Technology Mandi. Participation was voluntary, and all participants signed a consent form before starting the study. Participants were anonymously recruited via Amazon Mechanical Turk, a crowdsourcing website [25]. Sixty-six percent of participants were male, while the rest thirty-four percent were female. Ninety-four percent of participants possessed a college degree, while the remaining six percent were still pursuing a college degree. Seventy-four percent of participants majored in science, technology, engineering, and mathematics, while the rest belonged to humanities and social sciences. Participants were paid INR 50 (USD 0.72) for their participation in the study.

5 Results

5.1 Influence of Different Probe Costs on Adversarial Decisions During Probe and Attack Stages

First, one-way ANOVAs were performed to investigate the influence of the different probe costs on adversaries' decisions during the probe stage. The proportion of different probe decisions was found to be insignificant across different cost conditions. The proportion of regular webserver probe decisions in increasing-cost condition, no-cost condition, and constant-cost condition were 0.44, 0.47, and 0.45, respectively (F (2, 117) = 0.919, p = 0.402, η^2 = 0.015). The proportion of honeypot webservers probe decisions in increasing-cost condition, no-cost condition, and constant-cost condition were 0.43, 0.47, and 0.43, respectively (F (2, 117) = 1.454, p = 0.238, η^2 = 0.020). The proportion of no webserver probe decisions in increasing-cost condition, no-cost condition, and constant-cost condition were 0.13, 0.06, and 0.12, respectively (F (2, 117) = 1.359, p = 0.261, η^2 = 0.024). These results were as per our expectations.

Similarly, for the attack stage, one-way ANOVAs were performed to investigate the influence of the different probe action costs on adversaries' decisions during the attack stage. The proportion of different attack decisions was found to be insignificant across different cost conditions. The proportion of regular webserver attack decisions in increasing-cost condition, no-cost condition, and constant-cost condition were 0.42, 0.45, and 0.42, respectively (F (2, 117) = 0.606, p = 0.547, η^2 = 0.010). The

proportion of honeypot webserver attack decisions in increasing-cost condition, no-cost condition, and constant-cost condition were 0.40, 0.44, and 0.43, respectively (F (2, 117) = 1.454, $p = 0.238$, $\eta^2 = 0.024$). The proportion of no webserver attack decisions in increasing-cost condition, no-cost condition, and constant-cost condition were 0.18, 0.11, and 0.14, respectively (F (2, 117) = 1.359, $p = 0.261$, $\eta^2 = 0.023$). Again, these results are as per our expectations.

5.2 *Influence of Different Cost Conditions Over the Trials on Adversarial Decisions During Probe Stage*

Mixed-factorial ANOVAs were performed with probe decisions over blocks as a within-subject factor and different cost conditions as a between-subject factor.

Figure 2 shows the proportion of regular probes over blocks in different cost conditions. As shown in Fig. 2, we found that there was a significant interaction between different cost conditions and blocks (F (10, 585) = 2.052, $p < 0.05$, $\eta^2 = 0.034$). Also, averaged over all conditions, the proportions of regular probe decisions over the blocks were significant and decreasing (F (5, 585) = 2.529, $p < 0.05$, $\eta^2 = 0.021$). These results are as per our expectations.

However, the proportion of honeypot webserver probes over blocks were not significant (F (5, 585) = 1.662, $p = 0.142$, $\eta^2 = 0.014$). Also, the interaction between honeypot webserver probes and different cost conditions was not significant (F (10, 585) = 1.667, $p = 0.085$, $\eta^2 = 0.028$). Similarly, the proportion of no webserver probe decisions over blocks were not significant (F (5, 585) = 1.348, $p = 0.243$, $\eta^2 = 0.011$). Also, the interaction between different cost conditions and the no webserver probe decisions were not significant (F (10, 585) = 1.171, $p = 0.307$, $\eta^2 = 0.020$). Again, these results meet our expectations.

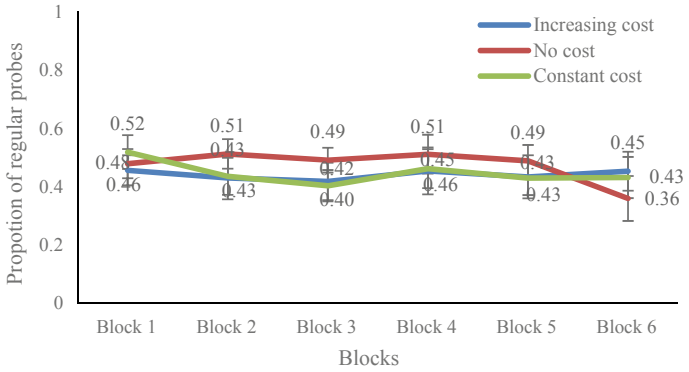


Fig. 2 The proportion of regular probe actions over the rounds across different cost conditions. The error bars denote a 95% confidence interval

5.3 *Influence of Different Cost Conditions Over the Trials on Adversarial Decisions During Attack Stage*

In the attack stage, we had three different dependent variables regular webserver attack, honeypot webserver attack, and not attack decisions. We performed mixed-factorial ANOVAs with attack decisions over blocks as a within-subject factor and different cost conditions as a between-subject factor. There was no significant interaction between different cost conditions and the following proportions of attack decisions over blocks: regular webserver attack (F (10, 585) = 0.579, $p = 0.832$, $\eta^2 = 0.010$), honeypot webserver attack (F (10, 585) = 0.664, $p = 0.758$, $\eta^2 = 0.011$) and no webserver attack (F (10, 585) = 1.422, $p = 0.166$, $\eta^2 = 0.024$). Also, the proportion of decisions over blocks was not significant for these decisions: regular webserver attack (F (5, 585) = 0.111, $p = 0.990$, $\eta^2 = 0.001$), honeypot webserver attack (F (5, 585) = 0.936, $p = 0.457$, $\eta^2 = 0.008$), and no webserver attack (F (5, 585) = 1.854, $p = 0.100$, $\eta^2 = 0.016$). Overall, these results meet our expectations.

6 Discussion

Deception via honeypot has been proven to be a key technique to counter modern cyber-attacks [10]. Recently, researchers have studied the various human factors involved that effects the adversary's decision in deception-based games [26, 27]. In this paper, we investigated the influence of different costs of probe actions on adversarial decisions in DG. Results revealed that different costs of probing actions did not influence the adversarial decisions making during the attack phase in DG. However, there was a significant interaction between regular probe decisions over blocks in DG. The results also revealed that in constant-cost and increasing-cost conditions, the proportion of regular probe decisions had a similar constant pattern over rounds. Also, the proportion of regular probe decisions decreased over blocks.

The results derived from our study can be explained with the help of cognitive theories like IBL. As per IBL theory, humans choose those alternatives that maximize their blended values. When there is a cost associated with the honeypot probe, the adversary encounters negative outcomes. This negative experience lowers the blended value of the honeypot probe/attack decision. Whereas in the no-cost probe, the adversary does not suffer negative outcomes on probing/attacking the webserver. Thus, we see a decline in the regular probe decisions over blocks. Second, there was an overall decrease in the regular probe actions over blocks. This result can again be explained based upon IBL theory. As adversaries would learn about honeypots with negative payoffs over rounds and participants would tend to minimize negative payoffs, there was a decrease in the proportion of regular webserver probes across all conditions. Third, there was no influence of different cost conditions on the adversarial decision-making during the attack phase. As the attack phase followed

the probe phase and the cost was associated with probing. Thus, the proportion of actions during the attack phase across different cost conditions was similar.

One limitation of this research is that the results are derived from a lab-based study. Thus, the conditions in the real world may vary from those present in the lab-based study. Also, in this study, the adversaries did not possess the knowledge of deception rounds and the real identity of webservers, which might influence the adversary's decisions in the probe and attack stages.

Overall, we tried to replicate the real-world variables of cyber-attacks in DG, where the adversary first searched about the state of the webservers and, after that, made a final choice to attack the network. Therefore, some of the conclusions from our experiment may be valid for the real world. One implication of this work is that making probes on the network costly to adversaries may not influence their attack decisions. However, the cost of probing webservers does counterintuitively influence the proportion of probes on regular webservers: They keep the proportion of probes on regular webservers about constant over blocks. Thus, enterprises planning to make probing costly make also reconsider this strategy. In addition, the tool developed in the experiment may help in determining the minimum number of honeypots required for the network to capture the adversarial behavior on scaling based on the number of webservers in the network. Specifically, the tool could aid in lowering the total costs of deploying honeypots in the network.

Overall, we plan to investigate several other non-linear cost functions during probing to build upon the reported results as part of our future research.

Acknowledgements This work was supported by the Department of Science and Technology (DST), Government of India, under the grant to Dr. Varun Dutt and Dr. V. S. Chandrasekhar Pammi (IITM/DST-ICPS/VD/251). Besides, we are grateful to the Indian Institute of Technology Mandi for providing the required resource for this project.

References

1. Business Insider: Hackers have become so sophisticated that nearly 4 billion records have been stolen from people in the last decade alone. Here are the 10 biggest data breaches of the 2010s, Retrieved from: https://www.businessinsider.in/slideshows/miscellaneous/hackers-have-become-so-sophisticated-that-nearly-4-billion-records-have-been-stolen-from-people-in-the-last-decade-alone-here-are-the-10-biggest-data-breaches-of-the-2010s-/slidelist/71652791.cms#slideid=71652805. Last Accessed 5 Mar 2021
2. Quick Heal Blog: Biggest cyberattacks of 2020. Retrieved from: https://blogs.quickheal.com/biggest-cyberattacks-2020so-far/. Last Accessed 5 Apr 2021
3. Trustwave Global Security Report. Retrieved from: https://trustwave.azureedge.net/media/16791/2020-trustwave-global-security-report.pdf?rnd=132339614670000000. Last Accessed 5 Apr 2021
4. E. Sayegh, More cloud, more hacks: 2020 cyber threats, *Forbes* (2021). Retrieved from: https://www.forbes.com/sites/emilsayegh/2020/02/12/more-cloud-more-hacks-pt-2/?sh=4c261d1269b3. Last Accessed 5 Apr 2021
5. Y. Shang, Hybrid consensus for averager–copier–voter networks with non-rational agents. Chaos, Solitons Fractals **110**, 244–251 (2018)

6. P. Mell, R. Lippmann, C. Hu, J. Haines, M. Zissman, An overview of issues in testing intrusion detection systems, *NIST*. Retrieved from: https://www.nist.gov/publications/overview-issues-testing-intrusion-detection-systems. Last Accessed 5 Apr 2021 (2021)
7. Y. Shang, False positive and false negative effects on network attacks. J. Stat. Phys. **170**(1), 141–164 (2017)
8. Y. Shang, Consensus of hybrid multi-agent systems with malicious nodes. IEEE Trans. Circuits Syst. II Express Briefs **67**(4), 685–689 (2020)
9. M. Almeshekah, E. Spafford, Cyber security deception, in *Cyber Deception*, (2016), pp. 25–52
10. N.C. Rowe, E.J. Custy, Deception in cyber-attacks. Cyber warfare and cyber terrorism: IGI Global, pp. 91–96 (2007)
11. P. Aggarwal, C. Gonzalez, V. Dutt, Looking from the hacker's perspective: Role of deceptive strategies in cyber security, *in 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, (London, UK, 2016), pp. 1–6
12. P. Aggarwal, C. Gonzalez, V. Dutt, Cyber-security: Role of deception in cyber-attack detection. Adv. Hum. Factors Cybersecur. 85–96 (2016)
13. P. Aggarwal, C. Gonzalez, V. Dutt, HackIt: A real-time simulation tool for studying real-World cyberattacks in the laboratory. in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, ed. by B. B. Gupta, G. M. Perez, D. P. Agrawal, and D. Gupta (Cham, Springer, 2020) International Publishing, pp. 949–959
14. K. Heckman, M. Walsh, F. Stech, T. O'Boyle, S. DiCato, Active cyber defense with denial and deception: A cyber-wargame experiment. Comput. Secur. **37**, 72–77 (2013). https://doi.org/10.1016/j.cose.2013.03.015
15. C. Kiekintveld, V. Lisý, R. Píbil, *Game-Theoretic Foundations for the Strategic Use of Honeypots in Network Security* (Cyber warfare, Springer, 2015), pp. 81–101
16. N. Garg, D. Grosu, Deception in honeynets: A game-theoretic analysis, in *2007 IEEE SMC Information Assurance and Security Workshop* (IEEE, 2007), pp. 107–113
17. T.E. Carroll, D. Grosu, A game theoretic investigation of deception in network security. Secur. Commun. Netw. **4**(10), 1162–1172 (2011)
18. H. Katakwar, P. Aggarwal, Z. Maqbool, V. Dutt, Influence of network size on adversarial decisions in a deception game involving honeypots. Front. Psychol. **11**(2385) (2020). https://doi.org/10.3389/fpsyg.2020.535803
19. C. Gonzalez, V. Dutt, Instance-based learning: Integrating sampling and repeated decisions from experience. Psychol. Rev. **118**(4), 523 (2011)
20. C. Gonzalez, J.F. Lerch, C. Lebiere, Instance-based learning in dynamic decision making. Cogn. Sci. **27**(4), 591–635 (2003)
21. P. Aggarwal, C. Gonzalez, V. Dutt, Modeling the effects of amount and timing of deception in simulated network scenarios, in *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 19–20 June 2017, pp. 1–7. https://doi.org/10.1109/CyberSA.2017.8073405
22. P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, E. Vázquez, Anomaly-based network intrusion detection: Techniques, systems and challenges. Comput. Secur. **28**(1–2), 18–28 (2009)
23. L. Wang, S. Jajodia, A. Singhal, S. Noel, K-zero day safety: Measuring the security risk of networks against unknown attacks, in *European Symposium on Research in Computer Security, 2010* (Springer, 2010), pp. 573–587
24. A. Lenin, J. Willemson, D.P. Sari, Attacker profiling in quantitative security assessment based on attack trees, in *Nordic Conference on Secure IT Systems* (Springer, Cham, 2014), pp. 199–212
25. W. Mason, S. Suri, Conducting behavioral research on amazon's mechanical turk. Behav. Res. Methods **44**(1), 1–23 (2012)
26. P. Aggarwal, A. Gautam, V. Agarwal, C. Gonzalez, V. Dutt, Hackit: a human-in-the-loop simulation tool for realistic cyber deception experiments, in *International Conference on Applied Human Factors and Ergonomics, 2019* (Springer, 2019), pp. 109–121
27. V. Dutt, Y.S. Ahn, C. Gonzalez, Cyber situation awareness: modeling detection of cyber attacks with instance-based learning theory. Hum. Factors **55**(3), 605–618 (2013)

Impact of Digital Wellbeing in Intelligent Knowledge Management Systems



Sapna Jain and M. Afshar Alam

Abstract Digital wellbeing is frequently defined in terms of the skills that people require to prosperously make use of digital technologies. Social, personal, and professional life is affected by the way people handle digital life which affects the overall development of an individual. The paper discusses and analyzes how digital wellbeing apps are useful for people in various scenarios and performed a survey on youths to identify what effect does it have on youngsters. The paper explains the role of digital wellbeing in different fields such as education system, health care, and agriculture which are the pillars of society.

Keywords Digital wellbeing · Healthcare · Education system · Agricultural sector · Challenges · Information systems

1 Introduction

Digital wellbeing is frequently defined in terms of the skills that people require to prosperously make use of digital technologies. The appearance of digital professionals in designing online environments which affect their social responsibility in encouraging or discouraging practices of wellbeing [1]. The word "Digital" is used in our lives today and people of every age group are spending more time with digital devices in daily life. This technological impact has many positive effects such as learning new knowledge and connecting with others from all over the world through using many apps. These days it is becoming necessary for the young generation to gain healthy habits and understand how to use digital devices so that they fully develop their physical and social wellbeing [2].

S. Jain (✉) · M. A. Alam
Jamia Hamdard, New Delhi, India
e-mail: drsapnajain@jamiahamdard.ac.in

M. A. Alam
e-mail: aalam@jamiahamdard.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_63

2 Literature Review

Ms. Shika Dua et al. proposed a solution to overcome the issues and challenges of traditional education in the era of digital technologies. They have also deliberated about the imminent trends in the digital education system that will create a fantasized digital environment for the upcoming future generation. Discussed factors for digital learning including primary factors and secondary factors. Primary factors consist of students, faculty, institutions, and technology whereas secondary factors include course, cost, society, and support [3, 4]. Authors analyzed that what are the problems faced by digital wellbeing at the time of digital learning. G.N. Wikramanayake et al. examined how digital technologies influence individuals within the field of education. The author explained the process of generation, creation, and acquisition of knowledge via technology and such activities could be performed by tools like relational database management system (RDBMS) and electronic document management system (EDMS). RDBMS is a tool used for managing information in a system, manage primitive data like numbers and dates, and manages organizational data of the education system. EDMS applications emphasized on control of electronic documents EDMS enables the process of managing documents effectively [5]. Regarding the education system, the work is accomplished through an enhanced and more effective way known as e-learning. Also, describe how technology is used to access and apply such knowledge. Discussed how effects of technology, in general, with the help of some examples. Sarah Diefenbach et al. researcher mentioned the opportunities and challenges in the period of digital technology design from a knowledgebase perspective with theoretical and practical contributions [6].

3 Role of Digital Wellbeing in the Field of Intelligent Education Systems

Digital wellbeing plays a significant role in the field of education. Typically, education is self-contained on many sources like school, colleges, teachers, and print media. The learners can access the information sources by matriculating themselves in school and colleges [7]. Before the digital period, delivery of information among people was not possible and even those accessed were unable to perceive current information regarding the context. Everyone wants to know about the situation as it happens and when it happens and nowadays the world leads our mindset to a knowledgeable world via digital wellbeing [8]. Thus, education becomes the highest priority. Digital technologies provide many opportunities for learning and become an integral part of our life. Young people, being digital native, can become their educators. And it was seen that youth knows more about technical things and are quite familiar with it than their family members or elders, teaching them how to access digital devices including tablets, I-pad, PowerPoint, Word, etc. or how to send text and capture pictures [9].

3.1 Challenges Faced by Intelligent Education Systems

From the perspective of digital wellbeing, there are numerous challenges that befall different stakeholders within the context of education. Every improvement has two sides, leading to the development and others are related to some challenges with some the enhancement of this development. Another challenge faced by digital wellbeing in the field of education is unaccustomed of employees towards technology; managers must need to handle this [10]. Usually, people oppose changes even if the changes make the current situation superior to the earlier situation. They cannot believe that a technology-based learning program as a conversation with an instructor would be helpful [11].

Characteristics of multimedia allow making the material high fascinating and easier to allude [12]. This privilege the accomplishment of learning within a less amount of time. Among students, effective communication gives deep knowledge and enables them to accept learning via digital devices. The next challenge is how we can keep our students motivated for a long time to complete the course. This is a common challenge that employees did not work properly; they may not explore the material [13]. The puissance of learners to pierce and interact with the course material dictates the utility they will get out of the program. To overcome this resistance some measures can be taken. Another challenge of digital learning is identifying the course whether the course intention is being affected or not. It is important to know how many employees using digital learning programs, how much time they spend on it, but above that, it is more important to know that performance acquires new knowledge. If they display the skills and information gleaned from digital learning programs in their work, then the digital learning program in their work, then the digital learning implementation has been effective [14].

4 Role of Digital Wellbeing in the Intelligent Healthcare Systems

In the healthcare industry, digital opportunities are a positive aspect of a healthcare system that influences eulogistic impacts on others. Blockchain health records, artificial intelligence (AI), and telemedicine which allow medical devices are examples of digital transformation in the healthcare sector [15]. Lamentably, the healthcare and pharmaceutical industry retreat in the back at the time of implementing digital strategies. From a recent study, it is analyzed that only seven percent of peers said they had gone digital as compared to the other fifteen company industries [16]. Every individual has grateful for this opportunity or transformation of technology, due to these opportunities such as virtual reality tools, wearable devices, telehealth, and 5G technologies. Facilities are provided to the people as soon as possible and also who need it in the very shortest time, this saves a lot of time. The burden of lifestyle-related illness devours almost 70% of healthcare budgets in western economies, and

the accurate value of these budgets is set to rise rapidly because of the aging population in many of these countries. With healthcare budgets at breaking point already, clearly, there is a requirement for another way. The promise of Digital Health to alter higher self-care and stop or table the event of significant malady appears to supply the way out of a tough state of affairs. Big data analysis helps us to identify these people and implement deterrent plans to keep them from returning. Big data's predictive analysis could help hospitals, as well as clinics, also compute future admission rates, which helps these facilities allocate the proper staff to deal with patients. It saves a lot of money and when a facility is understaffed then it decreases emergency room wait times [17, 18]. Development of wearable medical devices within the time of digital healthcare is doctors can easily gather their patient information or their health-related information from medical devices such as wearable devices. Nowadays in the digital era, patients and doctors both are emphasized on maintenance and prevention and demanding about their reports. Artificial intelligence (AI) is quite simply a digital transformation trend in healthcare. Artificial intelligence (AI) shows the abstract of medical innovation and industry players are eager to invest millions in it. The healthcare AI-powered tools market is anticipated to exceed $34 billion by 2025, which implies this technology will shape almost all aspects of the industry. Virtual health assistants and chatbots are examples of AI-based technology that patients are becoming sociable with.

4.1 Challenges in the Field of Intelligent Healthcare Systems

The digital transformation of the healthcare industry can radically ameliorate the ability of doctors, hospitals, and organizations to treat patients and help them live longer healthier lives. In the healthcare industry, processing and analysis of data have become one of the major challenges. Part of the problem is because of the sheer amount of information that hospitals, clinics, and health professionals collect. Without robust AI systems that can investigate information or data, it is difficult for organizations to provide better and more personalized care to patients [19]. Another challenge is that the process of collecting and synchronizing data. Organizations should be very attentive about cyber threats, which can be very expensive. As an example, a study by IBM displayed that healthcare organizations had the very best costs related to data breaches, which were thrice higher as compared to other industries. In the healthcare industry, this is very necessary since many products will be used by both patients and medical professionals. a comfortless or poorly designed IoMT device, for example, can smudge a patient's experience. Besides, if the flexibility and usability become difficult then it will also limit the overall willingness of medical professionals to use or prescribe the device to other patients [20, 21].

5 Role of Digital Wellbeing in the Field of Intelligent Agriculture Systems

Digital wellbeing in agriculture used communal media podium related to digital technology to enhance human wellbeing. The interested farmers work and distribute videos describing the perfect management training that workers can use for enhanced productivity. Mobile cash is a different interference under digital wellbeing that changes paper money. Mobile cash is secure and takes less time to transfer and also helps for human wellbeing. Digital wellbeing has become a game changer for the agriculture sector, many mobile apps have become a field that makes agriculture sector simple. Some apps give information to farmers on present weather for days to come, agriculture helper advice in a time of growing, and to be used fertilizers. Large trading companies, leading information technology sectors, and organizations have also involved in agriculture sector and the environment for technology improves and wellbeing of farmers. E-Choupal of Indian Tobacco Companies a digital platform that gives service to the farmers of over 3500 villages and farmers have the capacity to manage food grain department and changes [22]. Trringa,a mobile app for farmers to rent motors using digital devices to help workers using the machine and it is helpful for farmer wellbeing. Concept of Custom brings in the agriculture launched over this app and all these apps are very helpful for poor farmers and workers who have only paid their rent and have not to spent large money for buying other farm machinery. Tax Collected at Source, India's top Information Technology firm, offering visual and audio developers to farmers using smartphones through its mKRISHI services. Stellapps app uses to enhance milk production. Ekgaon Technologies village for network, offering services to farmers, and women using mobile transmission to enhance the sustainable improvement of small farmers. Digital wellbeing is very helpful for those farmers, who are not able to do farming because of some reason.

5.1 Challenges Faced by Digital Wellbeing in the Field of Intelligent Agriculture Systems

Digital agriculture uses software and hardware systems that understand their atmosphere through best devices, provide the multifunction and take the move that decreases the chances of gaining a distinct goal. There are challenges that digital wellbeing facing for agricultural digitization. In technology, adding new features is easy, but the time and money it takes are very tough, but rather than focusing on the amount that this technology is proposed to increase the feature, focuses on wellbeing also. Another challenge faced by digital wellbeing is import of information that is provided the concept, it is all about place the structural hardware and software device in the right way [23]. For developing agriculture sector need of food scientists are very important so that it is helpful for farmers and their wellbeing, need of business development, and organizations. Typically, involvement of different backgrounds is

important for understanding many problems. All the stages of the project digital device mainly takes high cost. But farmers are not able to buy and pay the bills of costly technology. This is the biggest challenge for the digital wellbeing in agricultural sector. Many digital agriculture organizations are enhancing technology for helping farmers and their wellbeing, but it is also a big challenge for digital wellbeing and agriculture sector for improving productivity [24, 25].

6 Impact Analysis

From research, we have analyzed how digital technologies influence digital wellbeing or in the healthcare sector. Typically, there are so many technologies that impact a patient's health in both aspects that are positive and negative. Concerning the performance of digital technologies in the healthcare sector, these technologies perform very well from the perspective of an advantage as shown in Fig. 1. In the education sector, we have examined that nowadays technologies have a great impact on students but the effect of technology becomes vary on different ages such as teenagers or youths are more influenced by technology as in Fig. 2. Due to the increment of technology, many things become possible which was not possible in previous eras, and technology makes our life too easy. Technology is a source through which a student can get more knowledge, experience, and skills also. But besides that, technology resembles bad behavior towards student health in the education sector. The above graph indicates that almost 95% students use social media including LinkedIn, Twitter, Instagram, etc. which is a part of technology. Hence, it impacts the students of age group between18 and 19 mainly. Apart from that person whose ages are between 20 and 24 are also impacted by digital technologies in their academic period. But it was seen that people whose age is more than 30 are also affected by technology. But

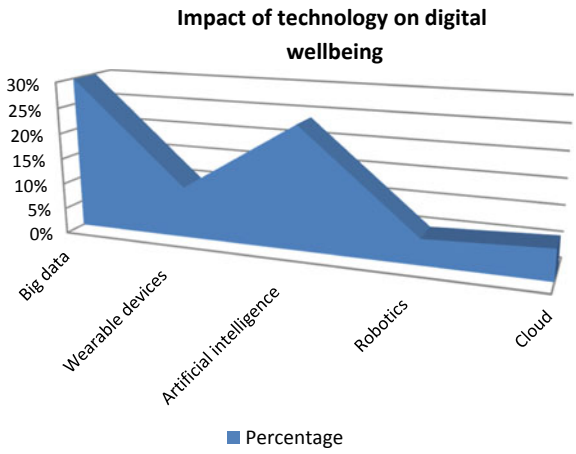


Fig. 1 Health sector analysis

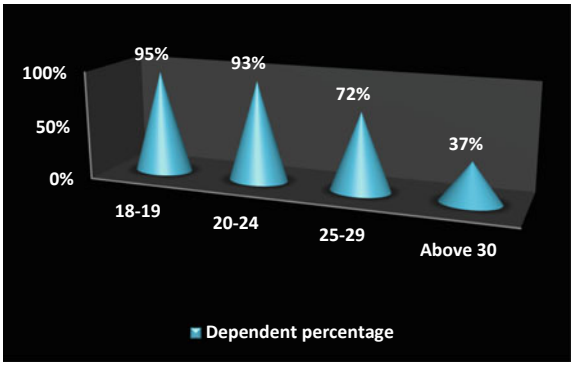


Fig. 2 Education sector analysis

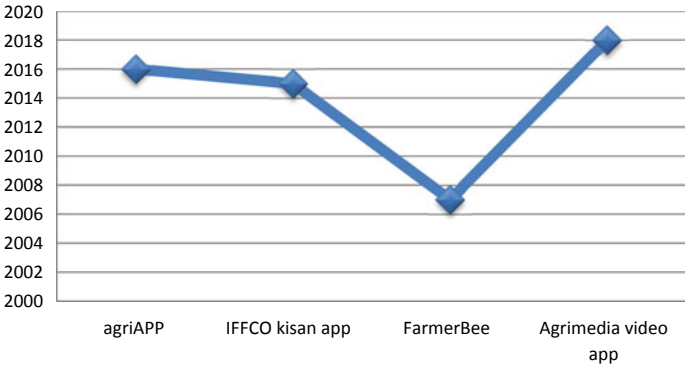


Fig. 3 Agriculture sector analysis

it was seen that people whose age is more than 30 are also affected by technology. In today's period, technology is progressing not only in the field of education or health but also in other areas also like agriculture. Many of the farmer's work was done which used to take a lot of time and resources were more but technology has solved it for a long time. There are many digital apps, due to which the problems of farmers have improved. If we have seen from the aspect of influence, it would have a good effect on farmers as in Fig. 3.

7 Conclusion

Digital Wellbeing play a crucial role in the education system, in the healthcare system, and the agricultural sector [26]. Although positive and negative effects of digital wellbeing on human health indicate that how to use technology in the right way

and what people to avoid for healthy health [27]. Inequalities digital conversion decreases more heavily on people with decreased levels of the education system and skills, and its privileges may be for the advantage of a few. Digital wellbeing is more important for future development of human wellbeing, especially in the education system, health care system, and agricultural sector [28, 29].

References

1. A.A. Lijadi, Theoretical foundations to outline human well-being: Meta analytic literature review for defining empowered life years. (Feb 2018)
2. A. Gaggioli, Digital wellbeing : Considering self-transcendence digital wellbeing : Considering. pp. 0–4 (May 2019)
3. A.M. Ronchi, A.M. Ronchi, Well-being in the digital age, in *e-Citizens*. pp. 23–41 (March 2019) https://doi.org/10.1007/978-3-030-00746-1_3
4. A. Maccagnan, S. Wren-Lewis, H. Brown, T. Taylor, Wellbeing and society: Towards quantification of the co-benefits of wellbeing. Soc. Indic. Res. **141**(1), 217–243 (2019). https://doi.org/10.1007/s11205-017-1826-7
5. C. Burr, J. Morley, M. Taddeo, L. Floridi, Digital psychiatry: Ethical risks and opportunities for public health and well-being. SSRN Electron. J. **1**(1), 21–33 (2019). https://doi.org/10.2139/ssrn.3477978
6. C. Burr, M. Taddeo, L. Floridi, The ethics of digital well-being: A thematic review. SSRN Electron. J. (2019). https://doi.org/10.2139/ssrn.3338441
7. C. Burr, M. Taddeo, L. Floridi, *The Ethics of Digital Well-Being: A Thematic Review*, no. 0123456789 (Springer, Netherlands, 2020)
8. C.D. Ryff, Psychological well-being revisited: Advances in the science and practice of eudaimonia. Psychother. Psychosom. **83**(1), 10–28 (2013). https://doi.org/10.1159/000353263
9. C.M. Pulido, L.C. Mara, V. Ionescu, T. Sordé-Martí, Social impact of psychological research on well-being shared in social media. Front. Psychol. **11**(February), 1–12 (2020). https://doi.org/10.3389/fpsyg.2020.00135
10. D. Gasper, *Discussion Paper No . 2004/06 Human Well-being : Concepts and Conceptualizations*. (May 2004)
11. D. Teghe, K. Rendell, Social wellbeing: a literature review. Sch. Soc. Work Welf. Stud. **10**(August), 2005 (2005). https://doi.org/10.13140/RG.2.2.28891.26406
12. E.C.W. Ng, A.T. Fisher, Understanding well-being in multi-levels: A review. Heal. Cult. Soc. **5**(1), 308–323 (2013). https://doi.org/10.5195/hcs.2013.142
13. E. Diener, S. Oishi, L. Tay, Advances in subjective well-being research. Nat. Hum. Behav. **2**(4), 253–260 (2018). https://doi.org/10.1038/s41562-018-0307-6
14. F. Burchi, C. Gnesi, A review of the literature on well-being in Italy: A human development perspective. Forum Soc. Econ. **45**(2–3), 170–190 (2016). https://doi.org/10.1080/07360932.2014.995197
15. H. Moilanen, S. Äyrämö, S. Jauhiainen, M. Kankaanranta, C.C. Chiou, Collecting and using students' digital well-being data in multidisciplinary teaching. Educ. Res. Int. **2018** (2018). https://doi.org/10.1155/2018/3012079
16. J. Mcalaney, M. Aldhayan, B. Almourad, S. Cham, Predictors of acceptance and rejection of online peer support groups as a digital wellbeing tool predictors of acceptance and rejection of online peer support groups as a digital wellbeing tool digital media including social networks, gaming and online s. (Jan 2020)
17. https://www.frontiersin.org/articles/https://doi.org/10.3389/fpsyg.2018.00331/full
18. https://medicaltechnology.nridigital.com/medical_technology_mar19/connected_medical_devices_what_challenges_as_digital_healthcare_is_normalised

19. https://seismic.com/company/blog/5-challenges-of-digital-transformation-in-healthcare/
20. https://www.aconnect.com/knowledge/opportunities-and-challenges-in-digital-health-2017/
21. https://www.healthcareguy.com/2014/10/26/health-it-and-digital-health-job-opportunities-qualifications-and-certification-benefits/
22. M. Gui, M. Fasoli, R. Carradore, Digital well-being. Developing a new theoretical tool for media literacy research. Ital. J. Sociol. Educ. **9**(1), 155–173 (2017)
23. N.M. Trendov, S. Varas, M. Zeng, Digital technologies in agriculture and rural areas. Brief. Pap. FAO 26 (2019)
24. N.N. Surtaeva, Social well-being research problems in modern world. pp. 393–399, (Dec 2017). https://doi.org/10.15405/epsbs.2017.07.02.50
25. P. Anand, 2016 UNDP human development report: Happiness, well-being and human development: The case for subjective measures (Background Paper) (2016)
26. P. Howard-Jones, The impact of digital technologies on human wellbeing, in *Atlantic* (2011), pp. 98
27. S. Grand-Clement, A. Devaux, J. Belanger, C. Manville, Digital learning: Education and skills in the digital age. Digit. Learn. Educ. Ski. Digit. Age (2017)
28. U.H. Ufz, Human well-being, in *Open NESS Ecosystem Services Reference Book. EC FP7 Grant Agreement no. 308428*, eds. by M. Potschin, K. Jax, Available via www.openness-Proj., vol. 1, pp. 1–6 (2016)
29. U. Varshney, C.K. Chang, Smart health and well-being. Computer (Long. Beach. Calif.) **49**(11), 11–13 (2016). https://doi.org/10.1109/MC.2016.351

Social Media Community Using Optimized Clustering Algorithm



Muskan Pandey, Om Avhad, Ankita Khedekar, Aarya Lamkhade, and Minakshi Vharkate

Abstract The purpose of this paper is to present an optimized approach for clustering the social media community. The current system works on traditional algorithms and uses rule-based classification and clustering algorithms. This paper presents an approach wherein current pre-processing techniques are enhanced and an optimized approach for an augmented target user base leading to an effective advertisement is presented. The categories for classification are based on professions, stages of life, activities, etc.

Keywords Data mining · Pre-processing · Social media · Clustering · Advertising · Similarity matching algorithm(SMA) · Hierarchical clustering algorithm(HCA)

1 Introduction

Everyone nowadays uses social media sites for a variety of reasons. Our daily lives have become increasingly reliant on social media. Some people use it to show off their talents, while others use it for advertising, networking, and so on. Social networking is a versatile platform that produces a large amount of data for research and improved user experience.

M. Pandey (✉) · O. Avhad · A. Khedekar · A. Lamkhade · M. Vharkate
MIT Academy of Engineering, Pune, India
e-mail: mpandey@mitaoe.ac.in

O. Avhad
e-mail: odavhad@mitaoe.ac.in

A. Khedekar
e-mail: askhedekar@mitaoe.ac.in

A. Lamkhade
e-mail: arlamkhade@mitaoe.ac.in

M. Vharkate
e-mail: mnvharkate@comp.maepune.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_64

The importance of communities can be demonstrated in the following example. In real world too, humans tend to form communities, social groups, unions, teams, etc. based upon common features. Similarly, extending this analogy toward social networks, communities can be formed based on common features and other similarities existing.

The aim of this project is to create a social media community clustering. Identification of the common attributes for grouping is an essential part of this system. It is designed to group together related types of media profiles to make advertising to a specific group of people easier. Since there are so many products in the market, related products can often go unnoticed. The system can be used to bridge the gap between potential buyers and the product while also filtering out the background noise. For example, if you want to advertise a paintbrush, you can target a group of artists or painters. This will augment the product's effective customer base and increase its scope and outreach.

2 Objective

The first objective of this project is to provide an optimized approach to enhance the current data pre-processing techniques and clustering algorithms, and another objective is to provide categorized data to users. This categorized data can be sold to companies to enhance their target user base. This will help them augment their outreach and enhance current advertising practices.

3 Literature Survey

The current practices involved in social media clustering make use of algorithms like k-means clustering and graph clustering based on similar intuitive notions of what a community is, but with different implementations. The similarity between these algorithms and our approach is only restricted till the aim, the implementation varies greatly.

Very relevant work is of Fortunato [1] in 'Community detection in graphs' examined in a very systematic way a wide range of network community detection methods that are originating from theoretical computer science, scientific computing, and statistical physics, etc. also originated from the discussion of crucial issues like the significance of clustering and how methods should be tested and it compared against each other, to the description of applications to real networks.

Visualization methods studied by Jin et al. [2] in Research on Visualization Techniques in Data Mining can be roughly divided into the following groups- The first group is composed of traditional methods of visualization or algorithm independent of data mining. The second group is describing the mode of extraction through data

mining algorithms or methods; thus, it is contributing to a better understanding of the model.

A new idea about k-means clustering is taken from Bhatia [3] New Improved technique for initial cluster centers of k-means clustering using a genetic algorithm. In that, she illustrates that the performance of the k-means algorithm is more efficient in terms of complexity and converges to a global optimum. The results produced were satisfactory in terms of achieving accuracy.

Another interesting case study on data mining is by Seah et al. [4] in Data Mining Approach to the Detection of Suicide in Social Media: A Case Study of Singapore in which they proposed the efficiency of various data mining techniques. Data mining is an efficient way of analyzing different\posts and comments of an individual on social media.

One research paper that gave an idea about data mining techniques is written by Rajesh Kumar et al. [5] which is the Students Performance Prediction Using Data Mining Techniques. It shows that data mining is a rapidly growing area that is being used in educational settings to improve student insight and learning strategies. The aim of this paper is to compare classification methods and predict student results.

Another paper about clustering is a review of spectral methods for clustering written by JingMao and YanXia [6]. It involves the study of spectral clustering (SC). Spectral clustering (SC) is a clustering technology based on the graph theory method. It does not make any assumptions on the basis of the structure of the data, so the algorithm performs well on non-convex data and gets the globally optimal result.

Data Clustering: Algorithms and Its Applications by Oyelade et al. [7] gives the idea about the clustering algorithms and their different applications. When it comes to clustering strategies, there are many things to remember. These considerations include data forms, methodology bias, the existence of outliers, data length, data dimension, and so on. The comparative study of the different clustering algorithms in terms of data types was highlighted.

Comparison of Clustering Techniques for Measuring Similarity in Articles by Rani and Sahu [8] compares the k-means clustering, hierarchical clustering. The 'Cityblock method' for hierarchical clustering and the 'correlation method' for k-means clustering are found to be the best for identifying text similarities in this paper.

Singh et al. [9], in Clustering of people in a social network based on textual similarity, concluded that a social network's textual similarity was highlighted. The textual similarity is determined by looking at words used on social media platforms.

Alsayat and El-Sayed [10] in social media analysis uses optimized k-means clustering. To cluster data, researchers used the k-means clustering algorithm, as well as the genetic algorithm and the optimized cluster distance (OCD) process. And they came to the conclusion that this is the best way to cluster the results.

Narantsatsralt and Kang [11] in, Analysis and Applications of Complex Social Networks, for detecting groups, implemented an agglomerative spectral clustering with conductance and edge weight. In the first step, the proposed method projects the original points into eigenvector feature space. The eigenvector space and the number of edges between nodes are used to determine the similarity between nodes in the

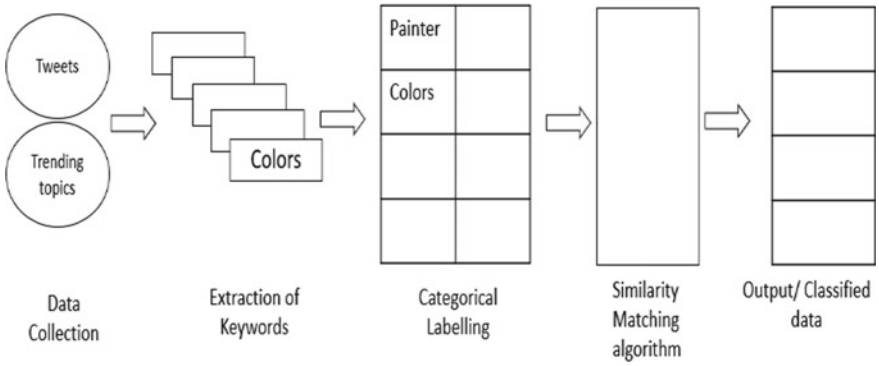


Fig. 1 System architecture of the project

second step. Each node selects a candidate for the nodes that are the most similar. The conductance between the node and its candidate is discovered in the third level. The nodes are agglomerated if only the conductance increases. Iterate the three-stage procedure until the network no longer needs agglomeration.

Mueller and Massaron [12] in Clustering Social Networks in Groups concluded that by simulating what happens in physics between electrically charged particles or magnets carrying the same symbol, the Fruchterman-Reingold force-directed algorithm for creating automatic graph layouts creates understandable layouts with separated nodes and edges that appear not to cross.

4 System Architecture

Tweets and trending topics are mined from social networking websites from which the keywords are extracted. This is followed by categorical labeling of the data. Then, similarity matching algorithm is applied through which the final classified output is obtained (Fig. 1).

5 Methodology

The project is subdivided into key modules. Each of these modules forms a critical step in the development of the system. The modules are as follows:

- Data Mining
- Pre-processing
- Identification of unique categories
- Designing the algorithm to cluster into identified categories

- Testing and optimization
- Visualization

Data can be obtained by scraping various web-based social media platforms. For the purpose of this project, Twitter data was mined using the tool Tweepy. This data included tweets, captions, user bio, hashtags used/followed, etc.

For pre-processing the raw data, various tools were used to gain complete insight into the data and minimize the noise. Tools like multilingual data handler, punctuations removal, contractions handler, emoji context provider, hashtag splitter, etc. All these pre-processing tools help add relevant context to the data as well as help in effective cleaning and filtering.

Based upon the distribution of data, unique categories were identified for effective categorization. These categories include— 'automotive,' 'beauty,' 'books and literature,' 'business,' 'careers,' 'education,' 'events,' 'family and parenting,' 'food and drink,' 'gaming,' 'health,' 'hobbies and interests,' 'home and garden,' 'law, government, and politics,' 'life stages,' 'movies and television,' 'music and radio,' 'personal finance,' 'science,' 'sports,' 'style and fashion,' 'technology and computing,' 'travel.' For optimized clustering, the use of a basic, simple clustering algorithm is not enough. A better adaptive algorithm is designed that is an amalgam of various approaches.

A dictionary of keywords mined from hashtags along with categories associated with them. The words from sentences can directly be used for obtaining the tags. A single keyword can have multiple categories. After the keywords are categorized, context addition is necessary to make the categorization more relevant and meaningful. For this purpose, *N*-gram (bi-gram) is being used. When there are more than two keywords with different categories in the same sentence, their occurrences together are referred, and conclusive categorization is done.

For efficient keyword picking, we are using an *n*-gram technique. An *n*-gram is a contiguous sequence of n items from a given sample of text or speech, e.g., 'system design' is a 2-g or bi-gram. In an *N*-gram-based text categorization, the system calculates and compares profiles of *N*-gram frequencies. Training sets are used as the baseline, generating category profiles for particular languages or subjects. The keyword mapping with categories was done by intricate web scraping and a condensed, normalized version was developed.

Testing data for a group/organization. Taking an example of a particular organization and testing their user base before and after the use of the system to verify the augmentation.

Effective visualization helps demystify ambiguities and understand the minute details better. Various charts can be used to delineate the result and juxtaposition it with the previous reach.

6 Expected Outcome

The expected outcome of the project is:

Optimization:
An optimized approach to enhance the current pre-processing and clustering algorithms.

Augmentation:
An augmented target user base for effective advertisement.

Cognizance:
Using effective visualization to help demystify and better understand the available user data.

7 Result

The test data constituted of about two thousand random bios, and they were categorized. The accuracy obtained was: 94% (Table 1).

After clustering the keywords based on categories, word cloud was generated for three categories: 'Automotive' and 'careers.' (Fig. 2).

Table 1 Sample results

Sr. No	Bio	Keywords	Category
1	Sports Reporter/PxP Broadcaster for @SpecSports360 @mynews13–Twin, Virgo, traveler, foodie and lover of live music. Story Ideas/Tips Despina.Barton@charter.com	['sports reporter,' 'pxp broadcaster,' 'live music,' 'story ideas,' 'twin,' 'virgo,' 'traveler,' 'foodie,' 'lover']	['sports,' 'music and radio,' 'movies and television,' 'food and drink,' 'travel']
2	I'm a proud Blockhead who lives in a small town. I take care of my mother who has cancer and i'm Followed by 2 of 5 nkotb members. #LoveEternal	['proud blockhead,' 'small town,' 'care,' 'cancer,' 'nkotb members,' ' love eternal']	['health,' 'events,' 'music and radio']
3	-2010 UCF Alum. Volleyball coach at Boomers Volleyball Academy	['2010 ucf alum,' 'volleyball coach,' 'boomers volleyball academy']	['life stages,' 'careers,' 'sports']
4	fries before guys	['fries']	['food and drink']
5	French geek living in Japan Youtuber, JavaScript lover, and more	['french,' 'geek,' japan,' 'youtuber,' 'javascript lover']	['travel,' 'technology and computing']

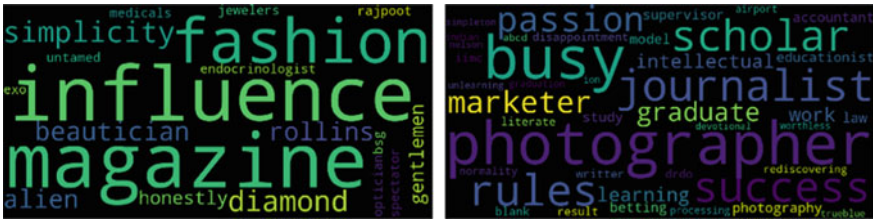


Fig. 2 Word cloud for 'style and fashion' and 'careers' categories

8 Conclusion

This project provides an optimized approach for clustering social media profiles and is an enhancement to the current clustering algorithms. Clustering of profiles is not rule-based but combines an amalgam of various techniques. The data is presented in an efficient way for boosting the user base for directed advertisements.

References

1. S. Fortunato, Community detection in graphs. Phys. Rep. **486**(3–5), 75–174 (2010)
2. H. Jin, H. Liu, Research on visualization techniques in data mining. pp. 1–3 (2009)
3. S. Bhatia, New improved technique for initial cluster centers of K means clustering using genetic algorithm, in *International Conference for Convergence for Technology-2014*, pp 1–4 (2014)
4. J.H.K. Seah, K. Jin Shim, Data mining approach to the detection of suicide in social media: A case study of Singapore, in *2018 IEEE International Conference on Big Data (Big Data)* (2018), pp. 5442–5444
5. T.R. Kumar, T. Vamsidhar, B. Harika, T.M. Kumar, R. Nissy, Students performance prediction using data mining techniques. Int. Conf. Intell. Sustain. Syst. (ICISS) **2019**, 407–411 (2019)
6. Z. JingMao, S. YanXia. Review spectral methods for clustering, in *34th Chinese Control Conference (CCC)* (2015), pp. 3791–3796
7. J. Oyelade et al., Data clustering: Algorithms and its applications, in *19th International Conference on Computational Science and Its Applications (ICCSA)* (2019), pp. 71–81
8. U. Rani and S. Sahu. Comparison of clustering techniques for measuring similarity in articles, in *3rd International Conference on Computational Intelligence & Communication Technology (CICT)* (2017), pp. 1–7
9. K. Singh, H. Kumar, S.B. Biswas, Clustering of people in a social network based on textual similarity. Perspect. Sci. (2016)
10. A. Alsayat, H. El-Sayed, Social media analysis using optimized K-Means clustering, in *IEEE 14th International Conference on Software Engineering Research, Management and Applications (SERA)*, pp. 61–66 (2016)
11. U.-U. Narantsatsralt, S. Kang, Analysis and applications of complex social networks. Complexity **2017**, 1–2 (2017)
12. J.P. Mueller, L. Massaron, Clustering social networks in groups, in *Algorithms for dummies* (2017), pp 198–203

Optimal Allocation of Distributed Generation in Order to Improve the Performance of Power System Networks



R. B. Singh, R. P. Payasi, and K. S. Verma

Abstract The optimal allocation of distributed generation at optimal bus so that the performances of power system networks have been improved which is presented using Particle Swarm Optimisation Technique. The voltage stability and power losses are main concern for safe operations of power system networks. Recently due to their stressed operations for increasing electrical power loads, voltage instability and voltage collapse are evitable, which are main problems in the power system networks. By using different type of DG of optimal size at optimal location, the overall power losses are reduced and voltage profile of power system network is improved. The particle swarm optimization (PSO) technique has been used for optimal location of distributed generation (DG type-1) of the Optimal value to reduce overall power losses and maintained voltage profile. The results show that the overall power losses of the power system networks are reduced and at the same time the voltage profile is maintained using optimally locating DG in the power system networks. The proposed methodologies are tested on IEEE-9 bus, IEEE-24 bus and IEEE-30 bus distribution systems using MATLAB tool-box and MATPOWER 6.0 software package.

Keywords Distributed generation · Optimal location of DG · Optimal size of DG · Particle Swarm Optimization

1 Introduction

The distributed generation (DG) is an insignificant generator covered all over power system network providing electricity locally to load customers [1]. DG could be innovative for business, industrial and residential applications. DG uses the latest contemporary technology that is powerful, reliable and easy enough to compare in some areas with conventional large generators [2, 3]. The power industry has experienced major

R. B. Singh (✉)
Goverment Polytechnic, Kenura Sultanpur, Uttar Pradesh 228159, India

R. P. Payasi · K. S. Verma
Kamla Nehru Institute of Technology, Sultanpur, Uttar Pradesh 228118, India
e-mail: ksv211@rediffmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_65

changes in the distribution power system in recent years largely due to the implementation of smart grid technology and the gradual adoption of distributed generation. Distributed generation (DG) is clearly characterized as power plant decentralization by putting smaller generating units closer to the point of demand, usually ten megawatts or less. Although DG is not a new idea, DG is gaining extensive attention principally for the behind reasons: client demand development, technical developments, economics, globalization, environmental and national security concerns. Conventionally, the distribution system is radial and operates without mounted generating systems. The electrical power is delivered to the distribution network via transmission at the grid supply point. Consequently, the power is flow from transmission to distribution in one direction. At present, the number of generations related to the delivery network is rising, which is commonly called distributed generation. The location and quantity of power supplied to the distribution system by the DG have an influence on system operation. They can either improve or diminish the system's effectiveness and stability. Large power supplied by the DG can also reverse the current flow direction. Hence, the DG's correct location and size are preferred.

The optimal location of a particular sizing DG is calculated in [3] using the technique of particle swarm optimization. Today, technical advances, environmental policies, as well as the growth of finance and electrical markets, foster new conditions in the electricity generation sector [7]. New technologies allow the generation of electricity in small sized plants. In addition, the growing use of renewable sources to reduce the environmental effect of producing electricity contributes to the creation and implementation of new schemes for electrical energy supply.

The generation is not confined to level 1, in this modern conception. Therefore the centralized generation supplies some of the energy-demand and another part is provided by distributed generation. The electricity will be generated more close to the customers. In other words, the electrical network is defined as the distribution system between the substation being supplied by the transmission system and the meter of the customer. Feeders, retailers, and the service mains are the central components of a distribution system. The single line diagram of a typical low voltage distribution system is shown in Fig. 1.

1.1 Distributed Generation

A new concept originated in the electrical system map known as "distributed generation" (DG) as a result of deregulation in the electric power market. Distributed generation (DG) is not a completely new phenomenon, but it is an innovative solution to power generation in the heart of the power system. If the installation of a portfolio of low, lightweight and clean power-based optimization and evolutionary computational (EC) technique which is encouraged using social behavior of bird flocking and fish schooling [23]. The PSO technique is required some memories and very generation units at or near the load (customer) depends mainly on the installation.

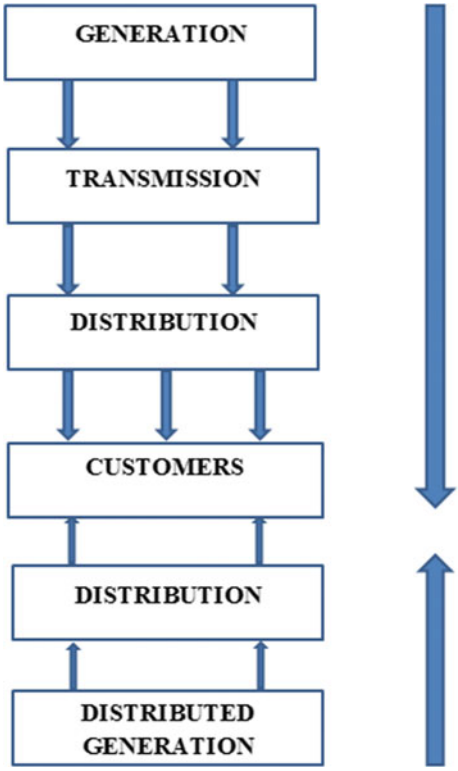


Fig. 1 New industrial conception of the electrical energy supply

According to new technologies, the trend in the generation of electricity uses distributed generation units sized from kW to MW at load sites instead of using conventional centralized generation units sized from 100 MW to several GW and placed for loads where natural resources are available [3]. Small-scale generation technologies, such as gas turbines, small hydro-turbines, photo- voltaic, wind turbines and fuel cells, replace conventional generating technologies in various applications in the electrical power system [4]. There are several advantages to these distributed technologies, such as high fuel consumption, short contribute to their increasing popularity. Considering the way the very earliest power utilities were working to produce and distribute electricity. Utilities have their own designated area, which topically produces and delivers electricity. Then national grids or regional grids came from a large interconnected network that made power systems more cost-effective and reliable [4, 5].

New issues that have arisen recently in the power sector viz. Although hydropower plants have been recognized as environmentally friendly, finding new hydropower plant sites in developing countries is difficult. In addition, lows to decommissioned nuclear power plants were introduced by some countries such as Germany and Sweden and closed nuclear power plants will not be replaced. In addition, it is not easy to persuade market participants in the pronominally deregulated power industry to invest in billions of dollars in power generation and transmission projects where the payback period increasing very long. Such problems, the decentralization of the energy network and the liberalization of the electricity market, along with the significantly increasing demand for electricity in developing countries, have made DG an interesting one that has been reconsidered by various entities such as consumers, suppliers, power producers, regulators and researchers [5] as well.

Various distributed generation (DG) devices can be strategically installed in grid power networks, reducing power losses, improving voltage profile and load factors, minimizing network upgrades and enhancing system quality, reliability and effectiveness. In this paper Particle Swarm optimization technique is used to achieve the optimum size and position of DG for which the system's power loss is negligible, voltage control is maintained at each bus, and the device frequency is stable.

1.2 Particle Swarm Optimization (P_{so})

In 1995 Kennedy and Eberhart provided the first fundamental description of the Particle Swarm Optimization (PSO) technique. In this paper, using PSO technique we find that the DG of "optimal size at optimal bus location" is placed. During this process, the overall power losses of the power system are reduced at the same time as the overall voltage profile of the power system network is also improved compared to that of the power system networks without using DG. We take three test bus systems IEEE9, IEEE 24 and IEEE30 for this purpose.

2 Results and Discussion

2.1 Results for IEEE 9 Bus System

Voltage profile improvement is shown in Fig. 2 and it is clear from the graph that the voltage profile is enhanced after installation of DG at optimal located bus no 2 and optimal size 83.3014 MVA type 1 DG. Blue line is representing voltage profile before installation of DG and red line is representing voltage profile after installation DG (Table 1).

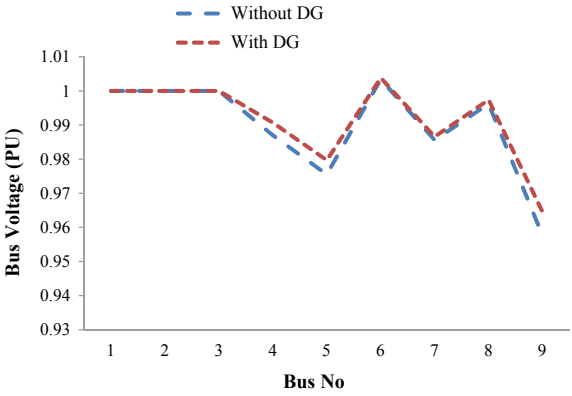


Fig. 2 IEEE 9 Bus voltage profile with and without installation of DG

Table 1 IEEE 9 bus systems for bus voltage

Bus no	Bus voltage without DG	Bus voltage with DG
1	1.0000	1.0000
2	1.0000	1.0000
3	1.0000	1.0000
4	0.9870	0.9907
5	0.9755	0.9797
6	1.0034	1.0038
7	0.9856	0.9866
8	0.9962	0.9974
9	0.9576	0.9645

After installation of DG, the losses in electrical power system network of IEEE 9 bus system have been reduced which is shown in Fig. 3. Without installation of DG the overall total loss is 4.9550 MW after installation of type 1 DG of optimal size 83.3014 MVA at optimal located bus no 2. The overall total loss is reduced such as 2.9404 MW. Blue line is representing network loss with DG and red line is representing network loss without DG (Table 2).

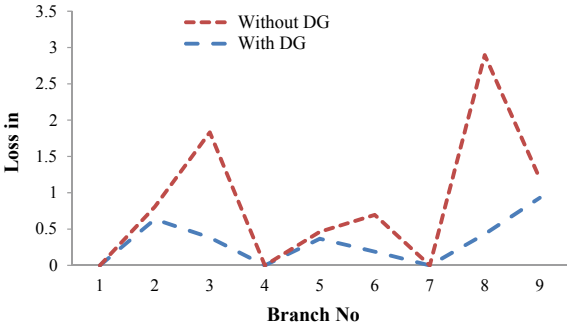


Fig. 3 IEEE 9 system network losses with and without installation of DG

Table 2 IEEE 9 bus systems for branch loss

Branch no	From bus	To bus	Branch loss without DG	Branch loss with DG
1	1	4	0.000	0.000
2	4	5	0.174	0.635
3	5	6	1.449	0.384
4	3	6	0.000	0.000
5	6	7	0.095	0.368
6	7	8	0.506	0.19
7	8	2	0.000	0.000
8	8	9	2.465	0.432
9	9	4	0.266	0.931

2.2 Results of Voltage Profile for 24 Bus and Branch System

The voltage profile enhancement is shown in Fig. 4 and it is clear from the graph that the voltage profile is enhanced subsequently installation of DG at optimal located bus no 22 and optimal size 386.6614 MVA type 1 DG. Blue line is representing voltage profile before installation of DG and red line is representing voltage profile after installation DG (Table 3 and 4).

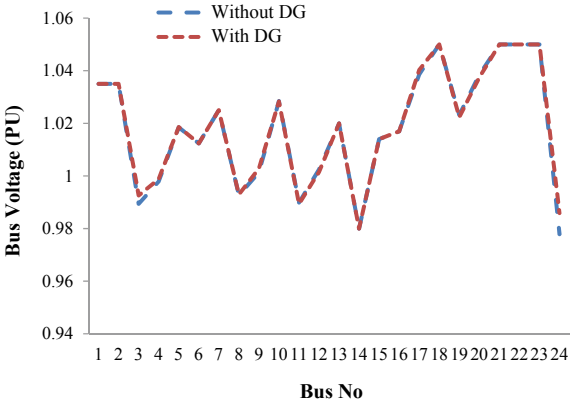


Fig. 4 IEEE 24 Bus voltage profile with and without installation of DG

Table 3 IEEE 24 bus systems for bus voltage

Bus no	Bus voltage without DG	Bus voltage with DG
1	1.0350	1.0350
2	1.0350	1.0350
3	0.9894	0.9926
4	0.9979	0.9988
5	1.0185	1.0186
6	1.0124	1.0124
7	1.0250	1.0250
8	0.9927	0.9930
9	1.0013	1.0028
10	1.0285	1.0283
11	0.9899	0.9894
12	1.0025	1.0015
13	1.0200	1.0200
14	0.9800	0.9800
15	1.0140	1.0140
16	1.0170	1.0170
17	1.0386	1.0403
18	1.0500	1.0500
19	1.0232	1.0224
20	1.0385	1.0375
21	1.0500	1.0500
22	1.0500	1.0500
23	1.0500	1.0500
24	0.9779	0.9859

Table 4 IEEE 24 bus systems for branch loss

Bus no	From bus	To bus	Branch loss without DG	Branch loss with DG
1	1	2	0.004	0.000
2	1	3	0.342	0.223
3	1	5	0.741	0.533
4	2	4	0.587	0.523
5	2	6	1.093	0.84
6	3	9	0.24	0.076
7	3	24	1.113	0.597
8	4	9	0.364	0.420
9	5	10	0.046	0.104
10	6	10	1.067	1.209
11	7	8	2.118	2.113
12	8	9	0.604	0.524
13	8	10	0.303	0.336
14	9	11	0.277	0.313
15	9	12	0.369	0.563
16	10	11	0.546	0.525
17	10	12	0.641	0.814
18	11	13	0.618	3.308
19	11	14	1.778	0.099
20	12	13	0.271	1.634
21	12	23	6.399	3.883
22	13	23	5.438	1.284
23	14	16	7.054	2.834
24	15	16	0.290	0.007
25	15	21	2.913	1.167
26	15	21	2.913	1.167
27	15	24	3.219	1.717
28	16	17	3.353	0.661
29	16	19	0.433	0.103
30	17	18	0.638	0.372
31	17	22	2.454	0.051
32	18	21	0.111	0.042
33	18	21	0.111	0.042
34	19	20	0.113	0.716
35	19	20	0.113	0.716
36	20	23	0.291	0.908
37	20	23	0.291	0.908
38	21	22	1.994	0.397

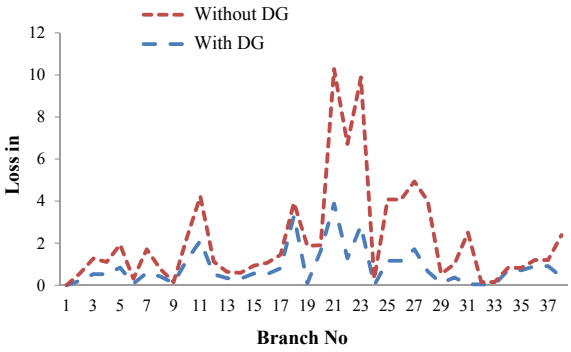


Fig. 5 IEEE 24 system network losses with and without installation of DG

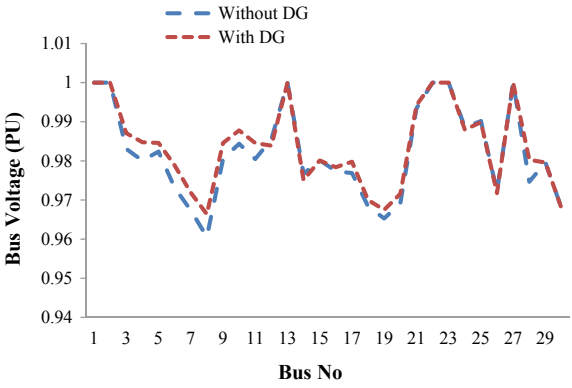


Fig. 6 IEEE 30 Bus voltage profile with and without installation of DG

After installation of DG, the losses in electrical power system network of IEEE 24 bus system have been reduced which is shown in Fig. 5. Without installation of DG the overall total loss is 51.2460 MW after installation of type 1 DG of optimal size 386.6614 MVA at optimal located bus no 22. The overall total loss is reduced such as 31.7260 MW. Blue line is representing network loss with DG and red line is representing network loss without DG.

2.3 Results of Voltage Profile for 30 Bus and Branch System

The voltage profile improvement is shown in Fig. 6 and it is clear from the graph that the voltage profile is enhanced subsequently installation of DG at optimal located bus no 10 and optimal size 43.1937 MVA type 1 DG. Blue line is representing voltage profile before installation of DG and red line is representing voltage profile after installation DG (Table 5).

Table 5 IEEE 30 bus systems for bus voltage

Bus no	Bus voltage without DG	Bus voltage with DG
1	1.0000	1.0000
2	1.0000	1.0000
3	0.9831	0.9871
4	0.9801	0.9848
5	0.9824	0.9846
6	0.9732	0.9789
7	0.9674	0.9719
8	0.9606	0.9664
9	0.9805	0.9846
10	0.9844	0.9878
11	0.9805	0.9846
12	0.9855	0.9839
13	1.0000	1.0000
14	0.9767	0.9751
15	0.9802	0.9801
16	0.9774	0.9784
17	0.9769	0.9798
18	0.9684	0.9700
19	0.9653	0.9675
20	0.9692	0.9716
21	0.9934	0.9942
22	1.0000	1.0000
23	1.0000	1.0000
24	0.9886	0.9880
25	0.9902	0.9899
26	0.9722	0.9718
27	1.0000	1.0000
28	0.9747	0.9803
29	0.9796	0.9796
30	0.9679	0.9679

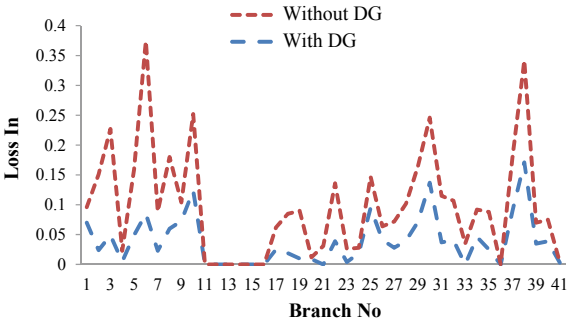


Fig. 7 IEEE 30 system network losses with and without installation of DG

After installation of DG, the losses in electrical power system network of "IEEE 30 bus system" have been reduced which is shown in Fig. 7. Without installation of DG the overall total loss is 2.4440 MW after installation of type 1 DG of optimal size 43.1937 MVA at optimal located bus no 10. The overall total loss is reduced such as 1.5850 MW. Blue line is representing network loss with DG and red line is representing network losses without DG (Table 6).

3 Conclusion

In the distribution power system networks, the power losses and maintaining the voltage profile is difficult task. In this paper, we use "particle swarm optimization technique" for all allocating the capacity of the DG and the site selection of the DG. We use PSO technique for appropriate capacity of the DG at optimally located bus and the overall power loss of electrical power system is abridged and at the same time "voltage profile of the power system network" is enhanced. The power losses are major concern in the distributed power system networks so the use of proper size of DG at optimal position bus is very important. Thus from the above results, it can be concluded the "power losses of the power system networks" are abridged appreciably, and at the same time, the voltage profile is maintained.

Table 6 IEEE 30 bus systems for branch loss

Bus no	From bus	To bus	Branch loss without DG	Branch loss with DG
1	1	2	0.026	0.070
2	1	3	0.127	0.024
3	2	4	0.178	0.049
4	3	4	0.018	0.005
5	2	5	0.110	0.049
6	2	6	0.289	0.085
7	4	6	0.066	0.023
8	5	7	0.120	0.060
9	6	7	0.031	0.073
10	6	8	0.128	0.124
11	6	9	0.000	0.000
12	6	10	0.000	0.000
13	9	11	0.000	0.000
14	9	10	0.000	0.000
15	4	12	0.000	0.000
16	12	13	0.000	0.000
17	12	14	0.037	0.025
18	12	15	0.066	0.019
19	12	16	0.080	0.010
20	14	15	0.003	0.009
21	16	17	0.031	0.000
22	15	18	0.097	0.039
23	18	19	0.022	0.004
24	19	20	0.009	0.019
25	10	20	0.052	0.095
26	10	17	0.023	0.041
27	10	21	0.044	0.028
28	10	22	0.062	0.040
29	21	22	0.093	0.071
30	15	23	0.109	0.137
31	22	24	0.078	0.037
32	23	24	0.066	0.041
33	24	25	0.035	0.000
34	25	26	0.046	0.046
35	25	27	0.063	0.025
36	28	27	0.000	0.000

(continued)

Table 6 (continued)

Bus no	From bus	To bus	Branch loss without DG	Branch loss with DG
37	27	29	0.090	0.090
38	27	30	0.171	0.171
39	29	30	0.035	0.035
40	8	28	0.036	0.039
41	6	28	0.001	0.003

References

1. M. Ali Eltamaly, M.S. Al-Saud, Nested multi-objective PSO for optimal allocation and sizing of renewable energy distributed generation. J. Renew. Sustain. Energy **10**, 035302 (2018). https://doi.org/10.1063/1.5028484
2. A. Apparao, K. Bhashna, Optimal allocation of DG considering loss minimization and voltage profile using PSO. Int. J. Sci. Res. (IJSR) ISSN (Online): 2319-7064
3. A. Mishra, A. Bhandakkar, Selection of optimal location and size of distributed generation in distribution system using particle swarm optimization. Int. J. Eng. Res. Technol. (IJERT) **3**(1) (Jan 2014) IJERT ISSN: 2278-0181
4. S.K. Injeti, V.K. Thunuguntla, Optimal integration of DGs into radial distribution network in the presence of plug-in electric vehicles to minimize daily active power losses and to improve the voltage profile of the system using bioinspired optimization algorithms. Prot. Control Mod. Power Syst. (2020)
5. B. Singh, K.S. Verma, P. Mishra, FACTS controllers power system (PS); performance parameters of systems" department of electrical engineering. Kamla Nehru Institute of Technology, Sultanpur. 228118 (U.P.)
6. B. Singh, K.S. Verma, D. Singh, C.N. Singh, Introduction to FACTS controllers a critical review. IJRIC **8** (Dec 2011)
7. M.M. Farsangi, H. Nezamabadi-Pour, K.Y. Lee, Multi-objective VAR planning with SVC for a large power system using PSO and GA, (Fellow, IEEE, PSCE, 2006)
8. C.N. Ko, Y.P. Chang, C.J. Wu, A PSO method with nonlinear time-varying evolution for optimal design of harmonic filters. Vol. 24, No. 1, (Feb 2009)
9. S. Auchariyamet, S. Sirisumrannukul, Optimal reactive power planning with facts devices by particle swarm technique. King Mongkut's University of Technology North Bangkok, Thailand
10. H. Yoshida, K. Kawata, Y. Fukuyama, A particle swarm optimization for reactive power and voltage control considering voltage security assessment. Vol. 15, No. 4 (Nov 2006)
11. K. Sundareswaran, B. Hariharan, F.P. Parasseri, D.S. Antony, B. Subair, Optimal placement of static VAR compensators (SVC's) using particle swarm optimization. IEEE (2010)
12. R. Benabid, M. Boudour, Optimal placement of FACTS devices for multiobjectiv voltage stability problem. Member, IEEE, and, M. A. Abido, Member, IEEE
13. S. Sakthivel, R. Vetrivel, V.S. Kannan, Optimal location of SVC for voltage stability enhancement under contingency condition through PSO algorithm. V.R.S. College of Engg and Tech, Villupuram, Tamil Nadu
14. T. K. Das, S.R. Jetti, G.K. Venayagamoorthy, Optimal design of SVC damping controllers with wide area measurements using small population based PSO. Member IEEE International
15. K. Dhananjaya Babu, M. Damodar Reddy, M. Eghbal, E.E. El-Araby2, N. Yorino1, Y. Zoka1, Application of metaheuristic methods to reactive power planning: a comparative study for GA, PSO and EPSO. Member IEEE
16. M. Eghbal, N. Yorino, Y. Zoka, Comparative study on the application of modern heuristic techniques to SVC placement problem. Graduate School of Engineering, Hiroshima University, Higashihiroshima, Japan

17. M.M. Farsangi, H. Nezamabadi-pour, K.Y. Lee, Multi-objective VAR planning with SVC using immune algorithm and guaranteed convergence particle swarm optimization. Dept. EEE Shahid Bahonar University, Kerman, Iran, Journal of Comp. Vol.4, No. 6 (June 2009)
18. B. Singh, K.S. Verma, K.K. Singh, A.K. Shukla, A. Singh, J.V. Narlikar, Clearance of fault in power system networks by SVC and Statcom. Dept. of EE KNIT, Sultanpur-228118 (U.P.), India 6–11 July 2008
19. M.M. Farsangi, H. Nezamabadi-pour, K.Y. Lee, Implementation of GCPSO for multi-objective VAR planning with SVC and its comparison with GA and PSO. Follow IEEE
20. S. Nagalakshmi, N. Kamaraj, Loadability enhancement for pool model with FACTS devices in transmission system using differential evolution and particle swarm optimization. Member IEEE
21. V.K. Jain, H. Singh, L. Srivastava, Minimization of reactive power using particle swarm optimization. Dept. EEE, Madhav Institute of Technology and Science, Gwalior (M.P.), India, IJCER, May-June, 2012, Vol.2, Issue No.3, pp. 686–691
22. A. Banga, S.S. Kaushik, Modeling and simulation of SVC controller for enhancement of power system stability, ECE Deptt., Advanced Institute of Technology & Management, Palwal
23. N.G. Hingorani, L. Gyugyi, Understanding FACTS, IEEE Press, New York 2000

E-Aid: Open Wound Identifier and Analyzer Using Smartphone Through Captured Image



Joie Ann W. Maghanoy, Daryl G. Guzman, Joan Stephen D. Paz, Dale R. Policarpio, Ansley D. Yanga, and Shaneth Ambat

Abstract E-Aid is a study that aims to develop an application based on the convolutional neural network algorithm. The central idea for the creation of E-Aid is to provide a mobile application which offers more advanced capabilities and leads to a strong emergence for the medical health applications in the market. The reliability for the usage of CNN as an algorithm produces positive results which is essential for this study. The researchers trained CNN model that will be used later on during the execution of the CCN algorithm, and this CNN model must be able to identify 4 types of open wounds (laceration, puncture, abrasion and avulsion) and 4 types of skin burns (1st-, 2nd-, 3rd- and 4th-degree burn) and also must be able to classify it whether the wound is infected or not infected. The researchers tested the accuracy of the CNN model before sending to our respondents. The researchers tested the accuracy by getting a random image of open wounds and skin burns in the Internet and run it on the E-Aid app. After the researchers finish testing the accuracy of the app, they distributed the app to their respondents to test furthermore the accuracy and reliability of the app. The researchers' respondents are composed of 6 medical professionals (doctors/nurses), 5 IT/CS professionals and 14 students (in the field of medicine and computer studies).

Keywords Convolutional neural network · Effective wound analyzer · Effective · Effective skin burn detection · Computer-aided medical application · Medical-related mobile application

1 Introduction

The treatment and management of wounds is a nonstop health challenge for the people in the world, especially the elderly and bedridden people. Recognizing the wound area would be the first step in assessment and treatment for the wound.

J. A. W. Maghanoy (✉) · D. G. Guzman · J. S. D. Paz · D. R. Policarpio · A. D. Yanga · S. Ambat
FEU Institute of Technology, P. Paredes St., Sampaloc Metro Manila, Philippines

S. Ambat
e-mail: Scambat@feutech.edu.ph

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_66

However, according to a study by Navas et al. (2013) the evaluation of the wound is mostly based on visual checking and hands-on examination which are subjective and imprecise. Digital-based and computer-aided applications have proved effective in exceeding the expectation of accuracy in terms of wound assessment. The computer-aided approach obtained great results which enables a reliable diagnosis with the use of a computational system.

The researcher's study will be able to examine and give an assessment to the 4 types of open wounds, abrasion, laceration, puncture, and avulsion. The application provides and analyzes the basic information provided by the user and will be turned into a data file which can be used for further monitoring assisted by a medical professional. The application will be able to analyze skin burn as well as its severity levels.

2 Problem Statement

For people in the world, especially elderly and bedridden people, the treatment and management of wounds is a nonstop health challenge. In 2018, retrospective analysis of Medicare beneficiaries identified that 8.2 million people had wounds with or without infections. An open wound, typically affecting the skin, is an injury involving an external or internal split in body tissue. At some point in their lives, almost everyone will experience an open wound. Most open wounds are superficial and are treatable at home. Digital-based and computer-aided applications have proved effective in exceeding the expectation of accuracy in terms of wound assessment. This mobile application will be using convolutional neural network, also known as *ConvNet or CNN*, which is a deep learning algorithm which can take in an input image, assign differences and be able to differentiate one from the other. The application will also be using Dijkstra's algorithm for finding the shortest path for the nearest clinic or hospital that will be available for the user's convenience for further checkup and consultation. Finally, the TTS algorithm or text-to-speech synthesizer will be an added feature for the application. It will provide the application a feature that can aid the visually impaired people by offering a computer-generated spoken voice that would read text to the user. Entering the technology revolution in our generation is full innovation to ease the life of people. Everything runs through the Internet, gadgets and other forms of technology which in the case of the proposed study by the proponents, a health application will be of great use not just in the current time but for the future and betterment of the society.

3 Theoretical Framework

Increasing understanding of electronic wound care applications could enhance timely evaluation, diagnosis and treatment initiation for wound care. The lack of wound

care education of the care provider negatively affects the comfort level in treating the wounds (Kulikov, 2019). The proponents developed a mobile application that helps people gain knowledge about the treatment of open wounds and skin burns to improve the evaluation, diagnosis and initiation of treatment for wound care and prevent further wound complications.

This mobile application used a convolutional neural network (CNN), a deep learning algorithm that can consider an input image, assign differences and distinguish one from another. The use of machine learning is necessary for developing the application and is a component in creating an effective wound and skin burn detector and analyzer. The CNN algorithm can distinguish the percentage, wherein some wounds might result in more than one classification of the type of open wound. This was also used as the learning algorithm for analyzing skin burn and its level of severity.

The application also used Dijkstra's algorithm for finding the shortest route available for the user's convenience for a further checkup in the nearest clinic or hospital. It is the backbone of every system for navigation, such as Google Maps. Mathematically, the Dijkstra algorithm always finds the shortest path, as long as at least one route is possible.

Finally, the text-to-speech (TTS) algorithm was added feature for the application. It provides the application a feature that can help visually impaired people by producing a computer-generated voice that reads text to the user for a user.

4 Problem Statement

4.1 General Objectives

This study aims to develop E-Aid, an open wound and skin burn identifier and analyzer using smartphone through captured image.

4.2 Specific Objectives

The study aimed at accomplishing the following: (1) to provide a mobile application that will be able to provide a platform where users can contact health professionals with a messaging system in the application; (2) to provide a mobile application that can give necessary information about first aid treatments quickly and effectively; (3) to generate accurate results for the detection, classification and analysis of open wounds and skin burns applying the convolutional neural network; (4) to design a database that can generate the daily reports and the weekly reports of every accident that occurs; and (5) to store analyzed data from produced results to a database for further evaluation and enhancement of the application.

5 Scope and Limitation

5.1 Scope

The application focuses only on the 4 types of wounds such as abrasion, laceration, puncture and avulsion. The application will be focusing on analysis of skin burn severity levels as well as the monitoring of diabetic wound healing. The application will be accessible to the user that has a smartphone and tablet. Users can use the application even if they are online or offline. Users must turn on their GPS and Wi-Fi or data connection to help them to locate any hospitals or doctors in their vicinity in case of a medical emergency. It uses their GPS to find their location and show relevant hospitals near them. The application has a voice.

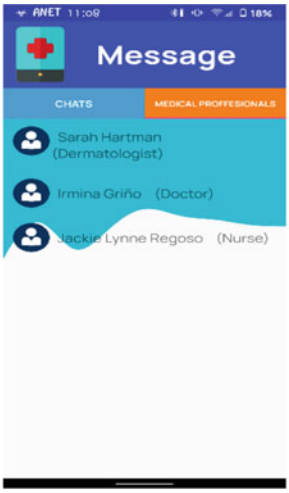
5.2 Limitations

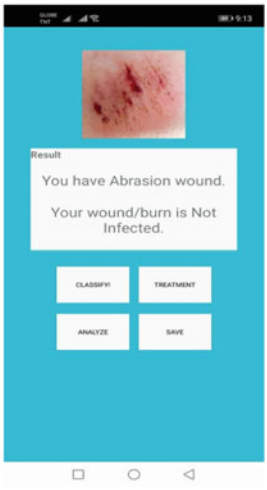
The application will only be available to the user that has access to a smartphone or a tablet, and any form of other gadget that has no access to an application store for the E-Aid to be downloaded cannot and will not be able to use it. The last consideration for the limits of the application would be the different types of wound that is not available to the stored data of the application, meaning it is not classified under the 4 types of wound provided by the mobile application, E-Aid. The application can only identify and examine open wounds, and other than that, it will not be able to provide information. The application will also be able to provide first aid treatment only and not medicines such as drugs, tablets and syrups. It is also limited to the skin burn availability from degree one to four (1–4) and providing the classification, analysis and the treatments.

6 Figures

Below is the list of build-in and user-defined classes and functions used in the software:







7 Survey Analysis

The researchers have successfully developed and designed a health-related mobile application that can detect, identify and analyze captured open wound and skin burn images. In addition, when measured through the survey in terms of effectiveness, the application was able to score 4.57 for speed, 4.62 for user-friendliness and 4.34 for security. The three indicators under the effectiveness category of the application coming from the feedback from the respondents suggest that the application is acceptable. The respondents, however, gave fair ratings when it comes to the efficiency category, which there are two indicators, accuracy and reliability. The general rating of feedback from the respondents suggests that there is a required minimal level of improvements to achieve an overall result that are beyond satisfactory.

8 Conclusion

The researchers were able to have a conclusion based on the results gathered from online surveys and interviews. The conclusion of the proponents is based on the study's objectives. Based on the findings of the study, the following conclusions were drawn: (1) The application provides great applicability and usability for people interested in a health-related application that will serve as a good contribution to health-related applications in the market. (2) The application's messaging system will serve as a tool for virtual communication between doctors and patients for pre-consultation and be a source of reliable data for further analysis and evaluation. (3)

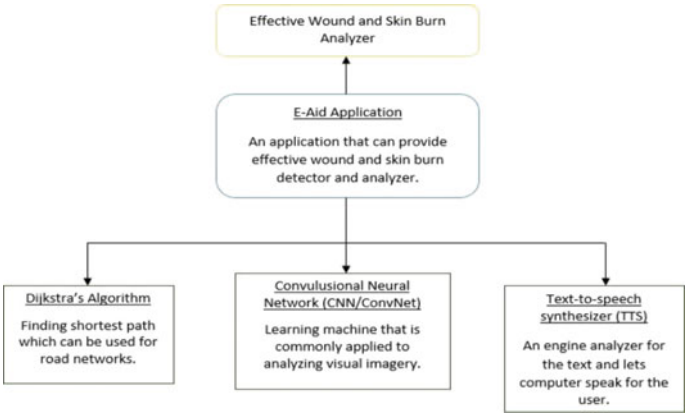


Fig. 1 Theoretical framework

The application will be applicable to be further utilized with other health-related studies as well as development of an application.

9 Recommendation

Based on the conclusions drawn from the findings and conclusions of the study, future researchers or students who will engage in the same study conducted may consider the following recommendations: (1) The future researchers and/or students are highly encouraged to use strong algorithms to speed up the detection and the accuracy of the results. (2) Implement more data augmentation on dataset to improve detection. (3) Input more data regarding the detection of the image in terms of the dimension. (4) Add feature such as the monitoring for the wound healing. (5) Provide the availability and supportability of the application for the iOS system. (6) Create a steady version for the android system that supports lower models. (7) Get in the latest trends in terms of technology and in medical field for the betterment of the study.

References

1. Bonner, A.: The Complete Beginner's Guide to Deep Learning: Convolutional Neural Networks. Retrieved from https://towardsdatascience.com/wtf-is-image-classification-8e78a8235acb Ding, W. and Marchionini, G. 1997. *A Study on Video Browsing Strategies.* Technical Report. University of Maryland at College Park. (2019, June 1).
2. Bryne, M.: The Simple, Elegant Algorithm That Makes Google Maps Possible. Retrieved from https://www.vice.com/en/article/4x3pp9/the-simple-elegant-algorithm-that-makes-google-maps-possibleTavel, P. 2007. *Modeling and Simulation Design.* AK Peters Ltd., Natick, MA. (2015, March 22).

3. Dujovny, M., & Kositzke, C.:Pressure Injury Evolution: Mobile Wound Analyzer Review. Retrieved from http://www.imedpub.com/articles/pressure-injury-evolution-mobile-woundanalyzer-review.php?aid=22999. (2018, July 3).
4. Han, G., & Ceilley, R.:Chronic Wound Healing: A Review of Current Management and Treatments. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5350204/. (2017, March).
5. Navas, M. N., Baena, R. M. L. B., Morente, L. M., & Coronado, D. C.: Computer-Aided Diagnosis in Wound Images with Neural Networks. Research Gate. https://www.researchgate.net/publication/261851842_Computer-Aided_Diagnosis_in_Wound_Images_with_Neural_Networks. (2013, June).
6. Pires, I. M., & Garcia, N.: Wound Area Assessment using Mobile Application. Retrieved from https://www.researchgate.net/publication/270958252_Wound_Area_Assessment_using_Mobile_Application. (2015, January).
7. Stanojev, C. S.:Will Mobile Apps Bring Wound Care Technology to the "Cutting Edge"? Today's Wound Clinic. https://www.todayswoundclinic.com/articles/will-mobile-apps-bring-wound-care-technology-cutting-edge. (2018, January 4).

Intelligently Trained Elman Neural Network-Based MPPT for Photovoltaic Systems



Sangita Bapu Patil and L. M. Waghmare

Abstract In rural area, the photovoltaic system is augmented by additional resources like wind, diesel generator. Such systems are called hybrid energy systems and mainly used for supplying electrical energy to independent loads in small towns where the access of electricity is lacking. In this research paper, an analysis is conducted to examine the control strategy of a PV generator connected with the grid and facilitated with maximum power point tracking (MPPT) control unit. The DC-to-DC boost amplifier is used to increase the voltage at the output of photovoltaic (PV) generator to the required voltage at the converter input side. In addition, the boost amplifier enables the tracing of the efficient operating point of the PV panels which ensures the peak output power production. An Elman neural network (ENN) online trained controller is designed to track the effective and excellent/maximum operating point of the PV generator. Employing the developed ENN, a better steady state and stable response is achieved with reduced fluctuations near the maximum power point (MPP) in comparison with the perturb and observe (P&O) technique findings. The simulation results prevailed using MATLAB 2019a/Simulink exemplify the dynamic performance of the online trained intelligent ENN controller.

Keywords Photovoltaic systems · Maximum power point · Elman neural network · Backpropagation algorithm

1 Introduction

Non-conventional energy sources are attractive solution to the increasing trends in the prices of the fossil's fuels. Due to many advantages, PV generation has a distinguished place among all renewable energy sources and hence is paid a great attention. PV panels are made up of a number of PV cells that can be joined end to end or across

S. B. Patil (✉)
Department of Electrical Engineering, G. H. Raisoni Institute of Engineering & Technology, Pune, MS 412 207, India

L. M. Waghmare
Swami Ramanand Teerth Marathwada University, Vishnupuri, Nanded, MS 431 606, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_67

each other to convert energy of photons into electrical energy. The power vs. voltage (PV) characteristics of a PV source are nonlinear and depend totally on climatic conditions which cause variable power generation. Therefore, MPPT control unit must be associated with PV generator which forces it to operate constantly at optimum operating point. In literature studied, many researchers [1–3] have concentrated their studies on MPPT controllers aiming at efficiency optimization despite of continuous variations in climatic conditions. The general requirements of any MPPT controller are that it is simple and gives rapid tracking of MPP under changing conditions of weather, and it should have low cost and give small fluctuations in power. The different traditional methods to achieve MPP are Hill climbing method, perturbation and observation (P&O) method and incremental conductance method, but they do not have good tracking performance. Perturb and observe (P&O) technique is one of the extensively accepted MPPTs [3, 4]. A single simple neuron network with an online learning-based back propagating method is used in [1]. [2] proposes a Wilcoxon radial basis function (RBF) network with an online training methodology. For online training of the MPPT controller, the well-known backpropagation of the error gradient is used [5]. The work of this paper is organized in sequence: the mathematical modelling PV generator, DC-DC boost converter control scheme followed by the simulation results and conclusions.

2 The Structure of Proposed Online Trained Elman Neural Network MPPT Algorithm

2.1 PV Generator Modelling

A PV/solar cell is identified by an ambiguous current curve compared to a voltage (I vs. V characteristics) that may be reproduced using a 1- or 2-diode modelling. The main part of PV arrays structure is a solar cell, which is the only p–n junction diode that directly converts light energy into electrical energy. Its equivalent circuit is shown in Fig. 1. Ideally, it can be shown by a current source in shunt with a diode.

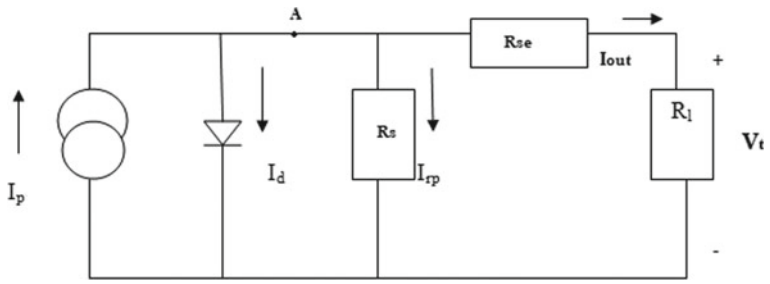


Fig. 1 Two-diode basic circuit of solar cell

But nothing is ideal, and hence, ideal solar cell equivalent diagram is modified by inserting series and shunt resistances to it. *Rs* is called series intrinsic resistance having very small value, and *Rp* is called shunt resistance having very high value.

$$I_{out} = I_p - I_o.\left[\exp\left(\frac{V_t + IR_{se}}{V_T}\right) - 1\right] - \left[\frac{V + IR_{se}}{R_s}\right] \tag{1}$$

where

Ip = photon current,

I_{out} = solar cell current,

I_o = reverse saturation current,

V_t = solar cell output voltage,

R_{se} = series intrinsic resistance,

R_{s} = shunt resistance,

V_T = thermal voltage $\left(\frac{Kt}{q}\right)$, K is Boltzmann constant, t is the temperature (Kelvin),

q = charge of an electron.

The efficacy of a solar cell is given in terms of ratio of maximum power to solar input power.

Simplification of PV array by mathematical model is represented by the following equation:

$$I_{out} = n_p I_p - n_p I_{rs}\left[\exp\left(\frac{q}{KTA} \times \frac{V_t}{n_s}\right) - 1\right] \tag{2}$$

2.2 DC-DC Boost Converter Control Scheme

To increase the final power at the output of the PV generator to the desired value at the on-input side of inverter, DC-DC amplifier/converter is used. In addition to this, it makes the tracking of efficient PV point for high power production. The most commonly known MPPT algorithm is the perturb and observe algorithm which is fine and known. But in P&O algorithm, the operational point oscillates near the MPP in stable state, and ultimately, it gives rise to the waste of some amount of available energy. In this work, an intelligently instructed Elman neural network (ENN) is presented [2, 6] to specify a PV power reference corresponding to the appropriate PV source optimum operating point. The improved type of the online trained ENN used the MPPT controller approved by Ref. [2], depends on the concept of the P&O findings. The primary goal is to control and improve the effective tracing of the commonly employed P&O algorithm in terms of converging rate and power variations.

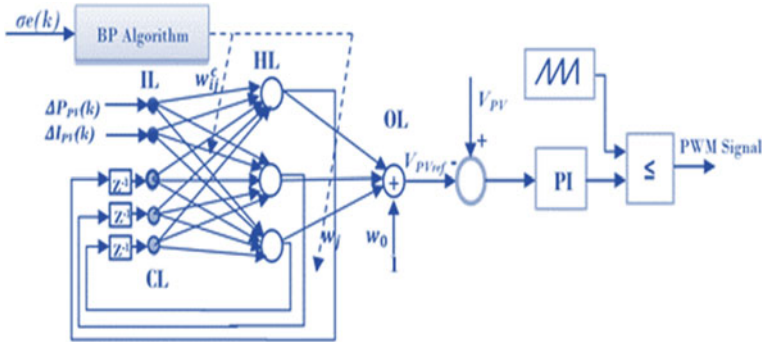


Fig. 2 Schematic of the ENN for the MPPT controller of PV source

As manifested in layout of Fig. 2, the ENN controller input is a change in the PV output current ($\Delta I_{\mathrm{PV}\,(k)} = I_{\mathrm{PV}\,(k)} - I_{\mathrm{PV}\,(k\text{-}1)}$) and the output power variant ($\Delta P_{\mathrm{PV}\,(k)} = P_{\mathrm{PV}\,(k)} - P_{\mathrm{PV}\,(k\text{-}1)}$) While the output is a V_{pvref}, i.e. PV voltage reference. The variation between the rated values and the reference values of the voltage error is also supervised by the PI controller which creates the control output via PWM, of the reinforcement converter as shown in Fig. 2. Basically, ENN is a biased recurrent neural network that comprises four layers, namely input layer (I), hidden layer (II), context layer (III) and output layer (IV) labelled as IL, HL, CL and OL in schematic diagram depicted in Fig. 2.

Main function of each layer of proposed ENN structure [2, 6] is explained with the help of the following equations:

The neurons in the input layer mediate the input signals into the hidden layer, such that

$$\begin{cases} Y_i^{(I)}(k) = G_i^{(I)}\left(m_i^{(I)}\right) = m_i^{(I)}(k) = X_i(k), i = 1, 2 \\ X_1(k) = \Delta I_{PV}(k),\ X_2(k) = \Delta P_{PV}(k) \end{cases} \tag{3}$$

where

E_i = input of ith neuron in the input layer

$G_i^{(I)}$ = the activation function of the ith neuron in the input layer

$Y_i^{(I)}$ = output of the ith neuron in the first layer

$m_i^{(I)}$ = activation level at apex/node i

The output at every hidden junction in the hidden layer is calculated as

$$Y_j^{(II)}(k) = G_j^{(II)}\left(m_j^{(II)}\right) = G_j^{(II)}\left(\sum_r Y_s^{(III)}(k) + \sum_i w_{ij}^c Y_i^{(I)}(k)\right),$$

$$i = 1, 2 jets = 1, 2, 3 \tag{4}$$

$Y_j^{(II)}(k)$ is output of jth node of the hidden layer, $G_j^{(II)}$ is the activation function, and the $\left(m_j^{(II)}\right)$ is the activation level of the jth node of the hidden layer. w_{ij}^c is the weight between the ith neuron of the input layer and the jth node of the hidden layer, and $Y_s^{(III)}(k)$ is the output of the neuron 's' of the context layer. For the hidden nodes, we have used the tangent-sigmoid activation function. The derivative of this activation function is calculated as

$$Y_j^{(II)} = G_j^{(II)}\left(m_j^{(II)}\right) = \frac{2}{1 + e^{-m_j^{(2)}}} - 1 \Rightarrow G_j^{(II)}\left(m_j^{(II)}\right) = \frac{1}{2}\left(1 - \left(Y_j^{(II)}\right)^2\right) \tag{5}$$

The outputs of hidden nodes get pass on as the inputs to the context layer, where

$$Y_s^{(III)}(k) = Y_j^{(II)}(k-1),\ jets = 1, 2, 3 \tag{6}$$

Then, final result of the ENN is determined as given below:

$$Y_0^{(IV)}(k) = G_0^{(IV)}\left(m^{(IV)}\right) = G_0^{(IV)}\left(w_0 + \sum_j w_j Y_j^{(II)}(k)\right) = V_{PVref},\ j = 1, 2, 3 \tag{7}$$

Activation function at the output point is sigmoid, $G_0^{(IV)}$. w_j—synaptic weight linking with the jth neuron of the hidden layer into the output junction. W_0—the bias of the output neuron.

Transfer function of the output node is sigmoid, whose derivative is calculated as

$$\begin{aligned} Y_0^{(IV)} &= G_0^{(IV)}\left(m^{(IV)}\right) = \frac{1}{1 - e^{-\alpha m^{(IV)}}} \Rightarrow G_0^{(IV)}\left(m^{(IV)}\right) \\ &= \frac{\alpha e^{-\alpha m^{(IV)}}}{\left(1 - e^{-\alpha m^{(IV)}}\right)^2} = \alpha Y_0^{(IV)}\left[1 - Y_0^{(IV)}\right] \end{aligned} \tag{8}$$

where α is a positive constant.

For the online training of the MPPT controller, backpropagation gradient descent algorithm for gradient [1, 2, 5] is utilized in this work. As regards to the gradient descent rule [1, 5, 7], ENN adapts the weights, and these laws of adaptation are given below:

$$\begin{cases} w_{ij}^{c}(k+1) = w_{ij}^{c}(k) - \mu \frac{\partial \sigma_e(k)}{\partial w_{ij}^{c}} + a\left(w_{ij}^{c}(k) - w_{ij}^{c}(k-1)\right) \\ w_0(k+1) = w_0(k) - \mu \frac{\partial \sigma_e(k)}{\partial w_0} + a(w_0(k) - w_0(k-1)) \\ w_j(k+1) = w_j(k) - \mu \frac{\partial \sigma_e(k)}{\partial w_j} + a\left(w_j(k) - w_j(k-1)\right) \end{cases} \tag{9}$$

$\mu \& a$ are the learning rate and the momentum factor, respectively. The concurrence speed of online learned algorithm is affected by learning measure insignificantly. There, a large rate of learning refers to the speed of integration quickly but with more system sensitivity where there is disruption, and vice versa. To improve the effective performance and robustness of the designed ENN controller, choice of a flexible learning scale is the best option. The formula of the variable learning factor at kth iteration is recommended in Ref. [7] and improved here as follows:

$$\mu(k) = \left[\frac{\mu_{\max} - \mu_{\min}}{2} \left(\frac{1}{1 + e^{-(\alpha' \delta_k)}} + 1 \right) + \mu_{\min} \right] \tag{10}$$

where $\mu_{\max} \& \mu_{\min}$ are the higher and lower limits of the learning coefficient, respectively, and α' is a constant. γ_k is described as $\delta_k = \frac{\omega_c}{\omega_c + s} \sigma_e(k)$ where ω_c is the low-pass filter cut-off frequency. To ensure the rapid integration speed of the BP algorithm, automatic alteration of the μ at the time of learning process is required. This removes static error and power oscillation during stability. $P_{\mathrm{PV}}(V_{\mathrm{PV}})$ curve of the PV source has the slope $(\mathrm{dP_{PV}/dV_{PV}})$, and it is equal to zero at MPP under given climatic situation. Ref. [1] author has identified the main use of the learning process of the neural-based MPPT in respect of the PV graph slope as $e_p(k)^2/2 = (0\text{-}(\mathrm{dP_{PV}/dV_{PV}}))^2/2$. Here, the performance indicator $\sigma_{e(k)}$ which is adopted for the training of the validated ENN in online mode is revealed as the quadrature error surface:

$$\sigma_e(t) = \frac{e_s(t)^2}{2} = \frac{\left(e_p(t) + C_1 \int e_p(t) dt\right)^2}{2} \tag{11}$$

Such that

$$e_p(k) = \left(0 - \frac{\Delta P_{PV}}{\Delta P_{PV}}\right) = \frac{P_{PV}(k) - P_{PV}(k-1)}{V_{PV}(k) - V_{PV}(k-1)} \tag{12}$$

c_1 is a constant which is positive. This selection of $\sigma_e(k)$ aims at enhancing the characteristic of the stable state of the proposed controller by preserving the error function $\sigma_e(k)$ equal to zero.

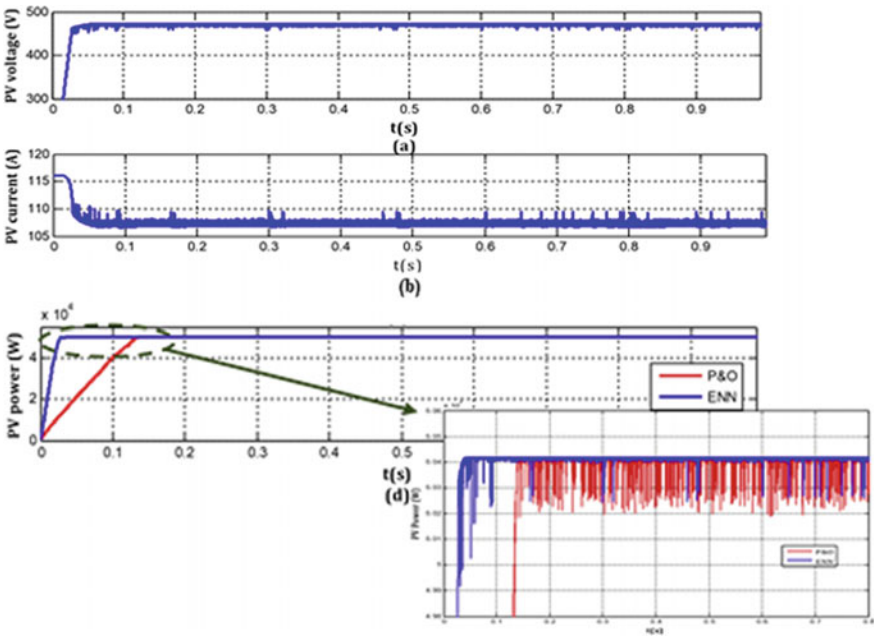
ENN MPPT controller block is implemented in MATLAB/Simulink. An example of implementation of an online measurement of the weights of the extraction layer is studied, and the results at various weather conditions are taken.

3 Simulation Results

To ensure the operation of the online trained ENN controller, various weather conditions are taken into account using the MATLAB 2019a/Simulink software. In the results, proposed MPPT is modelled and tested for climate change and variable load requirements. The following simulation tests in various scenarios are performed as follows:

3.1 Variable Load Situations

First test is conducted under constant weather conditions (temperature T-27 °C, solar irradiance $G = 1000$ W/m^2) and variable load conditions, where the initial SOC level of BEES which is used for backup was moderate (SOC initial = 70%). As shown in Fig. 3, the point of maximum output of the PV is quickly achieved using an Elman neural network controller which has been taught online after a small feedback span (approximately 0.0325 s) which found less as compared to the normal P&O controller (approximately 0.138 s).



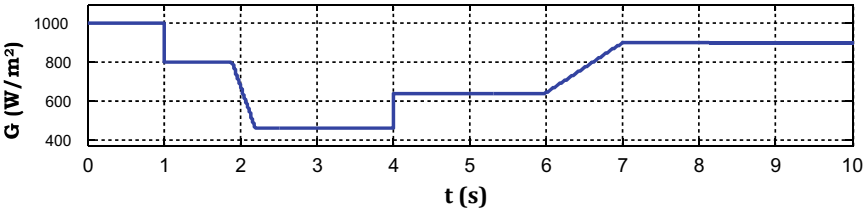
(c) Output power: comparison between P & O and ENN algorithm

Fig. 3 Variation of voltage, current and power of PV under unchanged weather and variable load conditions

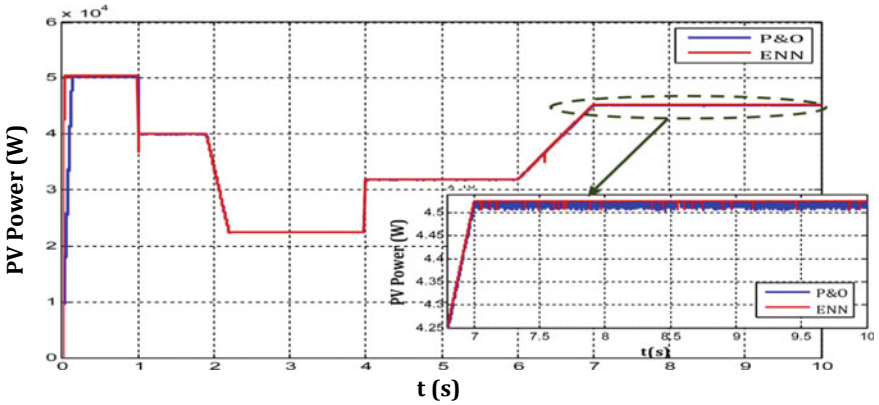
Also, the stable power variations found with the ENN controller significantly reduced compared to the perturb and observe tracker as shown in Fig. 3c.

3.2 *Variable Irradiation and Load Situations*

At a sustained temperature ($T = 25$ °C), the sun's rays vary during the experimentation as shown in Fig. 4a. Here, the proposed MPPT guarantee good tracking efficiency of changing radiation levels. At each level of sun rays, ENN finds the PV power reference accurately. Using the developed ENN, acceptable and stable condition is achieved by reduced variation near the MPP compared to the P&O algorithm (refer Fig. 4b).



(a) Solar insolation variation



(b) Output power: comparison between P & O and ENN algorithm

Fig. 4 Variation of irradiation and power of PV under variable irradiation and variable load

3.3 *Variable Temperature and Load Situations*

During third experimental simulation, the temperature slowly varied from 34° C to 27 °C and gradually decreased to 21 °C at constant insolation $G = 800$ W/m^2, as shown in Fig. 5a. Figure 5b shows the supremacy of the online trained ENN tracker when matched with P&O tracking during the short-term response and the stable condition.

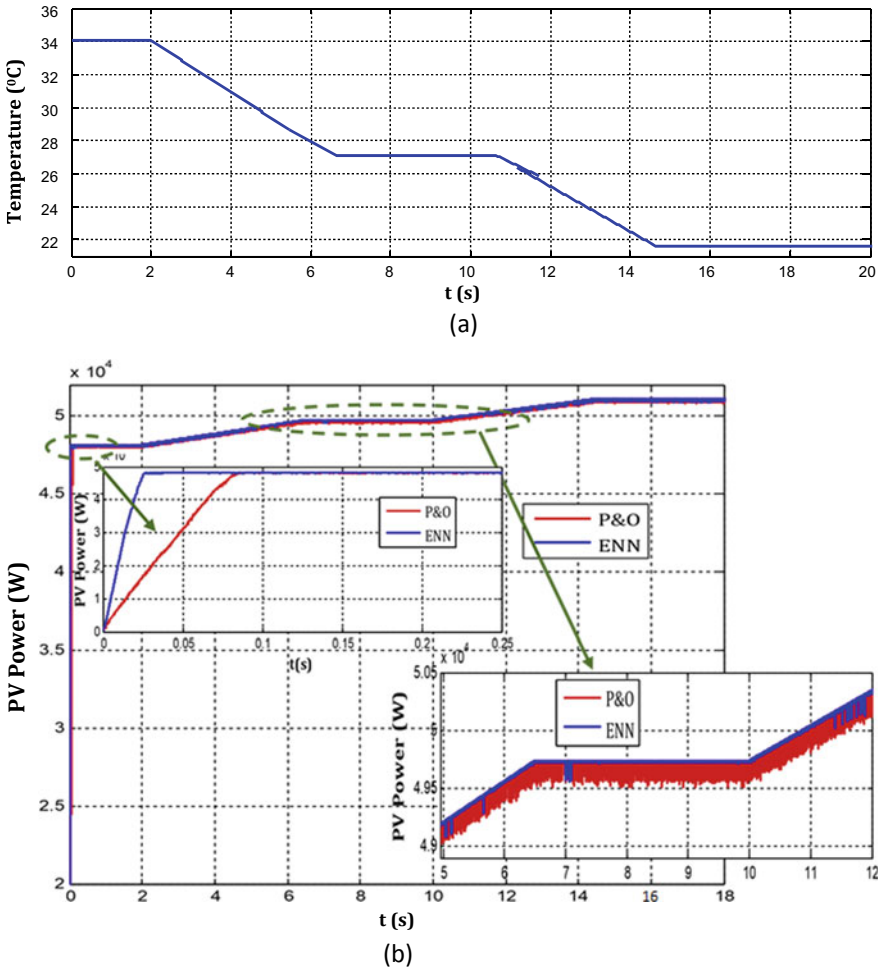


Fig. 5 Variations under variable temperature and load conditions: **a** Temperature, **b** PV power

4 Conclusions

In this paper, a smart DC-DC local controller for amplifying a voltage build on an artificial neural network is developed. The simulated model demonstrates the effectiveness of the control system adopted under changing weather conditions. ENNs-based PV online controller tracks MPP better compared to standard P&O MPP tracker. The automatic flexibility of the learning curve during online training ensures the fast integration rate of the backpropagation algorithm, and therefore, error and power fluctuations during steady state are eliminated. The simulation results show the efficiency and feasibility of an online trained ENN controller compared to the P&O controller.

References

1. P. Kofinas, A.I. Dounis, G. Papadakis, M.N. Assimakopoulos, An Intelligent MPPT controller based on direct neural control for partially shaded PV system. Energy Build **90**, 51–64 (2015)
2. C.M. Hong, T.C. Ou, K.H. Lu, Development of intelligent MPPT (maximum power point tracking) control for a grid-connected hybrid power generation system. Energy **50**, 270–279 (2013)
3. J. Ahmed, Z. Salam, A critical evaluation on maximum power point tracking methods for partial shading in PV systems. Renew. Sustain. Energy Rev. **47**, 933–953 (2015)
4. M.J. Khan, L. Mathew, Different kinds of maximum power point tracking control method for photovoltaic systems: a review. Arch. Computat Methods Eng. Springer (2016)
5. T.C. Ou, C.M. Hong, Dynamic operation and control of microgrid hybrid power systems. Energy **66**, 314–323 (2014)
6. F.J. Lin, Y.C. Hung, S.Y. Chen, FPGA-based computed force control system using elman neural network for linear ultrasonic motor. IEEE Trans Ind Electron **56**(4), 1238–1253 (2009)
7. W.Y. Han, S.M. Kim, S.J. Kim, C.G. Lee, Sensorless vector control of induction motor using improved self-tuning fuzzy PID controller, in *SICE annual conf* (FukuiJapan, 2003), pp. 3112–7

Automatic HTML Code Generation Using Image Processing



Shreya Khandekar, Shraddha Korade, Rutuja Kulkarni, Tejashree Pathak, and Satish Kamble

Abstract Outline of a website starts with creating models for each web page either by hand or using graphic design as well as expert model creation tools. Then the model is converted into systematic HTML or equivalent code by software engineers. This process is usually done frequently until the desired template is created. Our system will detect the text, input box, check box, buttons, etc. from the input image and convert it into Html code. To implement the proposed system, some deep learning methods are used. Any non-developer can create web pages using our system in a smaller amount of time with efficient results. 96% method accuracy and 73% validation accuracy will be achieved by the proposed system.

Keywords Object detection · Convolutional Neural Network · Deep Learning · Automatic code generation · HTML · Classification · Image processing · Machine Learning · Dataset · Cropping · Thresholding · OpenCV · Otsu's method

1 Introduction

The designing of a website begins with building models for each web page manually or using visual computerization and specified model development tools. Then models are transferred into systematic HTML or comparable labeled code by programming engineers. It's a common task for developers to transform a web page model into code [10]. This method is normally done frequently until the perfect desired design is created. Sadly, this procedure is complicated, time consuming, and tedious. Therefore, we present an approach to the code generation from mock-ups which will reduce time as well as be cost-effective. Some profound learning strategies like OpenCV and deep learning are used to actualize the proposed framework, i.e., an application that translates wireframe sketches directly into code. This application will have considerable benefits [10]:

- Faster iteration—a model can move to a website prototype with only the designer's involvement [10].

S. Khandekar (✉) · S. Korade · R. Kulkarni · T. Pathak · S. Kamble
Pune Vidyarthi Griha's College of Engineering and Technology, Pune, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_68

- Accessibility—allows non-developers to create web pages leading to the website [10].
- Removes the requirement of developers for initial prototypes, allowing developers to focus on the application logic rather than mundane GUI code [10].

2 Related Work

In [9], the authors used the MATLAB software tool for experimenting with morphological operations. Here morphological operations are used to remove the imperfections in the structure of the images. Most of the operations used here are dilation and erosion.

In [4], the author used parallel algorithms along with implementations on many core processors that enable high-quality and highly efficient image contour detection. They also explained in detail how one can use integral images to improve efficiency by replacing histogram construction with parallel prefix operations even under arbitrary rotations.

The author in [7], developed Animate Mobile Application User Interface. This application develops animate mobile applications using computer vision techniques. The P2A—generate user interface exhibits high pixel-to–pixel similarity with input screenshots.

In [6], the author used Otsu's algorithm based on improvement of the 2D histogram Otsu segmentation algorithm. This method is used to reduce noise and improve computing speed.

The author in [1], demonstrates the power of YOLO and it is used to detect interesting regions by training the network with single class and CNN is used to sub-classify and the solution also improves the quality of detection with minimum processing time.

In [8], the algorithm Reverse Engineer Mobile Application User Interface identifies user interface elements. The elements include image, text, container, and list through computer vision and optical character recognition techniques.

The author in [5], explained various Bootstrap framework tools, bootstrap typography, and how the framework allows us for rapid, responsive development.

3 Dataset

In this project, we have created our training dataset with HTML components according to sign conventions [10]. The sign conventions are simple shapes to make it easier for the user to create an input image. As our approach is supervised learning, labels/classes are provided for data. The classes in the dataset are as shown below in (Fig. 1).

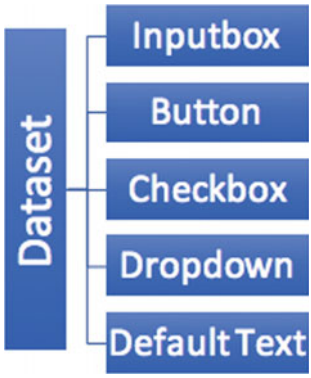


Fig. 1 Dataset

Our sampling dataset consists of images that contain multiple HTML objects drawn using sign conventions. It pertains to user input and will give webpage as output as shown in (Fig. 7).

4 Approach

The goal is to get the desired HTML web page as an output from mock-ups. To achieve this, we have to train our dataset for object detection using sign conventions in the input image. So, to find contour and detect the objects from the image given by the user, the image has to be converted to a binary image. Then, applying dilation on the binary image as shown in (Fig. 2) and finding the contours.

To convert it to a threshold image, we are using Otsu's method [6]. Detecting an object is done by selecting a region that has the same intensity in the image. Then the objects are contoured and their positional coordinates will be passed on to the next step. After taking coordinates of objects from the image and details about their

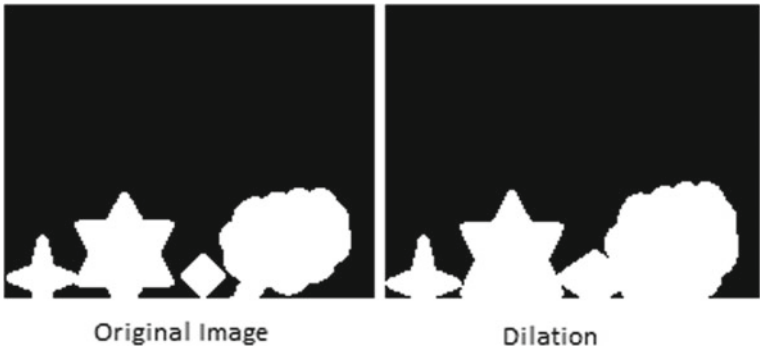


Fig. 2 Before and after dilation

exact location present in the image, that object is cropped and given to the model for classification. A label is assigned to the object, and it is stored in the HTML class. Our system is now prepared to create an HTML file for the corresponding input image and will store it along with project files.

5 Methods

To achieve the goal of this dissertation, we created and simplified it in three steps. In the first step, we will get a threshold image and will see how objects are detected and cropped. Classification of objects using our trained model will be done in the second step. In the last step, labels from classified objects will determine corresponding HTML code with help of the HTML builder algorithm. The output is as shown in (Fig. 8).

5.1 Object Detection and Cropping

After reading the input image, it is converted to a binary image using binary thresholding. Morphological operations are applied to it such as dilation and Otsu's thresholding. Otsu's threshold will separate pixels into two classes viz. background and foreground [6]. The output from this algorithm is a threshold image in binary form. Generally, this algorithm has black for the background, and white for the foreground as shown in (Fig. 3). This algorithm processes input and computes the threshold T.

After we get the image as above in (Fig. 3), objects are cropped. These cropped objects are then pre-processed for undergoing classification by model. For this, Keras preprocessing is used [2]. The cropped object is obtained as below in (Fig. 4).

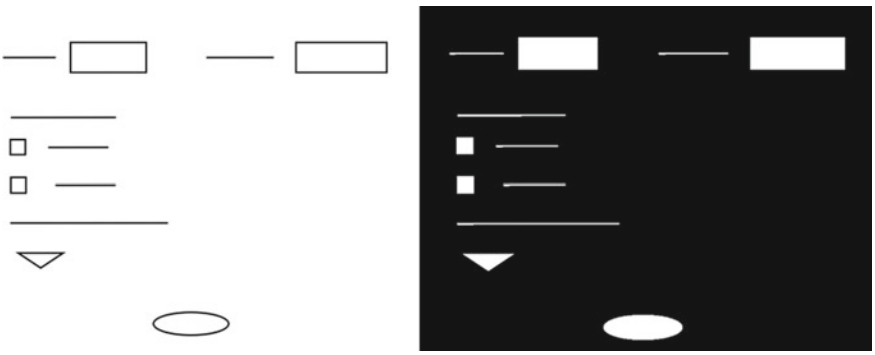


Fig. 3 Before and after thresholding



Fig. 4 Cropped Object

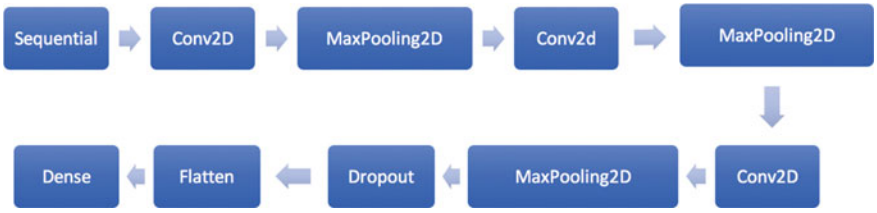


Fig. 5 Our Model

5.2 Object Classification

For model creation, our data is split into 80% training and 20% validation data. We have used data normalization to ensure that data from every class is trained properly. The images are trained in batches. Data prefetching has been used to train the model in less time. The activation function used is ReLU. We have used Adams optimizer due to its faster convergence. For loss estimation, categorical cross-entropy is used. Our trained model [11] as shown in (Fig. 5), is an image classifier that will identify HTML objects after cropping. After classifying the object, the returned label will be passed to the HTML builder algorithm for code generation.

5.3 HTML Code Generation

After obtaining labels for each object, HTML code will be generated by preserving the positional coordinates. To enhance the recognized components into corresponding HTML code and to make it interactive, we have used the bootstrap framework [5].

In the HTML builder algorithm, as shown in Fig. 6, we have created a header and footer section. Then, we detect how many objects are present in each row with the corresponding template code. Then we map the label of the object to the corresponding template code. In the end, the header, body, and footer section is combined. In this way, desired HTML code will be generated successfully.

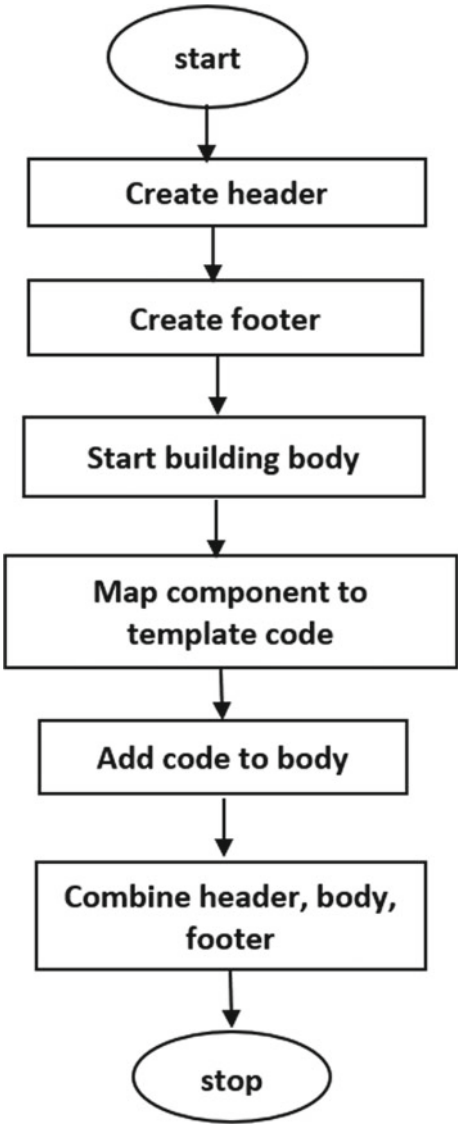


Fig. 6 HTML builder Algorithm

6 Results

In this study, the goal of generating automatic HTML code from mock-up images was successfully reached. For this, we had to perform three steps such as object detection and cropping, object classification, and HTML code generation.

In the first stage, morphological operations were carried out on images, and objects were obtained along with their positional coordinates, and their location information

was preserved for later use. These objects were cropped and pre-processed for further classification by our model. In the second stage, a label was assigned to each object where the label is the class of that object viz. input box, button, drop down, check box, and line for default text. Depending on preserved positional coordinates in the

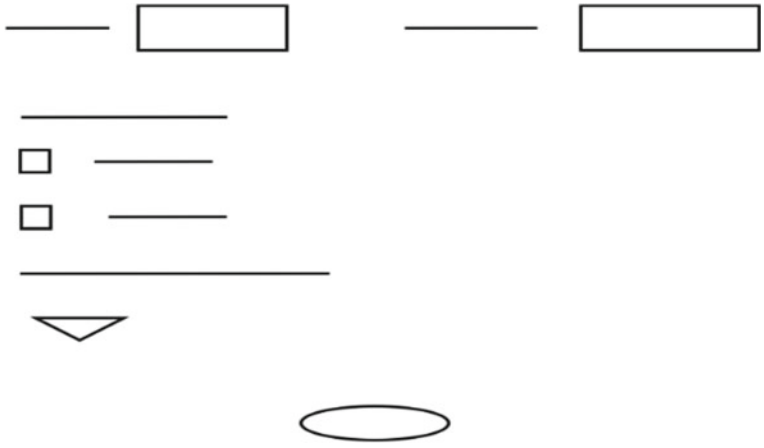


Fig. 7 Input image



Fig. 8 Generated Web Page

form of left, top, height, width, and label assigned by model, an HTML file was generated.

Given below is the result of how the HTML file will generate a web page as shown in (Fig. 8). With the usage of bootstrap, we have enhanced the layout. It can be improvised as required.

7 Conclusion

In this study, we have designed a system that converts sketches into corresponding HTML code. We have tried to convert the sketch into corresponding HTML code with minimum time and development cost. In this study, we have detected HTML components viz. input box, check box, button, drop down, and default text. Our system comprises not many limitations, but it is unable to detect the placeholders in the input box. As a result, we achieved 96% accuracy.

Our system has achieved the proposed task, i.e., creating a webpage and future scope can be linking these web pages to create the desired website. One more future scope can be of adding various frameworks to make the website look more interactive. The model can be trained for more features along with text detection instead of giving default text.

Acknowledgments The authors are indebted to Prof. Dr. S.A. Mahajan for his guidance, constant supervision, and for providing necessary information. We would also like to express our gratitude to Prof. S. S. Dixit who gave suggestions for this research work.

References

1. Algorry AM, Garcia AG, Wolfmann G.: Real-time object detection and classification of small and similar figures in image processing. In: International Conference on Computational Science and Computational Intelligence (CSCI), 2017
2. Aloysius N, Geetha M.: A Review on Deep Convolutional Neural Networks. In: International Conference on Communication and Signal Processing (ICCSP),2017
3. Aşıroğlu B, Mete EBR, Yıldız Y, Nalçakan A, Sezen M, Dağtekin T, Ensari.: Automatic HTML Code Generation from Mock-up Images using Machine Learning Techniques. In: Scientific Meeting on Electrical- Electronics & Biomedical Engineering and Computer Science (EBBT) ,2019
4. Catanzaro B, Su BY, Sundaram N, Lee Y, Murphy M, Keutzer K.: Efficient High Quality Contour Detection. In:IEEE 12th International Conference on Computer Vision,2009
5. Gaikwad SS, Adkar P.: A review Paper on Bootstrap Framework. In: Iconic Research And Engineering Journals IRE Journals Vol. 2, Page:349–351,2019
6. Lu C, Zhu P, Cao Y.:The segmentation algorithm of improvement a two-dimensional Otsu and application research. In: 2nd International Conference on Software Technology and Engineering,2010

7. Natarajan S, Csallner C.: p2A- A Tool for converting Pixels to Animated Mobile Application User Interface. In: IEEE/ACM 5th International Conference on Mobile Software Engineering and Systems (MOBILESoft) ,2018
8. Nguyen TA, Csallner C.: Reverse Engineering Mobile Application User Interfaces with REMAUI. In: 2015 30th IEEE/ACM International Conference on Automated Software Engineering,2015
9. Srisha R, Khan AM:Morphological Operations for Image Processing. In: National Conference on VLSI,2013
10. Robinson A.: Sketch2code—Generating a website from a paper mockup. In: University of Bristol,2018
11. Bai X, Yao C.: An End-to-End Trainable Neural Network for Image-based Sequence Recognition and its Application to Scene Text Recognition. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, Page:2298–230,2017

A Detailed Review on Text Extraction Using Optical Character Recognition



Chhanam Thorat, Aishwarya Bhat, Padmaja Sawant, Isha Bartakke, and Swati Shirsath

Abstract There exist businesses and applications that involve huge amount of data generated be it in any form to be processed & stored on daily basis. It is an implicit requirement to be able to carry out quick search through this enormous data in order to deal with the high amount of document and data generated. Documents are being digitized in all possible fields as collecting the required data from these documents manually is very time consuming as well as a tedious task. We have been able to save a huge amount of efforts in creating, processing, and saving scanned documents using OCR. It proves to be very efficient due to its use in variety of applications in Healthcare, Education, Banking, Insurance industries, etc. There exists sufficient researches and papers that describe the methods for converting the data residing in the documents into machine readable form. This paper describes a detailed overview of general extraction methods from different types of documents with different forms of data and in addition to this, we have also illustrated on various OCR platforms. The current study is expected to advance OCR research, providing better understanding and assist researchers to determine which method is ideal for OCR.

Keywords Optical character recognition · Data extraction · Data pre- processing · Segmentation · Classification · Post processing · Feature extraction · Neural networks

C. Thorat (✉) · A. Bhat · P. Sawant · I. Bartakke · S. Shirsath
MKSSS's Cummins College of Engineering for Women, Pune, India
e-mail: chhanam.thorat@cumminscollege.in

A. Bhat
e-mail: aishwarya.bhat@cumminscollege.in

P. Sawant
e-mail: padmaja.sawant@cumminscollege.in

I. Bartakke
e-mail: isha.bartakke@cumminscollege.in

S. Shirsath
e-mail: swati.shirsath@cumminscollege.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_69

1 Introduction

Businesses are expanding and updating as technology is advancing day by day making life and work easier to deal with. As this process tends to be a tedious task & data is in huge amount, it leads to excessive manual work. In order to automate this process of data collection and entry, Optical Character Recognition was introduced. It is used to recognize the text that is required to be extracted from scanned documents such as pdf, jpeg, handwritten etc. and convert it into machine readable text and store it in some target format. OCR allows this data to be quickly searched, edited, stored & displayed efficiently and that too digitally saving time as well as efforts. The capabilities of OCR provide endless possibilities throughout the entire industrial spectrum covering banking, healthcare, Education, Legal etc. thereby saving time and physical work required. Thus to gain insight from the data present in different kinds of documents and automatically extract the necessary data, OCR plays a key role and how it is done is thoroughly reviewed in the proposed paper.

2 OCR Process Flow

Building an OCR engine from the ground up is a step-by-step procedure that OCR professionals work on. The training process for an algorithm for efficient problem-solving with the use of optical character recognition typically involves six steps as shown in diagram (Fig. 1).

2.1 Image Acquisition

During the image acquisition phase, the recognition system collects a scanned image as an input image. The image must be in one of the supported formats, such as JPEG, PNG, or BMT. This image can be captured with a scanner, digital camera, or any other compatible digital input device.

2.2 Pre-processing

Pre-processing is a set of processes that are applied to the scanned input image. It basically, improves the image, making it segmentation-ready. In pre-processing, the image is subjected to a variety of activities. Binarization is one of them, which uses the global thresholding approach to convert a grayscale image to a binary image. The sobel technique is used to dilate the edges of the binarized image, and the image is

dilated and filled with holes in the final two phases to generate the segmentation-ready image.

2.3 Segmentation

During the segmentation stage, an image of a series of characters is divided into sub-images of individual characters. The input image is separated into discrete characters after it has been pre-processed. in the OCR system by employing a labelling procedure to assign a number to each character. The amount of characters in the image is indicated by this labelling. Each character is scaled to a standard size of 30×20 pixels.

2.4 Classification and Recognition

The decision-making stage of the OCR recognition system is the classification stage. This research employs a feed forward back propagation neural network to classify and recognise handwritten characters. The classifier is fed 600 pixels from the resized character in the segmentation stage. The neural classifier has two hidden layers in addition to an input and output layer. The log sigmoid activation function is used in the hidden layers, and the output layer is a competitive layer because one of the characters must be identified at all times. The output layer has a total of 26 neurons because the OCR system is designed to recognise English alphabets.

2.5 Post-processing

The post-processing stage is the final stage of the OCR recognition system. It computes the equivalent ASCII value using the test samples' recognition index and showcases the relevant identified characters in structured textual format.

3 OCR Methods

Many researches have been conducted in an attempt to recognize characters, forming varied combinations of techniques to achieve higher accuracy. The accuracy is dependent on multiple factors including quality of source, page layout, content type, OCR technique and various other factors. In some cases, pre-processing that involves eliminating shadows, background noises, adjusting skewness, etc. is a necessary

stage prior to OCR. Among a wide variety of methods [2] for performing OCR, the prominent ones are listed below.

3.1 Matrix Matching

A matrix is created for each character to find a particular pattern. This pattern is then compared with all the indexes of known characters. It is the perfect fit for one column layout document.

3.2 Fuzzy Logic

This strategy generates an output with multiple values in contrast to the binary values with only two values 0 or 1. Fuzzy logic signifies a more humanistic approach to logical thinking rather than binary-based computers. It makes an approximation between two characters to find similarities. An input with no noise is appropriate for this technique, for e.g. PDF document.

3.3 Extraction of features

Height, width, density, lines, loops, stems and some additional characteristics are the essential features involved in a character formation. Every character is constructed by mentioning presence or absence of these essential features. Mostly magazines, laser print, and high-quality images have such characters and hence this technique is useful there.

3.4 Structural Analysis

In this method, the image shape, sub-vertical and sub-horizontal histograms help to detect the characters. Structural Analysis has an exceptional potential to repair damaged characters. This makes it best suited for OCR on low-quality text and newsprints.

3.5 Neural Networks

Neural networks are based on human neural system. The pixels in an image are compared to an index of familiar character pixel patterns. Additionally, it has a great character abstraction capability ideal for faxed documents or distorted text.

Convolutional Neural network (CNN) and Long-short term memory (LSTM) [3] are some of the algorithms that help in recognition. Neural networks can be further utilized for analytical tasks.

4 Data Extraction from Specified Documents

As documents generated belong to different forms according to the need and usage, based on the research work done, this chronicle illustrates how data is extracted from the respective formats or type of document.

4.1 Exam Answer Sheets

The research paper [4] is a narrative of a unique approach for developing an automated, fast, flexible, and reliable system that can quickly recognize a student's enrollment number and related marks from an exam answer sheet and store it in a host computer. It makes use of hardware that takes each answer script's front page and processes it one at a time from the bundle. The entire procedure starts with preprocessing of the image which is captured by the Video Graphics Array (VGA) camera by using an adaptive noise removal algorithm, followed by the adaptive threshold for color detection algorithm which captures the roll number and marks from the answer sheet. The required data i.e. roll number and marks of the students are then passed on to the OCR system which converts it into a machine-readable format and generates an excel sheet of the same. As all educational organizations generate a large amount of student id and mark data, the proposed system helps reduce the manual work the staff is put through for the collection of marks from these exam sheets and saves up an adequate amount of time and effort required to do so. Integrating OCR will help enhance any Data entry system.

4.2 Print Bills and Invoices

The study [5] presents a methodology for extracting any data from printed bills and invoices, which may then be employed in machine learning or statistical analysis. It primarily focuses on extracting bill amount, schedule, date, and similar data in

order to obtain sufficient information about the user's purchases and transactions, as well as likes and dislikes. Initially, the invoice or bill from the image is first detected using the edge detection algorithm and then the unwanted noise from the image is filtered out before the text is extracted using Text Segmentation. Data in tabular format may be included in the bills or invoices. Automatically extracting data from tables is a challenging task in itself, mainly because tables being in diverse formats. These tables have no standard table design format, different table layouts, rows, columns, cell structure schemes (single, merged, etc.), content alignments, spacing, font sizes, etc. A large number of table detection algorithms are present that detect the table boundary and determine the table structure in a document. Apart from OCR other table detection methods are X–Y cut, tag classification, etc. Detection becomes difficult when there is no table border or outer ruling present. The results from the table recognition can be used to execute queries in the future.

4.3 Newspaper & Comics

This proposed system [6] detects and extracts the text in images automatically which has been collected from varied sources like newspapers, videos, ads, photographs, and checks. Text is detected using a multiscale texture segmentation approach, followed by spatial cohesion restrictions, clean-up, and ultimately extraction using a histogram-based binarization approach. A system for automatically evaluating performance is also proposed. The technique works well for standard documents as well as those with non-structured layouts or those with text written in shaded or textured conditions.

4.4 Multilingual Documents

The majority of accessible OCR engines are limited to a single language or a small number of languages. When different languages are present in a single text, additional challenges arise. Consider a document that has both English and Hindi text. As a result, the following processing stages are proposed for a typical multilingual OCR system:

- Binarization, layout analysis, and page segmentation are the first steps in pre-processing, followed by line finding and, if desired, word and character segmentation.
- Last but not least, feature extraction and classification or recognition.

This paper [7] also shows an automatic script identification methodology for documents, which is divided into two categories: segmentation-based and free techniques, depending on whether text lines are subdivided into finer units before recognition. To discover the best match, segmentation-based approaches break a text line into

a number of smaller units made up of characters or sub-characters and compare a combination of these units to likely lexical words. In contrast, segmentation-free OCR approaches, such as the left-to-right hidden Markov model, implicitly integrate character segmentation in producing a globally optimal character/word series as the recognition result (HMM). Different recognition modelling strategies can be utilized depending on whether a segmentation technique is segmentation-based or free.

5 OCR Platforms

With the introduction and expansion of computerised systems, many data scientists have attempted to solve the problem of OCR difficulties by developing a practical and efficient OCR engine that can produce accurate results. As we all know, there are a variety of OCR techniques and platforms accessible today, but we're just going to look at a few.

5.1 Google Docs OCR

It is easily available OCR facility proposed by Google within the Google Drive service where one can upload [9] an image file or a scanned document to Google Docs then it will automatically perform OCR on it generating an output file in any of the following formats such as PDF, ODT, TXT, DOC, RFT and HTML. Apart from that it also supports 30 languages.

5.2 Tesseract OCR

It's an open source OCR engine for a variety of operating systems. It includes an OCR engine called libtesseract as well as a command-line tool called tesseract. It also focuses on recognition with the addition of a new neural set (LSTM) based OCR service, Unicode (UTF-8) support, and the capacity to recognise over 100 languages. Tesseract supports a variety of output formats, including plain text, PDF, OCR (HTML), PDF with invisible text only, and TSV.

5.3 ABBYY FineReader

An international company named "ABBYY" designed and developed this OCR system which provides efficient OCR services. Prior to performing OCR on document, the program analyses the structure of the entire document and identifies

the region that comprises of the text or any images, tables and barcodes [8]. The results achieved through recognition are then displayed in the text window where unknown characters are emphasized in the window which helps the user to track down likely possible errors, figure them out and rapidly correct them within the software.

5.4 Transym

Another OCR solution that aids R&D organisations in obtaining precise and accurate information from digitised documents is Transym. The developed system is offered as an SDK with a high-level API, as well as a software package with a simple GUI that can be quickly installed and utilised.

5.5 I2OCR

It is a freely available online OCR tool which first extracts text from images and then converts it into text format which can be later edited, formatted, indexed, searched, or translated. The supports input images which are of following file types i.e. TIF, JPEG, BMP, PNG, GIF, PGM, PBM and PPM. It also supports more than 60 languages along with multi column analysis.

6 Future Work

OCR can read Screenshots supporting the information transfer between incompatible technologies, for example - .jpg and.docx. It is fascinating when combined with artificial intelligence to auto-extract information from scanned receipts to generate an expense report, or to translate a foreign language using a phone's camera. The future encompasses systems that first recognise the scanned text and then derives meaning from it. It can also facilitate development in the field of robotics. Robots comprehending text opens up a wide range of applications. Furthermore, OCR can be integrated in anti-viruses to catch viruses by detecting codes hidden in images.

7 Conclusion

There are many advancements in OCR that are still under development but this review paper discusses how data is automatically extracted from different types of documents be it an image or pdf, a handwritten document, multilingual documents,

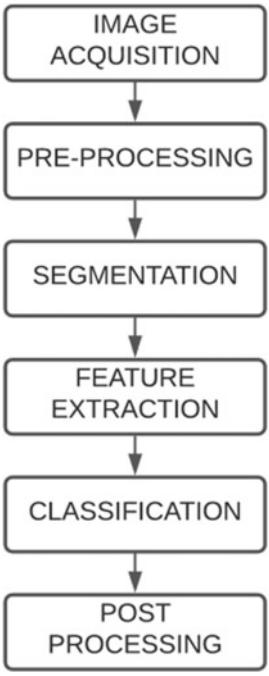


Fig. 1 Optical Character Recognition Process Flow [1]

invoices etc. using OCR. A generic methodology that goes in to make OCR work is also reviewed. The paper presents a brief survey of different OCR platforms that are available and have been used. This paper will act as a good guide for researchers preceding their study in the field of OCR.

References

1. J. Pradeep, E. Srinivasan, S. Himavathi, Neural network based handwritten character recognition system without feature extraction, in *2011 International Conference on Computer, Communication and Electrical Technology (ICCCET)*, pp. 40–44 (2011). https://doi.org/10.1109/ICCCET.2011.5762513
2. S. Singh, Optical character recognition techniques: A survey. (IJARCET) **2**(6) (June 2013)
3. R. Mittal, A. Garg, Text extraction using OCR: A systematic review, in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 357–362 (2020). https://doi.org/10.1109/ICIRCA48905.2020.9183326
4. D. Sharma, A. Sharan, H. Sharma, A. Agarwal, Data extraction from exam answer sheets using OCR with adaptive calibration of environmental threshold parameters, pp. 498–502 (2013). https://doi.org/10.1109/ICSPCom.2013.6719843
5. H. Sidhwa, S. Kulshrestha, S. Malhotra, S. Virmani, Text extraction from bills and invoices, in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 564–568 (2018). https://doi.org/10.1109/ICACCCN.2018.8748309

6. V. Wu, R. Manmatha, E. M. Riseman, Textfinder: an automatic system to detect and recognize text in images, IEEE Trans. Pattern Anal. Mach. Intell. **21**(11), 1224–1229 (Nov 1999). https://doi.org/10.1109/34
7. X. Peng, H. Cao, S. Setlur, V. Govindaraju, P. Natarajan, Multilingual OCR research and applications: an overview. *MOCR '13* (2013)
8. A. Mehdi, OCR as a service: A experimental evaluation of google docs OCR, Tesseract, ABBYY FineReader, and Transym. ISCV. Springer International Publishing AG, pp. 66 (2016) https://doi.org/10.1007/978-3-319-50835-1
9. S. Vijayarani, A. Sakila, Performance comparison of OCR tools. Int. J. UbiComp. **6**, 19 (2015). https://doi.org/10.5121/iju.2015.6303

Cyber Threats Landscape Overview Under the New Normal



Indraneel Mukhopadhyay

Abstract During the time of this pandemic, the dependency on Internet has increased manifolds. Employees are doing Work from Home, Students are Studying from Home, Teachers are teaching from Home, Everyone is shopping from Home and the list continues. All this has given rise to Cyber Security Vulnerability attacks like phishing attacks, malware attacks, ransomware attacks, social engineering attacks, identity theft, and a denial-of-service attack. This paper discusses the basic concept of cybersecurity and with a detailed review of recent cybersecurity attacks from January 2020 to March 2021 with a detailed analysis of motivation behind such attacks, attack techniques used, and targets of the attacks. This paper will also discuss cloud breaches, data breaches, and leaky buckets which have increased from 2021. The paper will discuss the types of cyber attacks, attack types, and targets of those attacks.

Keywords Cyber-attack · Cyber security · Data breaches · Leaky bucket

1 Introduction

Cybersecurity threats and breaches are taking away the sleep of Security Officers of the companies. They are not sure what kinds of attack, when and where will strike their network. Whenever we think of cyber attacks we can broadly classify it into three factors the spectacularity factor, the vulnerability factor and the fear factor. The spectacularity factor can be related to the impact factor of the attack that has been achieved on the targeted system. The impact can be financial loss, publicity loss for an individual or for the whole organization. An example of this impact factor is a Denial of Service (DoS) attack against any online service delivery platform business, which will result in stoppage of online service delivery and in turn lead to loss of substantial income. The vulnerability factor on the other hand is related to attacks on security system and security infrastructure. The fear factor plays on the attacker

I. Mukhopadhyay (✉)
Institute of Engineering & Management, Kolkata, India
e-mail: imukhopadhyay@iemcal.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_70

intention to create a sense of fear to its victim. Ransomware attacks have been one of the best methods to play fear factor on the government, organization or individual. Once the ransom has been paid the attackers decide whether to release the system or keep on going. The fear is always there with the victim. Nowadays all ransomware attacker uses cryptocurrency so that it becomes hard to trace.

Due to pandemic scenario change in working environment has seen increase in the motivation of cyber attack and also the target of the attack like government, healthcare facility and even pandemic research institutes [1]. If we take a survey 80% of the organizations do not spend enough budget on Threat Analysis and Prevention hence an overview threat landscape should give them the wake up call to do so. Though there was a 8% decline in global IT spending, the global spending for cybersecurity was increased to around 54.7 Billion US Dollar and its estimated that the spending will go up to 60.2 Billion US dollar compared to mere 40.8 Billion dollars I 2018 [2].

In this paper, we will compare the cyber security landscape of past few years and then we will compare it with pandemic scenario. We will also see how the motivation of a cyber security attacks' and its target have impacted our economy. We will also see major breaches that have happened in the Q1 2021 and its impact [3].

2 Comparison of Cyber Attack

As per a study conducted by AT&T most IT companies spend up to 10% of their IT budget on Cybersecurity [4]. This attracts hackers to attack the system. With the pandemic in employees working from home and login in to the company secure server it became a lucrative offer for all the hackers. What came was the never before seen threats to different sectors. If we compare the attack scenario of last three years, the per month attack has risen in 2020 and it is still on the rise. Figure 1 graphically shows the cyber attacks per month per year.

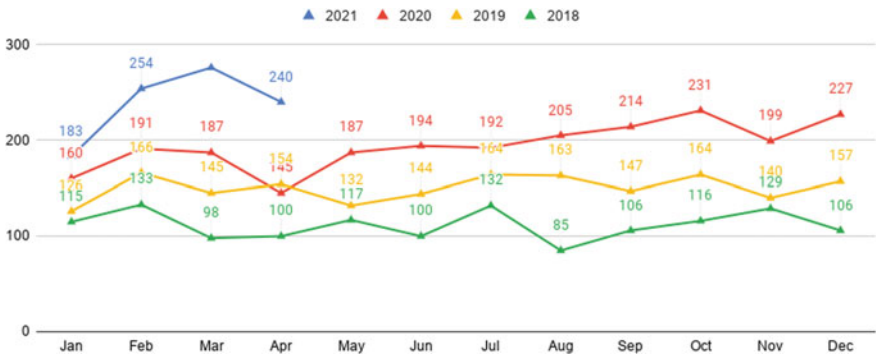


Fig. 1 Comparison of Cyber Attacks 2018–2021

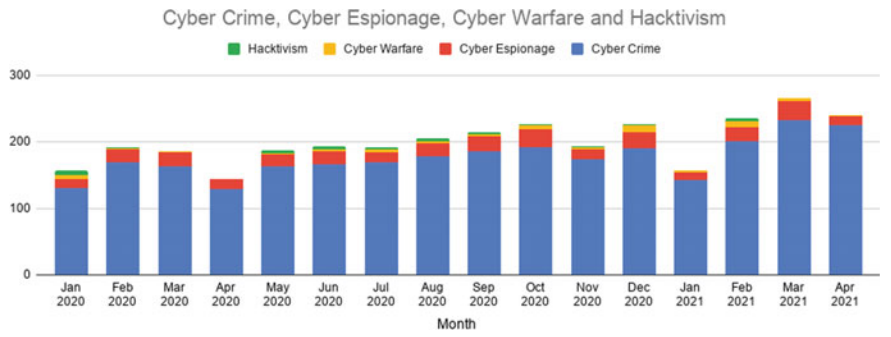


Fig. 2 What Motivates Hackers (2020–21)

Questions arises here that what is the motivation behind these attacks. As we have discussed in the earlier section the motivation behind cyber attack can be classified under spectacularity factor, the vulnerability factor and the fear factor. The other factors are cyber espionage, cyber warfare and Hacktivism.

Cyber espionage is a form of cyber-attack that steals classified, sensitive data or intellectual property data. The reason behind such a cyber attack is to make sure the victim which can be an organization or government entity losses their advantage. This data can then be sold to the highest bidder in the dark web. Cyber warfare uses current computer technology to disrupt the digital or online activities of the state or organization, especially when there is a deliberate attack on computer system for government, energy, strategic and military purposes. If strategic and military systems are compromised it can lead to the death of large number of people hence they are called Cyber Warfare. Hacktivism on the other hand is the act of hacking, or breaking into a computer system, for politically or socially motivated purposes. Example of Hacktivism in recent times are the operation #OpGeorgeFloyd, born after George Floyd was killed by police in Minneapolis in May 2020, amassed 8535 tweets in just three weeks. Some major hacks and cyber espionage of 2020 were like on July 15, 2020, more than a dozen high-profile Twitter accounts were commandeered by hackers who sent out tweets from the accounts of now President-Elect Joe Biden, Elon Musk, Bill Gates, Michael Bloomberg, Jeff Bezos, and others [5].

3 Comparisons of Cyber Attack Types and Target Industries

Before the Covid19 turned our life upside down the Industry was looking for an increase of cyber attack in the factor of 5 to 10% from the year 2019 to 2020 but little did we know the Covid19 scenario will create a tsunami of cyber attacks which took the advantage of the Work from the Home scenario. As the organizations were not ready with the new normal the organizations were forced to adapt protection protocol,

but not giving away precious data. In this paper we have taken into account the Top 10 attack types used by hackers and also its intended industry target of attacks. The following section graphically represents the same.

If we compare the different attack type's attacks that was used to compromise the system in the year 2020 and 2021 (Till April 2021) as shown in Fig. 3, we will see Malware was the highest followed by account hijacking, targeted attack, and vulnerabilities and so on. But if you look at 2021 vulnerability attack is on the rise. This is due to the fact the attackers are trying to access the vulnerability not only at organizational level but also at individual level via which they can get access to organization.

As we have seen the amount of cyber attack is on the rise we have to also see which are the different industries affected the most. Figure 4 shows the various targeted area of attacks. As clear from the graphical representation Individual have been attacked considerable compared to other heads like Public Administration, Education, Financial, Social Welfare.

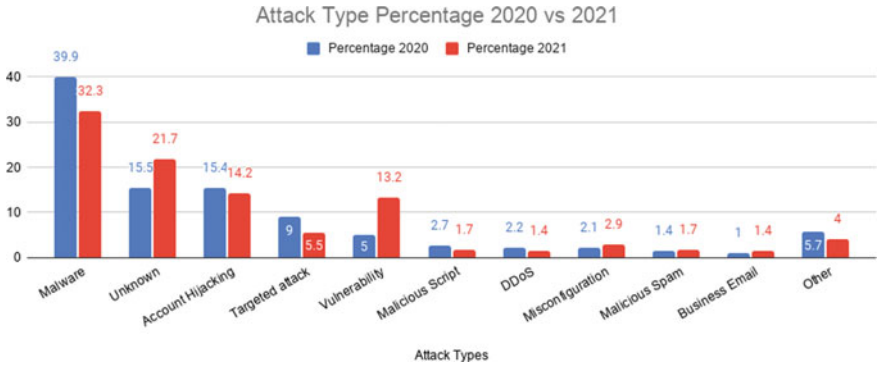


Fig. 3 Different Attack Type used



Fig. 4 Major Targets of Attacks

4 New Types of Threats in 2021

Threats are there but now the hackers have turned their attention to new types of attacks all due to the new normal. Due to the Work from Home scenario most of the organizations are trying to upload the data to the cloud so that the employees can login from anywhere and work. They do keep sensitive data on private network but the growth of cloud storage and work has risen considerably in the past one year. Due to this two major types of threats have become real. Cloud Misconfiguration threats.

4.1 Cloud-Native Threats

Cloud-native threats are action taken by malicious node via "Land" mechanism where attack is done taking into account the vulnerabilities in the cloud deployment by the organizations, without using an malware, Another mechanism is "Expand" where attacking of victim is achieved through the weakly or misconfigured or unprotected interfaces to locate classified and valuable data. Another method of attack is "Exfiltrate" where attack is done at data own storage location and is mostly done with the help of disgruntled employees. This is what is called an 'on-premises' attacks. Other methods by which a victim machine can be compromised is infecting the victim's machine with malware and then infecting in the network. These threats happen due to the prevalence of operating systems with well-documented vulnerabilities. In the cloud, there may not be a Windows, macOS, Linux, or even Android operating system to compromise. Attackers go after errors in configuration of the cloud and use stolen credentials for direct access for further increasing the severity of the cyber attacks [6].

The cloud native threats can be classified in four categories:

1. Delivery and Exploitation is the cloud service is exploited to deliver a malware strain or a phishing page e.g. Abuse Google Apps Script to steal credit cards from websites.
2. Actions on Objective is the cloud service is exploited to steal data, or launch other attacks e.g. ShinyHunters leaks personal information of over 20 million BigBasket user records,
3. Command and Control is the cloud service exploits attack the command and control infrastructure of the organization e.g. 30,000 MacOS endpoints New Silver Sparrow adware targeting Apple M1 Processors Exploited Service: AWS S3, and
4. Data Exfiltration is the cloud service is used as a drop zone for the exfiltrated data e.g. Multiple Targets Cybercriminals Target QuickBooks Databases Exploited service: Google Cloud Storage

Table 1 shows the different categories and percentage of attack. Figure 5 shows the graphical representation.

Table 1 Cloud Native threats and Percentage

Cloud Threat Categories	Percentage
Delivery and Exploitation	52.6
Action on Objectives	26.3
Command and Control	10.5
Delivery and Exploitation/Command and Control	5.3
Data Exfiltration	3.5
Delivery and Exploitation/Action on Objectives	1.8

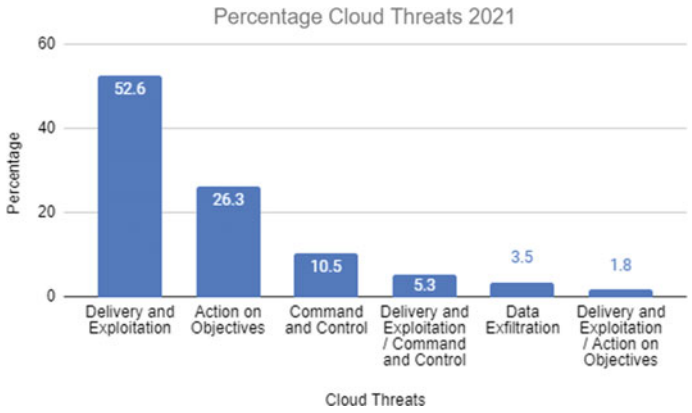


Fig. 5 Cloud threat Exploitation Categories

4.2 Leaky Buckets: A List of Cloud Misconfiguration Threats

Companies have been storing various types of data on the cloud, Over the last few years there have been multiple examples of leaky cloud services, exposing million of user records. This has been possible due to the victims are unaware, with can compromise the privacy of, or even lead to different kinds of attacks on the cloud infrastructure. For example two Magecart campaigns carried out compromising the AWS S3 buckets hosting the targeted sites' configuration files. And despite AWS S3 is the most common service to leak data, yet we use it [7, 8]. Figure 6 shows the leaky configurations percentage which leads to threats.

5 Data Breaches in Reported from India

Keeping the above number of threats that are looming above us, The Biggest Data Breaches that was there in India for the last 6 months is shown in Table 2:

The details of some of the major breaches in India in past 6 months:

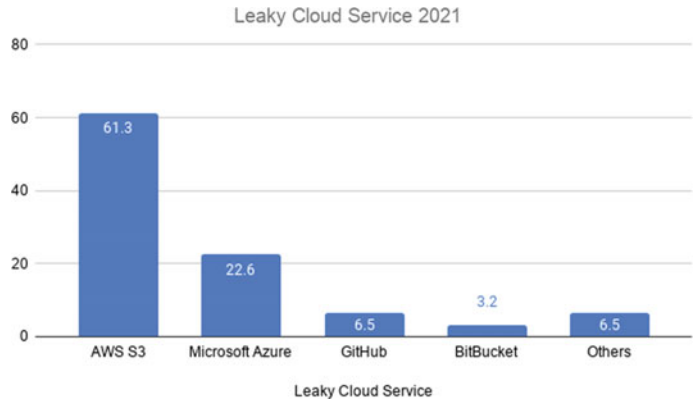


Fig. 6 Leaky Cloud Services

Table 2 Data Breaches from India

Date Reported	Date Discovered	Target	Target Class
25/04/2021	08/11/2020	BigBasket	Wholesale and retail trade
11/04/2021	–	Upstox	Financial and insurance
27/02/2021	Last week of February 2021	Zee5	Information and communication
02/02/2021	–	Airtel	Information and communication
29/01/2021	29/1/2021	(BPSSC)	Public administration and defence, compulsory social security

1. ShinyHunters leaked approximately 20 million BigBasket user records containing personal information and hashed passwords on a popular hacking forum.
2. Indian stock trading firm Upstox (Indian Stock Trading Firm) revealed that they might have given access to millions of customers' personal information due to Misconfiguration in their Server.
3. Zee5, an Indian OTT platform with over 150 million users data due to a security breach 9 million records have been leaked.
4. Personal details of 2.5 million Airtel customers were leaked by a hacker group 'Red Rabbit Team'
5. Database of 500,000 Indian citizens applied for Bihar Police Subordinate Services Commission (BPSSC) exam were discovered by CloudSEK.
6. The data of 35 million users from Juspay goes on sales in the dark web due to Cloud Misconfiguration

It is very clear from the description of the above breaches nothing is safe. In the last 6 months there have been around 46 major breaches, out of which 6 are from India amounting to **13%** of all breaches [9].

6 Conclusions

The 'New Normal' has made us think of security of digital devices that we thought we would never do. People have moved from free anti-virus software to anti-virus from McAfee or Norton for individual machines to security software's for organization. Software Vulnerability auditors are auditing the implementation to make sure it has been done correctly. But the hackers are always in the lookout to find the vulnerabilities. This paper gave a overview of type of vulnerabilities that have attacked the system in the last one and half year. In the interim, 15% may be "rubbed" with total data loss, resulting in a complete system reinstallation. To conclude, 5% of the devices will result in inoperability [10]. According to Data Breach Investigations Report, 60% of ransomware attacks are due to shareware software, which has been common in the new normal.

References

1. https://www.modernhealthcare.com/cybersecurity/hackers-taking-advantage-covid-19-spread-malware
2. https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/
3. M. Singh, I. Mukhopadhyay, Cyber Security Issues in the COVID-19 Times. Lecture Notes on Data Engineering and Communications Technologies **62**, 671–680 (2021)
4. Kim Crawley, Cybersecurity budgets explained: how much do companies spend on cybersecurity? May 2020
5. Michael Castellucio, 2020 Major Hacks and Syber Espionage. January 13, 2021
6. What Is a Cloud-Native Breach? mcafee.com/enterprise/en-in/security-awareness/cloud/what-is-cloud-native-breach.html#:~:text=Cloud-native%20breaches%20are%20a,and%20"Exfiltrate"%20that%20data%20to
7. Paolo Passeri, https://www.hackmageddon.com/about/ 2021
8. Top cybersecurity facts, figures and statistics for 2020 by Josh Fruhlinger, March 2020
9. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
10. https://cio.economictimes.indiatimes.com/news/digital-security/cyber-security-amidst-the covid-19-outbreak/75172086

Vulnerability Analysis of Bluetooth Technology for Defensive Application



Swapnil Sutar, Kishore Malladi, Priyanka Mekala, and Supriya Goel

Abstract Bluetooth technology operates on industrial, scientific and medical (ISM) unlicensed band which is an open wireless medium. Such radio waves are susceptible to various wireless attacks. Major smart devices manufacturers have integrated the Bluetooth with their latest smart devices to form a wireless personal area network (WPAN) with enhanced data rate (EDR) support. This paper demonstrates powerful open-source tools with its experimental set-up to exploit the vulnerabilities in Bluetooth technology. The collected results from each tools are analysed to identify and map the illegitimate device in the vicinity of legitimate areas.

Keywords Bluetooth · Ubertooth · GATT services · Mapping · Identification · Vulnerabilities

1 Introduction

Recent research in the area of Internet of Things (IoT) depicts that BLE-based devices are widely used in its infrastructure. These devices could be mobile phones, smart cameras, smart bulbs, sensors, smartwatch, etc. Moreover, these devices have less resources and tiny size. Internet connectivity to these devices provides access for fraudulent sniffing of the device owner's sensitive information. In the scenario of military base camp, secrete agencies and related government organizations, it is mandatory to detect the unauthorized peripherals to avoid their fraudulent data sniffing. Such activities are threatening towards the military agencies, industries and government organizations.

The aim of this paper is to address the intelligent solution in order to thwart data sniffing technique over BLE/Bluetooth frequencies. Various open-source tools are analysed for Bluetooth technology described in this paper with the focus of packet analysis. This analysis can be adopted for mapping the Bluetooth services and characteristics that ultimately leads to peripheral identification. It allows recognizing

S. Sutar (✉) · K. Malladi · P. Mekala · S. Goel
C. R. Rao AIMSCS, Hyderabad Central University, Serilingampalle (m), Telangana500046, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_71

legitimate/illegitimate devices in the premises. The outline of our contribution is as follows:

- Examine and identify the open-source tools
- Methodology: capture and analyse the decoded services
- Device recognition using characteristics
- GUI: Design of a IoT node mapper.

This paper is divided into four primary sections. Section 3 focuses on fundamental technical aspect of Bluetooth, followed by Sect. 4 in which we analysed the latest Bluetooth devices for its fingerprinting and service mapping. A complete experimental set-up with specific hardware and software is demonstrated in Sect. 5. Section 6 concluded the research paper with results and discussions.

2 Related Work

In the heterogeneous environment of the Bluetooth network, varieties of smart objects are employed. A remarkable research is carried out to recognize these varieties of smart objects previously that are based on traffic pattern or features extracted from software used. Few research work shows that traffic or driver-level features can be used for fingerprinting users or operating systems show device identification using radiometric signatures known as PARADIS system. It uses modulation imperfections as features to identify 802.11 wireless transmitters. In addition, Franklin et al. in [4] use driver-specific exploit for fingerprinting the WLAN with any tampering of the device. However, these approaches which rely on features extracted from software cannot differentiate devices that use same drivers. Usually, the frame formatting and content are indistinguishable except for few eccentric features. Adopting sophisticated techniques like digital signal processing detects and monitors the ZigBee devices which co-exist with Bluetooth in open radio spectrum as demonstrated in [5].

Sometimes simple measurements from the traffic are collected and analysed using classifier like SVM presented in [6] that help fingerprint drivers. However, such algorithms need huge database for training and classification. To detect anonymous users, Pang et al. [7] use traffic-based classification. To achieve higher accuracy, this type of identification will need large volumes of traffic which makes it difficult to use for real-time processing. Few works by Chernyshev [8] also include specialized hardware to measure the signal level and classify objects based on transients as shown by B. Danev and S. Capkun et al. [9]. Such hardware-based approaches are expensive to deploy in large volumes. The paper by Huang et al. displays how to identify Bluetooth devices using the device temporal features like clock skew of chipset. This approach is effective but is limited to only master device identification and cannot identify slave devices of any Piconet structure. Moreover, it depicts a mechanism for unknown Bluetooth device identification via syntactic similarity. However, it does not effectively help to avoid spoofing or identification of malicious nodes.

3 Technical Aspects of Bluetooth

In a Bluetooth communication, the *advertisement* packets have been transmitted on channels 37, 38 and 39 by each device to declare their existence prior to *scan-response* request [1].

Bluetooth-based smart devices allow to operate with the predefined set of services defined as profile. Bluetooth profile consists of procedure for functioning the devices. This procedure is developed by Bluetooth spacial group and specifies that each device should support minimum one device. The devices with same Bluetooth profile are capable of establishing the connectivity. However, devices from different vendors can connect appropriately using Bluetooth profile.

A fundamental Bluetooth network is formed with minimum two devices where any device can be master/slave known as "Piconet". Figure 1 represents variety of networks which exist in master/slave configuration. Master always handles the connection with slave in Piconet. Two different slave devices cannot communicate with each other directly irrespective of network design. Maximum eight different slaves can be connected with the single master at once, whereas all the devices are in synch with similar hopping sequence [2].

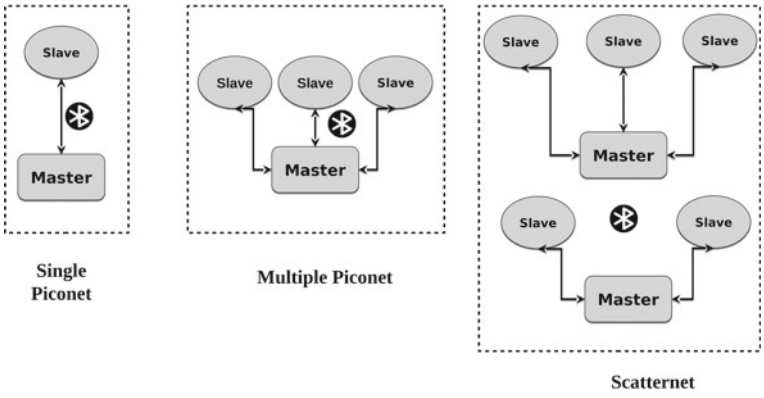


Fig. 1 Bluetooth Networks

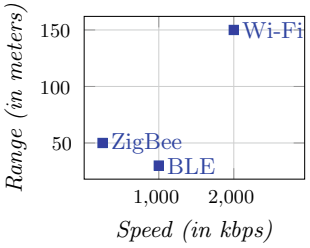


Fig. 2 Data rate versus coverage

Table 1 Short-range technologies

Technology	UWB (ultra wide band)	Wi-Fi	ZigBee	Bluetooth
Application	Indoor network	Network connectivity	Sensor network	Ad hoc network
Frequency band	3.1–10.6 GHz	2.4 GHz	2.4 GHz	2.4vGHz
International standards	No standards	IEEE 802.11b	IEEE 802.15.4	IEEE 802.15.1
Distance (physical range)	More than 100 m	50–150 m	10–30 m	10–50 m
Security	Time hopping spread spectrum	WPA PSK	AES—128	AES—128 / PIN

Table 1 represents the comparison of various short-range wireless technologies that have similar usage as Bluetooth. Other short-range wireless technologies have their own design-oriented limitation. That means application dominates the selection of wireless technology. For example, ZigBee creates a network with 65000 devices, whereas Bluetooth supports maximum eight devices per node at a time.

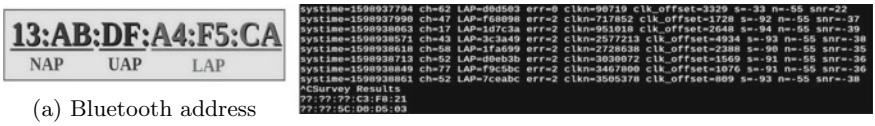
The data transfer rate with the coverage of three popular indoor technologies is plotted in the graph as shown in Fig. 2. It is found that the ZigBee is similar to Bluetooth with respect to range, whereas data rate of ZigBee is less. The unlicensed spectrum and cost effectiveness are main advantages of Bluetooth over ZigBee. However, Wi-Fi technology requires routers which is not mandatory in BLE/Bluetooth applications. In other words, the Bluetooth installation is easy and does not require coordinator/master.

Bluetooth device address (shortly known as BD_ADDR) is assigned to each Bluetooth node by its manufacturer. It is 48-bit wide represented in byte format separated by semicolon, e.g. 13:14:ae:ef:ad:27. Figure 3a represents the Bluetooth address structure divided into three unique parts as follows:

- **Non-significant address part(NAP)**: The 16 bits of data are used in hopping and frame synchronization.
- **Upper address part(UAP)**: The next 8 bits of data specify the Bluetooth algorithm used for connectivity.
- **Lower address part(LAP)**: These 3 bytes are vendor-assigned data to a device in order to identify the access codes uniquely.

The NAP and UAP collectively form organizationally unique identifier (OUI)[1] which is cumbersome to compute compared to LAP. Few upper address part(UAP)s and lower address part(LAP)s are captured and recorded in real time depicted in Fig. 3b. In addition, channel number (`ch`), clock offset (`clk_offset`), signal strength (`s`) and signal-to-noise ratio (`snr`) are recorded for BLE devices in the vicinity .

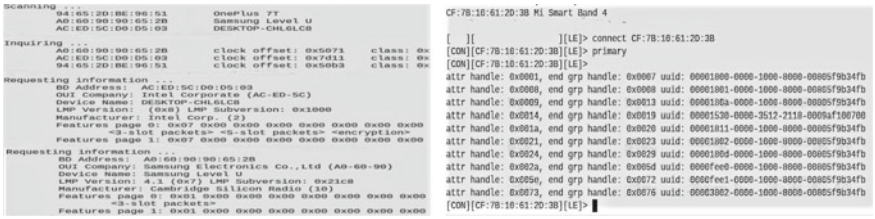
[1] http://standards-oui.ieee.org/oui.txt.



(a) Bluetooth address structure

(b) Real Captured Devices and its UAP+LAP

Fig. 3 Captured devices and its address structure



(a) Bluetooth configured devices using `hcitool`

(b) Decoded services of `MI Band 4` using GATT-TOOL

Fig. 4 Real-time Bluetooth decoding

4 Bluetooth Fingerprinting and Service Mapping

HCITOOL is a software-based human–computer interaction tool used to configure Bluetooth/BLE devices. This tool is adopted for analysis of Bluetooth protocol with help of on-chip Bluetooth hardware. This tool scans, inquires and provides the information about the devices in the vicinity, e.g. `OnePlus 7T, Samsung Level U, DESKTOP-CHL6LC8`, and its corresponding Bluetooth addresses are captured as shown in Fig. 4a. User-defined device's names are revealed, but category is unknown.

GATT-TOOL is a built-in tool available with various debian-based operating system. However, this tool is utilized to read/write the GATT services of connected BLE devices. The various decoded `MI Band 4` device services from collected packets using GATT-TOOL are shown in Fig. 4b. Table 2 represented the significance of decoded UUID using GATT Tool.

BlueHydra[2] tool is developed based on the `bluez` library, and it requires Ubertooth hardware to track both LE/LL and classic Bluetooth protocols. Technically, the services are captured and decoded to find the parameter such as Bluetooth version, addresses, received signal strength indicator(RSSI), user-defined names, manufacturer and type (or category) of the BLE devices as depicted in Fig. 5. Received signal strength indicator(RSSI) and distance can be related using equation received signal strength indicator(RSSI) which provides location of detected device.

[2] https://github.com/pwnieexpress/blue_hydra.

Table 2 Decoding of UUID using GATT-TOOL

S. No.	16-bit (UUID portion)	Significance
1	1800	Generic access
2	1801	Generic attribute
3	180a	Device information
4	1811	Alert notification services
5	1802	Immediate alert services
6	180d	Heart rate services
7	fee0/fee1	Fitbit band
8	3802	Unknown

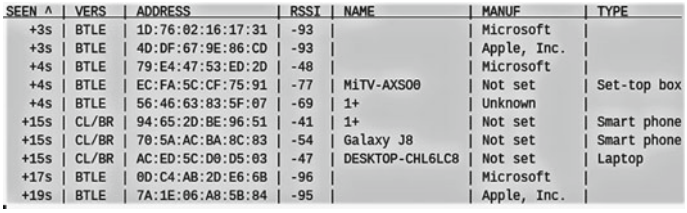


Fig. 5 BlueHydra Decoder

$$D = 10^{\left(\frac{P_{measured} - RSSI}{10 \times N}\right)} \tag{1}$$

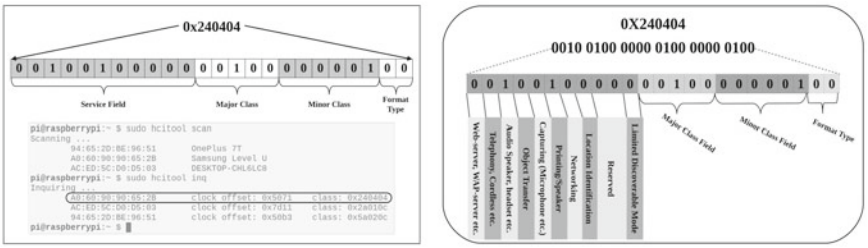
where $P_{measured}$: constant received signal strength indicator(RSSI) expected at 1 metre, D: distance and N: environmental factor (lies between 1 and 2). Mathematically, stability of received signal strength indicator (RSSI) is directly proportional to distance and power transmitted.

The format-type field usually consists of 24 bits (i.e. 23^{rd} - $0th$) where 0^{th} bit transmitted to air first. The first "00" bits in the CoD represent that it is a format-type field followed by information. Considering a example of "Samsung Wearable Headset", it shows the class of device as `0X240404`. The frame format of "Samsung Wearable Headset" with captured CoD/services is depicted in Fig. 6a.

The frame format showed that the major class value is `0X5`, means it is a audio/video speaker devices. Minor class for each major class is defined by Bluetooth Special Interest Group[3] which has value `0X1` pointing to "Wearable Headset" as shown in Fig. 6.

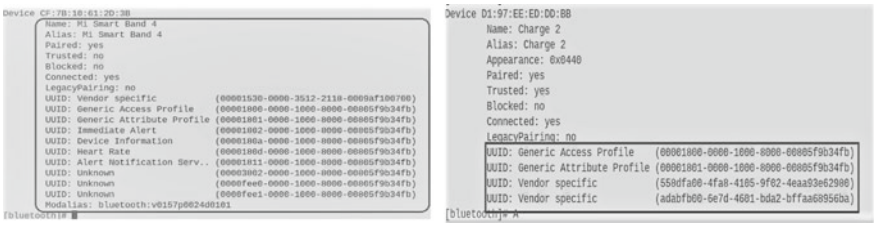
As per standard MA-L (MAC Address Block—Large) specified by IEEE, the first 3 octets, i.e. A0:60:90, are assigned to "Samsung Electronics co. ltd.". The combined information from MA-L and CoD is mapping the detected BLE device as a "Samsung Wearable Headset".

[3] https://www.bluetooth.com/specifications/assigned-numbers/.



(a) CoD/Service frame (b) Service bit fields

Fig. 6 Decoded CoD frame



(a) Decoded characteristics and services (MI Band 4) (b) Captured services on Charge 2 FITBIT

Fig. 7 GATT tool decoding

Further, BLE smart device creates an exclusive connection to the central node (i.e. master) via GATT (Generic ATTribute) profile. The GATT profile provides the request/response-based connection between devices using services and characteristics. Base UUID is represented as `0000XXXX-0000-1000-8000-00805f9b34fb` where `XXXX` is 16-bit value shows the specific services and characteristics of the captured devices (MI Band 4) as depicted in Fig. 7a, e.g. `180d` provides the information about heart rate in MI band 4.

5 Experimental Set-Up

In order to perform the experiment, Raspberry Pi (3B), Ubertooth and CSR 4.0 Dongle with specific software are used. Raspberry Pi from version 3 onwards offers in-built BLE/Bluetooth facility, hence CSR 4.0 dongle may be optional. The overall BLE testbed set-up is demonstrated in Fig. 8.

A specific prerequisite software, such as cmake, libusb, dev, make, pkg-config, libbluetooth-dev, Python3-NumPy, Python3-qtpy, gcc, g++, libbtbb & Ubertooth with btbredr (wireshark plug-ins) are essential, operates Ubertooth BLE sniffer.

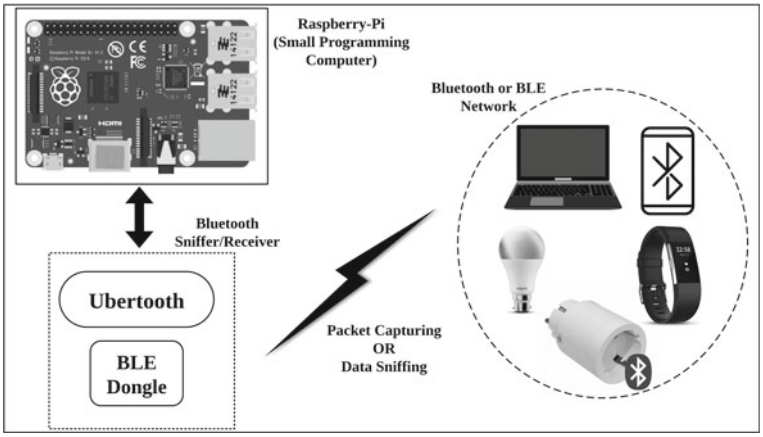


Fig. 8 BLE packet analysis testbed set-up



(a) Mapping SAMSUNG Headset (GUI) (b) Mapping Fit-Bit and MI smart band

Fig. 9 GUI-based mapping

Moreover, these various created databases are adopted by IoT node mapper to recognize BLE devices appropriately (Fig. 9).

6 Conclusion

The paper represents the collected result from various tools to exploit the Bluetooth. Collective result analysis highlighted significant metadata leakage which leads to expand the further attacks such as DoS, spoofing and hijacking in an offensive approach. This paper provides the generic approach to detect and identify illegitimate device to thwart sniffing in sensitive areas. This research work is limited to offline device tracking using node mapper which can be extended to real-time capturing.

References

1. P. Satam, S. Satam, S. Hariri, Bluetooth Intrusion Detection System (BIDS), in *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)* (2018), pp. 1–7. https://doi.org/10.1109/AICCSA.2018.8612809.
2. M. Tanriöven, K. Taşdelen, Establishing a mesh network with Bluetooth and investigating the range. Analysis. Mühendislik Bilimleri ve Tasarim Dergisi **8**(1), 12–19 (2020). https://doi.org/10.21923/jesd.522514
3. P.P. Ray, S. Agarwal, Bluetooth 5 and Internet of Things: potential and architecture, in *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)* (2016), pp. 1461–1465. https://doi.org/10.1109/SCOPES.2016.7955682.
4. F. Jason, M. Damon, T. Parisa, N. Vicentiu. R. Jamie, S. Douglas, Passive data link layer 802.11 wireless device driver fingerprinting (2006)
5. R. Zhou, G. Xing, X. Xu, J. Wang, L. Gu, WizNet: a ZigBee-based sensor system for distributed wireless LAN performance monitoring. IEEE Int. Conf. Perv. Comput. Commun. (PerCom) **2013**, 123–131 (2013). https://doi.org/10.1109/PerCom.2013.6526722
6. M. Mirza, P. Barford, X. Zhu, S. Banerjee, M. Blodgett, Fingerprinting 802.11 rate adaption algorithms, in *2011 Proceedings IEEE INFOCOM* (2011), pp. 1161–1169, https://doi.org/10.1109/INFCOM.2011.5934893
7. J. Pang, B. Greenstein, R. Gummadi, S. Seshan, D. Wetherall, 802.11 user fingerprinting, in *Proceedings of the 13th annual ACM international conference on Mobile computing and Networking (MobiCom '07)* (Association for Computing Machinery, New York, NY, USA, 2007), pp. 99–110. https://doi.org/10.1145/1287853.1287866
8. C. Maxim, An overview of Bluetooth device discovery and fingerprinting techniques—assessing the local context (2015)
9. B. Danev, S. Capkun, Transient-based identification of wireless sensor nodes. Int. Conf. Inf. Process. Sens. Netw. **2009**, 25–36 (2009)
10. J. Huang, W. Albazrqaoe, G. Xing, BlueID: a practical system for Bluetooth device identification, in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications* (2014), pp. 2849–2857. https://doi.org/10.1109/INFOCOM.2014.6848235.

A Recommendation System to Support the Student to Choose a Role in the College Election



Gayatri Bedse, Divya Ghorpade, Tejashri Gangurde, Shreya Kulkarni, and Swati Shirsath

Abstract Many AI/ML and data analysis-based recommendation systems are being used in various fields like education, e-business, and course selection to invoke the computerized intelligence solutions based on some basic knowledge of domain. In that role recommendations, course recommendations, job recommendations are also considered as one of the challenging tasks to do. Having this role recommendation system for the College Voting system or at university level voting system can be helpful. However, traditional voting needs to break the barrier and use new approaches to motivate students to vote in an effective way. The online voting system is one of the most important and convenient ways nowadays. So, choosing the correct responsibility and role for a candidate is also crucial. For this, the best solution is a recommendation system based on skills. This skill-based recommendation system which focuses on the abilities and interests of candidates and recommends the most suitable role to each candidate. Therefore, the system will illuminate the candidate's vision for selecting the role unambiguously. Finally, this paper presents an application scenario where the system analyzes and processes the data based on some inbuilt filters and presents the most appropriate solution.

Keywords AI/ML · Data analysis and processing · Candidate's skills · Role recommendation · Personalized analysis · Intelligence solution · Traditional voting · Inbuilt filters

G. Bedse (✉) · D. Ghorpade · T. Gangurde · S. Kulkarni · S. Shirsath
MKSSS's Cummins College of Engineering for Women, Pune, India
e-mail: gayatri.bedse@cumminscollege.in

D. Ghorpade
e-mail: divya.ghorpade@cumminscollege.in

T. Gangurde
e-mail: tejashri.gangurde@cumminscollege.in

S. Kulkarni
e-mail: shreya.shripad.kulkarni@cumminscollege.in

S. Shirsath
e-mail: swati.shirsath@cumminscollege.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_72

1 Introduction

System, which recommends things depending on some quality attributes and aspects of interest, is known as the recommendation system. There are various types of recommendation systems like collaborative filtering, content-based filtering, and hybrid filtering. In this paper, this paper is focusing on a content-based recommendation system. A content-based recommender works by the data that taken from the candidate explicitly; here data is skills that candidate selects, which is then used to suggest the roles to the candidate, as the candidate provides more input or takes more actions on the recommendation, the output becomes more accurate. Students have different types of skills and qualities, but it is not enough to just have the skills, and you must have to use them in the correct way to meet a certain task. For this, some search process is necessary to filter these skills. To achieve this, this paper presents you recommending role in an online voting system. This system applies filters to deliver appropriate roles for the candidate.

Considering this context, the motivation of this paper came when we noticed that some students are confused to choose roles as they have different skills. However, the traditional voting system has some basic procedures that need to be followed, and any small foul can cause a big effect on entire performance. To find the most relevant role, candidates must search the job responsibility for each role manually, and there is a huge uncertainty in getting the correct information causing more manual work to be done which tends to spend more time and energy on it. All these aspects tend to think about a system which will make the voting procedure more convenient and secure. The online voting system consists of a rule book, role registration, and online campaigning. Result displaying, email sending, role recommending. This paper focuses mainly on role recommendation to the candidate. This was perceived through the election conducted by MKSSS's Cummins College of engineering for Women, Pune. The college has a separate Student panel committee which includes various roles and responsibilities like operational secretary, cultural secretary, technical secretary, sports secretary, etc. For all these roles, it is observed that candidates must hold selective skills and qualities which helps them to carry out their responsibility effectively.

Analyzing the system used by students who participate in elections, they possibly need to categorize themselves into roles according to their skills and abilities. The student must search for the role duties, choose, and register for the role. Thus, the student ends up being responsible for analyzing their own skills and role duties, and if he does not know how to analyze and where to search, difficulties can hinder him. Thinking about it, this article describes a role recommender system, developed in a web platform, which recommends roles according to their skills/abilities. System provides personalized role suggestions to the candidate based on the individual's capabilities for handling that role. By using this system, students can get better at choosing the most suitable role for themselves.

2 Problem Formulation

The role recommenders are a way to encourage and motivate students to boost their confidence in the skill which they think they have. Because when entering a registration, participants see themselves engaged in a mission to prove their skills based on their knowledge. To analyze the required skills for each role in the election, a survey was conducted with the students of the previous panel members, from the MKSSS's Cummins college of Engineering for Women, Pune. It was applied through an online form designed into Google Drive Tool—Forms.

According to respondents, mostly the system works on manual registration, where the candidate chooses the role, submits registration form, and gets a confirmation message. Thus, the student himself is responsible for choosing the 'role,' and if he does not know how to work, the difficulties can hinder, because these systems do not have the concept of recommending the role. This can also cause demotivation because he can select an unsuited role regardless of his skills, thus causing a lack of interest toward his responsibilities. The results obtained from the survey were useful to verify the gaps in the previous and current system. Thus, the recommendation systems are useful to identify candidate's skills, save the choices and recommend roles, such as operational secretary, cultural secretary, technical secretary, sports secretary, etc. (Table 1)

Table 1 List of roles

S. No	Roles
1	Operations secretary
2	Cultural secretary
3	Technical secretary
4	Sports secretary
5	Treasurer
6	Editor
7	Magazine secretory
8	Library representative
9	Placement cell representative
10	Branch representative

3 Algorithm

```
X = { s1 ,  s2 ,  s3 ,  s4 ,  s5 , … }
Y = {(r1,r2):[s1,s2,s3,..],(r3,r5):[s1,s2,s3,...],...}
Z = {r1:[s1,s2,s3,...],r2:[s1,s2,s3,...],r3:[s1,s2,s3,
...],… }
Tot_Cnt = {r1:n1, r2:n2, r3:n3, ...}
Output = {r1:0, r2:0, r3:0, ... }
X_Cnt = len(X)

fun Role_Recommend( input ) :
    //Section_I
     temp1 = input ∩ X
     Val1  = len(temp1)
     Input = input − temp1

    //Section_II
     for i in Y.keys():
         temp2 = input ∩ Y[i]
         if temp2:
               for j in i:
                     Output[j] = Output[j] + len(temp2)
                     Input = input − temp2
  //Section_III
    for k in Z.keys():
         temp3= input ∩ Z[k]
         if temp3:
               Output[k] = Output[k] + len(temp3)

         //Section_IV
         Avg=((Output[k]+Val1)/(X_Cnt+Tot_Cnt[k]))*100
         Output[k] = Avg

  //Section_V
  Result_roles=Sorted(Cnt, key=Cnt.get, reverse=True)
  for p in range(3):
         print(Result_roles[p])
```

See Table 2.
e.g.,
Predefine data:
Skills:

$$X - s_1, s_2, s_3, s_4, s_5 \quad X_\text{Cnt} - 5$$

Table 2 List of variables

$s_1, s_2, \ldots$	Required skills
$r_1, r_2, \ldots$	Available roles
X	Set of skills required for every role
Y	Dictionary where key is referred as tuple of roles and values are their respective common skills
Z	Dictionary where key is referred as role and value is set of specific skills for that role
Tot_Cnt	Role-wise count of required skills
X_Cnt	Total number of skills in X set
Avg	Average percentage of role matching
Output	Store calculated Avg for each role

These are basic skills which are required for every role present in role list.

Group Skills (Table 3):

It is a key value pair where key is set of roles who shares similar skill requirements, and their corresponding values contain list of those required skills.

Individual Skills (Table 4):

It is a key value pair where key is individual available role/position, and value contains list of required skills for that specific role.

Total Skill Count (Table 5):

Table 3 Y(Elements)

Role combinations	Required skills for combined roles
r_1–r_5	s_6, s_7
r_3–r_4	s_8

Table 4 Z(Elements)

Roles	Required skills
r_1	s_9, s_{10}
r_2	s_{11}
r_3	s_{12}
r_4	s_{13}, s_{14}, s_{15}
r_5	s_{16}

Table 5 Tot_Cnt

Role	r_1	r_2	r_3	R_4	r_5
Count	4	1	2	4	3

Table 6 Input

Student	Input
Student1	$s_2, s_3, s_{13}, s_{14}, s_5, s_9, s_{15}$
Student2	$s_1, s_{16}, s_5, s_8, s_2, s_4,$

This contains the count of total number of required skills for each role. This value is further useful while calculating the value of each role's skill average.

User Input Data (Table 6):

Section wise output of algorithm.

3.1 Section 1

This section in algorithm calculates the number of common skills (X) occurred in input.

Skills and store it into variable Val1. These skills are common for every role so that instead of adding them in each role separately, algorithm counting them initially for using this 'Val1' value further for each role's average calculation.

$$\text{Student1}: \ \text{Val1} = 3(s_2, s_3, s_5 \text{ common in } X \text{ set and input})$$
$$\text{Student2}: \ \text{Val1} = 2(s_1, s_5 \text{ common in } X \text{ set and input})$$

3.2 Section 2

Checks if student has selected some skills which are required in more than one role. This information is predefined in 'Y' dictionary. If the skills entered by user finds any match with the skills mentioned in 'Y' data list, it updates the count value in 'Output' of every role present in key set.

Student1:

Skills entered by Student1 does not found any match in 'Y' data list.

Student2:

Student2's skill s8 is present in 'Y' data list where the key set includes role r_3 and r_4; therefore, count of r_3 and r_4 are updated by 1 in 'Output' dataset (Table 7).

Table 7 'Output' after Sect. 2

Student	r_1	r_2	r_3	r_4	r_5
Student1	0	0	0	0	0
Student2	0	0	1	1	0

Table 8 'Output' after Sect. 3

Student	r_1	r_2	r_3	r_4	r_5
Student1	1	0	0	3	0
Student2	0	0	1	1	1

Table 9 'Output' after Sect. 4

Student	r_1	r_2	r_3	r_4	r_5
Student1	44	33	57	66	37
Student2	44	66	71	55	62

3.3 Section 3

This section verifies the individual skill requirements from '*Z*' data list and updates appropriate count in 'Output' list (Table 8).

3.4 Section 4

It calculates and updates an average value for each role by using following formula. This average value is again stored in 'Output' data list.

$$\text{Avg} = ((\text{Output}[k] + \text{Val1})/(X_\text{Cnt} + \text{Tot_Cnt}[k])) * 100 \quad (1)$$

- k—index of role/position to calculate Avg for.
- Output[k]—last updated count values for kth role.
- Val1—value no. of common skills matched calculated in Sect. 1.
- X_Cnt—No. of commonly required skills.
- Tot_Cnt[k] —Total Count of skills required for kth role (Table 9).

3.5 Section 5

Top 3 Roles most suitable roles for Student1 and Student2 according to their entered skill set (Table 10).

Table 10 Final_output

Student	Recommended roles
Student1	r_4, r_3, r_2
Student2	r_3, r_2, r_5

4 Advantages and Disadvantages

Advantages:

- As system is content-based recommendations system, it does not need the data about other users. It will give the results specific to interest of individual user.
- Every user's own set of skills analyzed by system to serve appropriate recommendation of suitable roles.
- System helps user to make up her/his mind clearer for opting suitable role according to her/his skill set.
- Fast and easy self-analyzation of user's skill set.

Disadvantages:

- All skill sets and available roles must be predefined to process for analyzation.
- Choices of skills are limited for user due to already defined set of available skills.

5 Future Work and Conclusion

Future Work:

This system considers student's perspective for choosing role in college voting system according to her/his skills set. Further in future, this system can be considered for similar requirements where user needs to make a choice based on some dataset; here system may help to analyze the data and give appropriate suggestion to user.

6 Conclusion

Finally, with this work has been possible to identify that a recommendation system is an important and necessary tool for the students participating in an election. One of the advantages of developing this system is to make candidates does not worry about picking a role among all those available roles, without knowing if the chosen role is compatible with their skill set. The system takes care of looking the most appropriate role for the candidate.

Finite Element Method-Based Artificial Neural Network



Harshini Pothina and K. V. Nagaraja

Abstract Write-up is about the basics of finite element method (FEM) starts with the introduction of finite element analysis followed by the implementation of artificial neural networks (ANN) in brief, and finally, article explains the combination of FEM with the emerging ANN to provide an accurate mesh generation technique. It tells us the importance of FEM in the real-world engineering applications and moving on to the discretization of the domain for the generation of FEM mesh and the implementing steps of it. It gives us a glance of how a mesh refinement can be made from the coarse mesh using few refinement techniques and also the standard guidelines to be followed before computing for an adaptive mesh. Later on moving on to the working of an ANN in the feed forward process and the activation function which is used widely. It explains the cost/error function and, finally, computing for the desired output using back propagation algorithm. The final section explains the importance of implementing the FEM mesh using ANN. The elements that are generated in FEM domain are extracted using ANN algorithm by considering the neurons with the FEM nodes and the physical space of the domain with the weight space of the neural network

Keywords Finite element method · Mesh refinement · Artificial neural network · Self-organizing maps · Density function · Element extraction

H. Pothina (✉)
Department of Electronics and Instrumentation Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Bengaluru, India
e-mail: BLENU4EIE18031@bl.students.amrita.edu

K. V. Nagaraja
Department of Mathematics, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Bengaluru, India
e-mail: kv_nagaraja@blr.amrita.edu

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_73

1 Finite Element Method

The word FEM says a method for finite elements, which means that it is a technique to solve a complex system by dividing the domain into finite number of small elements. In general, finite element method is used to compute boundary value problems that are governed by partial differential equations of 1, 2, and 3-dimensional systems such boundary conditions, and governing equations are found in elastic problems, heat flow analysis, electro statics, and many more. In such scenario, finite element method helps in resulting set of simultaneous algebraic equations [1]. The word "finite" implies that it has finite number of degrees of freedom. Inverse problems, partial differential equations, and such boundary value problems cannot be solved analytically, and it requires a numerical technique to compute, and this FEM is the effective method which is used frequently. Inverse problems as in include finding the coefficients of the PDEs in such a way it can also deal with optimization problems. Predominantly, computation of data in finite element analysis is carried out by generating a finite element mesh which comprises of "elements" and "nodes of the elements." Elements here are simply the subdivisions of the domain of a given complex system, and nodes are the vertices or indices of the elements [1, 2]. Finite element analysis mainly involves four steps:

1. **Discretization**—Subdividing the domain into small elements
2. **Localization**—acquiring the behavior of each element present in the mesh
3. **Globalization**—assembling all the elements based on their connectivity element
4. **Solution and Post-processing**—solving for state variables (Fig. 1).

Discretization of the domain is followed by the interpolation process for the approximation of each element and then finding the properties of the elements by establishing a matrix form out of it and, finally, solving for the unknown parameters under the given boundary conditions [4, 5]. Taking care of the above-mentioned four

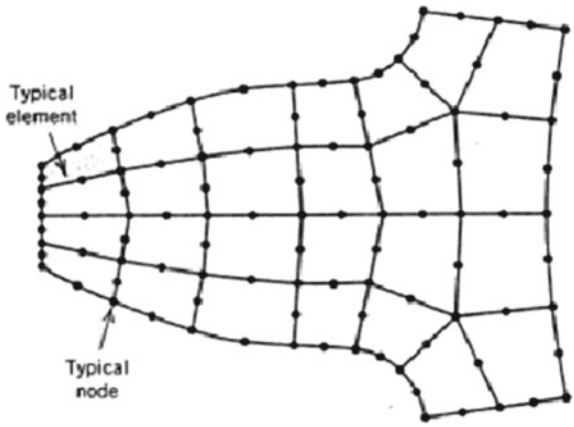


Fig. 1 Representation of elements and nodes [3]

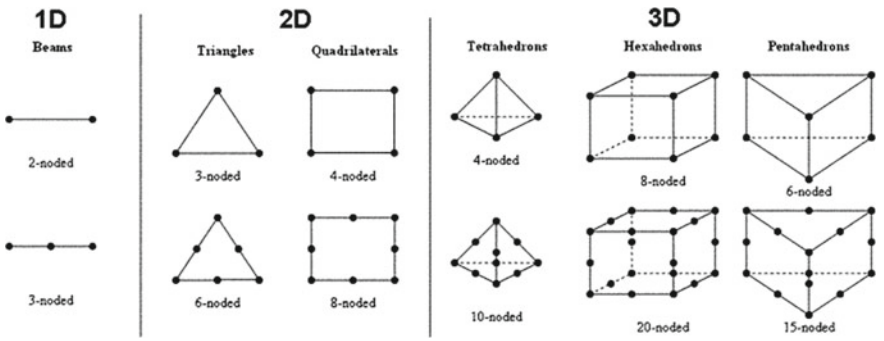


Fig. 2 Types of meshes in 1D, 2D, and 3D domains [6]

steps, one has to pay attention to the accuracy of the analysis as well. Its accuracy depends upon the proper placement of the nodes on the finite element mesh as well as deciding for the proper topology, material properties along with the suitable size of the mesh as in density of the mesh which depends upon the size of the largest element present in the mesh which subsequently leads to the adaptive computation. FEM meshes can be of 1D, 2D, and 3D. In general, a 2D mesh is usually discretized into triangular or quadrilateral elements (Fig. 2).

Based on the topology of the elements, one has to be an expert in creating a mesh in order to avoid errors, following are such few important guidelines which are considered standard [7]:

1. **Material Threshold**: Adaptive computation of the mesh can be achieved by creating a coarse mesh initially, and later refinement of the mesh should be made by estimating the solution errors of the elements present followed by splitting the elements into a smaller ones, whose errors exceed a certain threshold value.
2. **Mesh quality**: The ratio between the dimensions of the largest and smallest in the mesh should be kept close to unity, which is considered as "aspect ratio." It can also vary between 1.5 and 2. All of the elements should be proportioned properly.
3. **Number of mesh elements**: It is recommended to limit the number of mesh elements as it helps in increasing the computational efficiency of the model in order to meet the accuracy of the analysis.
4. All the elements interior angles on all sides should be kept lesser than 180 degrees. Inappropriate considerations like placing a quadrilateral with three of its vertices on a straight line is completely unacceptable.
5. In areas where the solution is expected to have high gradients or thought to be changing rapidly, the mesh should be finer. As a result, smaller components should be used at singularity points such as at the area where the boundary data changes rapidly, at the holes and at the re-entrant cracks or corners, etc.

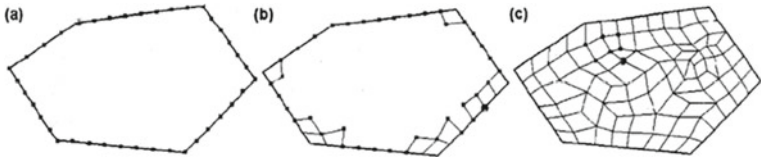


Fig. 3 Mesh generation steps starting with piece wise selection of boundary points, element generation, and the final mesh elements [10]

6. It is fine to have the ratio of sizes between two adjacent elements to be 1.5 or 2, but it should not be more than this. There should be a gradual transformation from larger to smaller elements [7–9] (Fig. 3).

Adaptive mesh refinement: Efficient mesh can be achieved with the adaption of the mesh refinement process by taking the domain error into consideration. Efficient mesh here means that the one whose domain error is distributed uniformly over the domain which helps in resulting the minimal domain error. By means of adaption domain error can be reduced as well as it can be distributed equally until the predefined error value becomes greater than the domain error [11]. Mesh refinement is the process of evaluating the model over some boundaries between two or more successively finer meshes and comparing the results of these different meshes in order to achieve the convergence of solution. After such two or more evaluation processes, the difference in their results shows minimal leading to the asymptotical behavior of the solution which finally converges the model. Modeling of meshes can be of two types: structured and unstructured models [12].

Structured mesh: These are often called as "grids," whose structure has ease of identification of elements and nodal positions. These meshes are commonly applied over analytical coordination systems like rectangular, spherical, etc., which forms a rectangular grid. Any curvilinear grid (cylindrical shape) can be easily mapped to a rectangular grid (Fig. 4).

Unstructured mesh: These meshes are more in general form and can approximate any kind of geometrical figures. As like structured mesh where it has ease of mapping coordinates into the elements of the grid, unstructured mesh cannot map easily in fact it requires a data structure like the list of nodes coordinates and the adjacencies. It does not require any kind of analytical shapes so its mesh nodes can be chosen arbitrarily (Fig. 5).

Unstructured meshes are usually preferred in discretization of the geometry of a problem under the boundary conditions of the governing equations and, finally, computing for the state variables since many real-world engineering applications cannot be solved in a rectangular domain. In general, a good quality quadrilateral mesh cannot be obtained directly by discretizing the domain into quadrilaterals, and it has to undergo a triangular mesh formation, and then a refined mesh with quadrilateral elements can be generated out of it [15]. This can be done by first dividing the domain into sub-regions of triangular elements secondly generating the fine triangular mesh using the triangulation technique (Delaunay triangulation). Then from an automatic

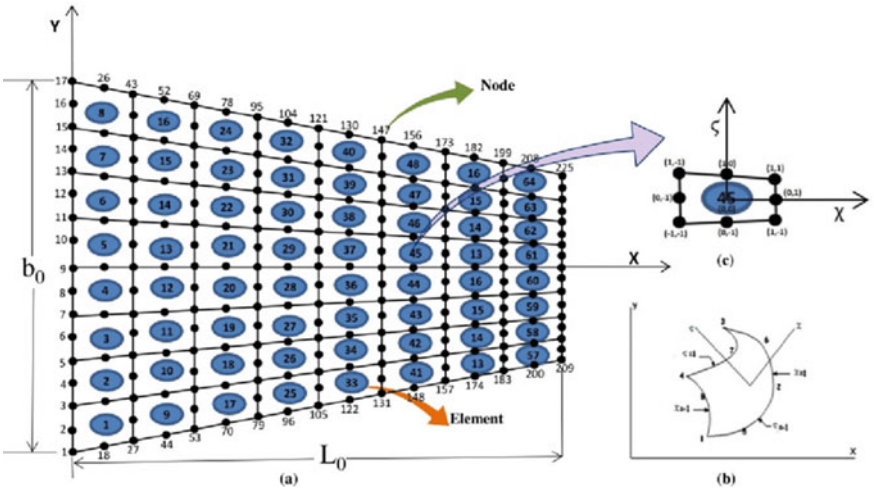
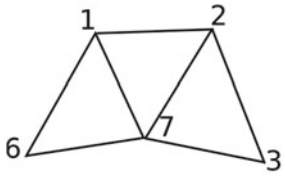


Fig. 4 Mapping a circular grid to a rectangular grid [13]

Fig. 5 Unstructured mesh with nodes and adjacencies [14]



Node	Adjacencies
1	2, 6, 7
2	1, 3, 7
3	2, 7
6	1, 7
7	1, 2, 3, 6

conversion of triangular mesh to quadrilateral mesh process is proposed, in which a standard right angled isosceles triangle mapped from an arbitrary triangle is divided into four quadrilaterals by taking three nodes on each of its sides and a node at the center of the triangle. Further dividing the quadrilaterals into standard triangles and again triangles into quadrilaterals finally heading to the refined quadrilateral mesh [16, 17] (Fig. 6)

Based on modeling and adaption of meshes, mesh refinement techniques are divided into few types:

1. ***h*-type**: "*h*' stands for geometric parameters like the length and the diameter of the element in which size of the element is reduced. If the refinement is taken throughout the domain, then it is said to be uniform h-refinement else it is said to be adaptive *h*-refinement.
2. ***p*-type**: Refinement in which order of the polynomial is increased. If is taken throughout the domain, then it is uniform p-type; else if it is carried out locally, then it is adaptive p-refinement.

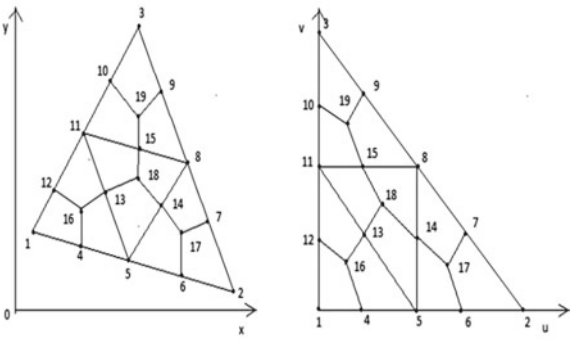


Fig. 6 Mapping an arbitrary triangular mesh to an isosceles triangle and dividing the triangular elements into quadrilateral elements [15]

3. ***hp*-type**: combination of both the "*h*' and "*p*"-type refinements, i.e., simultaneous increment in the order of the polynomial and reduction in the size of the element.
4. ***r*-type**: Refinement in which there is a movement in the position of nodes at a required location in order to increase the mesh density without altering the network connectivity of the mesh or number of nodes present in the mesh [8, 9].

2 Artificial Neural Networks

Artificial neural networks are a form of biological nervous system where processing of information takes place through a complex network. It consists of highly interlinked processing elements called neurons. All these neurons are connected to each other by means of three different layers, i.e., input layer, hidden layer, and output layer [18]. Data to be processed is given at the input side of the network, and after going through a huge process in the hidden layer, the final result is reflected at the output side providing a feed forward path to the neural network. Learning the unknown process at the hidden layer shows the functioning of a neuron. Once the network is structured according to the required number of neurons at different layers, it is ready to be trained. Generally, training of a neural network involves two ways [19, 20]:

1. **Supervised training**: In supervised training, network is provided with both the input and the output values, it processes the input data and verifies its output with the desired output value and propagates back by finding the error between the actual yield and desired yield in order to adjust the weights and propagates forward to meet the desired output.
2. **Unsupervised training**: In unsupervised training, network is not provided with output values as like in supervised, and it is provided with only input values. The network itself has to decide to which input section it belongs to when many number of input sections are given to process. It has no external feedback provided from the environment to compare it with the desired output. This is where self-organizing neural networks come into picture (Fig. 7).

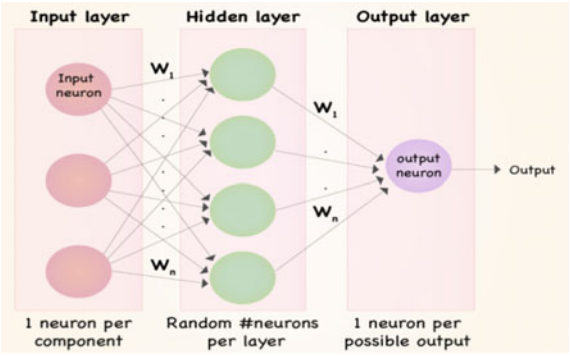


Fig. 7 Three different layers of the neural network [21]

Working of a neural network: In general, working/learning of a neural network involves dealing with two algorithms, i.e., feed forward and back propagation algorithms. Feed forward step is where all the processing of data from first layer to the last layer via hidden layers is done only in a forward direction, whereas the back propagation involves propagating the data backward from the last layer to the first layer in order to minimize the error found at the last layer. In a feed forward network, input data to the input neurons, weights (chosen randomly) and bias (1 by default) values at each node are allotted to activate the network in forward direction. In the first layer of the network, input vector gets multiplied with the weight vector [22] and sums up with bias vector to leave an output which is served as an input to the hidden layer. The actual training of the network takes place in the hidden layer with the help of activation functions such as sigmoid function, linear function hyperbolic tangent function, etc., among those sigmoid activation function is widely used to train the neuron at the hidden layer [23, 24].

Output at the layer 1:

$$Y = wX + b$$

where "X" is the input vector

"w" and "b" are the weight and bias matrix, respectively.

Sigmoid function:

$$\sigma(x) = \frac{1}{(1 + e^{-x})}$$

After processing under activation function, the output at the layer 2 becomes (Fig. 8):

$$F(x) = \sigma(wX + b)$$

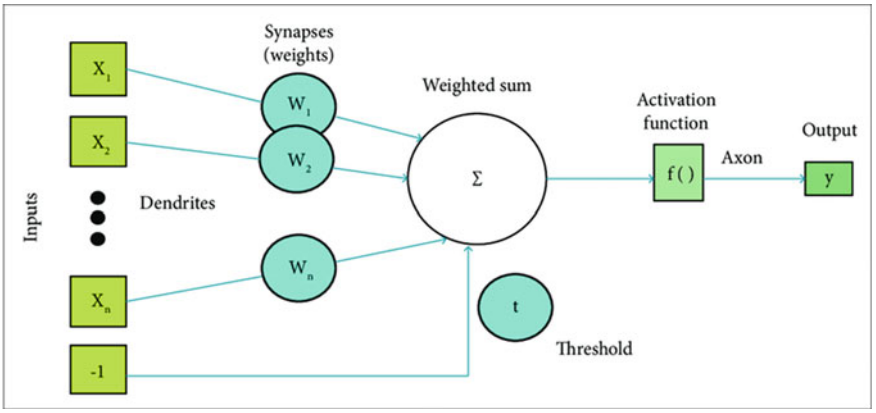


Fig. 8 Artificial neuron with a sigmoid activation function [25]

The input coming to the hidden layer neurons from the input neurons gets activated under sigmoid function with the help of weights and bias leaving an input to the output neurons. The process at the output layer repeats same as at the input layer and, finally, gives an output value which is the actual output to the network. The final actual output is then compared with the desired output value in order to compute the error/ cost function.

$$C(w, b) = \frac{1}{N} \sum_{j=1}^{N} \left| F_{j\,(\text{desired})}(x) - F_{j\,(\text{actual})}(x) \right|^2$$

"N" represents the total number of samples

"w" and "b" are weights and bias

"$F(x)$" is the activated output.

Gradient descent and back propagation algorithm: The network is now propagated back considering the last layer to be the first layer and first layer to be the last layer in back propagation process in order to change/update the weights and bias values accordingly to minimize the error and to meet the desired output [26]. This can be done by taking the differentiation of the cost function w.r.t all the parameters present at each layer starting from the output layer to the input layer. After updating the parameters, the feed forward network process proceeds the same way, and the output data is propagated back, and the computation continues until the desired output is reached.

Gradient of cost function w.r.t weights and bias is considered at each layer

$$\frac{\partial C}{\partial w_{(L)}} = \frac{\partial C}{\partial F_{L(\text{actual})}(x)} \frac{\partial F_{L(\text{actual})}(x)}{\partial Y_{(L)}} \frac{\partial Y_{(L)}}{\partial w_{(L)}}$$

$$\frac{\partial C}{\partial b_{(L)}} = \frac{\partial C}{\partial F_{L(\text{actual})}(x)} \frac{\partial F_{L(\text{actual})}(x)}{\partial Y_{(L)}} \frac{\partial Y_{(L)}}{\partial w_{(L)}}$$

Weights are updated to their new values as follows

$$w_{j(\text{new})} = w_{j(\text{old})} - \alpha \left(\frac{\partial C}{\partial w_j} \right)$$

$$b_{j(\text{new})} = b_{j(\text{old})} - \alpha \left(\frac{\partial C}{\partial b_j} \right)$$

"j" is the sample number

"α" is the learning rate.

3 FEM-Based ANN for Element Extraction

In finite element method-based artificial neural networks, FEM mesh is generated using artificial neural networks in which weights and bias parameters are assigned with the locations of the nodes present in the mesh based on the density distribution function. Weight vectors here generally take two or three components depending upon the either 2D or 3D meshes that we consider [27]. Geometric coordinates of the mesh is provided by the self-organizing neural networks which have the ability to adjust their weights based on the input data provided in order to generate a map of neurons called the self-organizing map(SOM) whose topology resembles with the input data. Such a map serves as a basis for the generation of a finite element mesh by reflecting the mesh nodes with neural nodes and the physical space of the domain with the weight space that is the interconnections between the neurons of the neural network [10]. The coordination of the mesh is carried out by the neural network algorithm by considering the coordinates of the randomly chosen sample (boundary) points based on the probability distribution in the domain as the input data to the self-organizing neural network for the element discretization, and the output would be the position of the elements that are to be extracted one after the other from the discretizing domain in order to generate a 2D mesh out of it [28, 29] (Fig. 9).

Here where the role of density function comes into picture, which is actually used to express the estimation of the placement of the mesh elements. Density function of the mesh is nothing but which indicates the number of elements present in a particular area, for a circle circumscribed over a triangle, it indicates the value of the radius of the circle. The accuracy of the mesh topology depends on the density of the mesh. Usually, higher density meshes produce more accurate results when compared to less density meshes [30, 31]. This mesh density vector is trained under neural networks on a selected area and is utilized by the mesh generator as the input data. Based on the application of the problem to be solved, the input data to the network is taken as

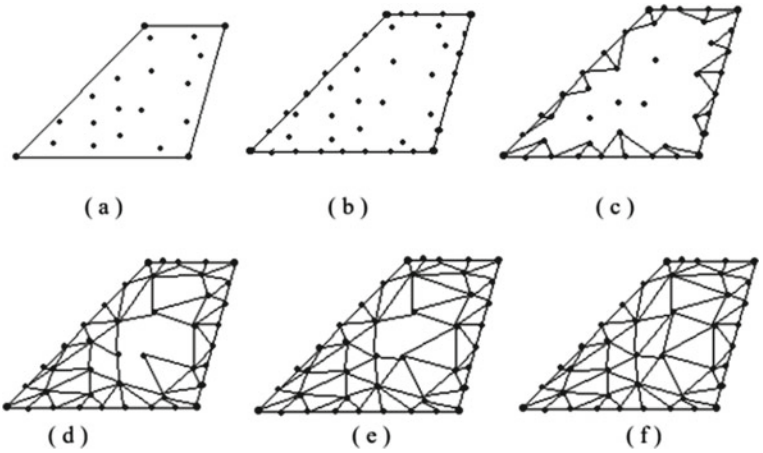


Fig. 9 Discretization of the domain and element extraction [26]

the parameters that influence the density function. In such a way, the coordination of the mesh is carried out by the Kohonen algorithm which is widely used for the generation of self- organizing maps [7, 28]. Input being the randomly chosen points reflecting the desired density function. This network automatically organizes itself for the best representation of the map with the mesh elements out of it. Points from the topology of the domain are chosen as input points in such a manner that winner takes all method. The location of the chosen node (neurons) is adjusted such that the coordinates of all the nodes are in the neighborhood with the selected node which ultimately generates the map of mesh elements (Fig. 10).

Firstly, a reference point is selected from the present boundary points in such a way that it obeys its boundary angle to be between 45 and 135 degrees in the domain,

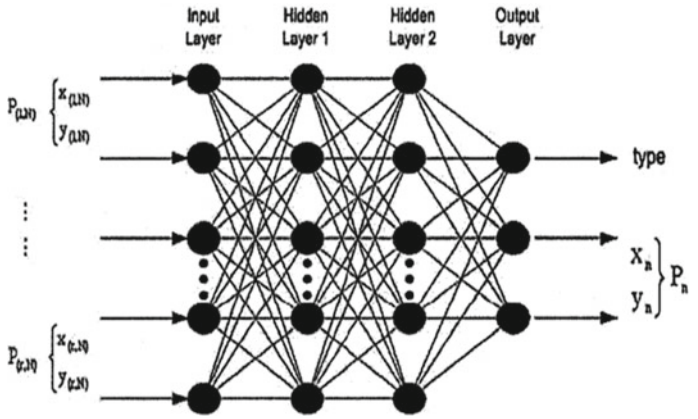


Fig. 10 Sample points as input data to the network for the element extraction [32]

and then the number of other points called the leading points is selected around the reference point whose coordinates along with the reference point coordinates are given as input to the neural network [8, 32]. An element from the boundary domain is extracted mainly in three types by considering a new point on the base of the boundary points and the other types being change in the relative location of the reference point. Newly extracted element is represented as [type, P_n] where type takes the value from any of the three types described above and P_n is the output element (Figs. 11 and 12).

All the elements are extracted from the domain based on few basic element extraction rules and boundary components provided in [31–33] and are trained under the neural network to output the parameters of the new element around the reference point until a good quality element is extracted, and further, the boundary is updated for the next element to be extracted, and this process continues until the domain is discretized into required number of good quality elements, and finally, the elements are trained for the mesh generation process.

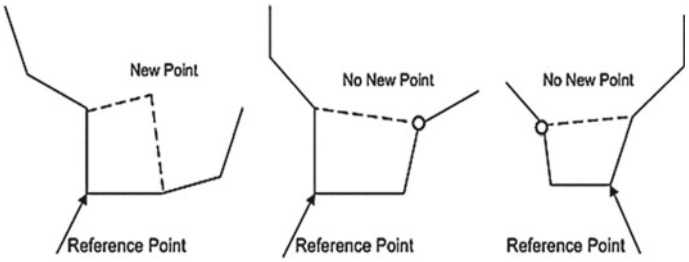


Fig. 11 Three types of selection of elements from the boundary domain [10]

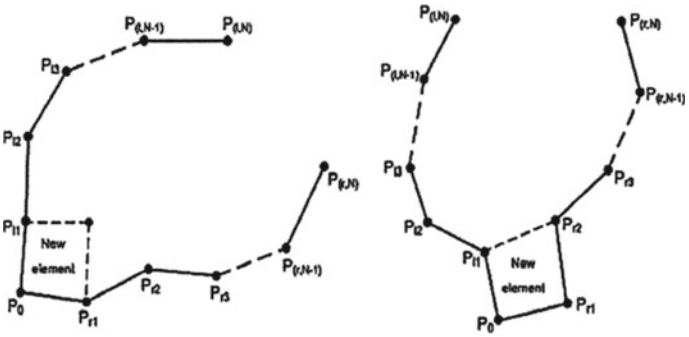


Fig. 12 Representation of leading points around a selected element [32]

4 Conclusion

Artificial neural networks can be combined with finite element method to increase the robustness of the numerical method in various applications like solving PDEs, optimization problems, heat flow analysis, and many such domains in engineering. In their convergence technique, fem mesh generation is carried out with the help ANN where the elements required for the mesh generation are extracted one by one from the domain by choosing the coordinates of the elements as the input data to the ANN and the output being the position of the element to be extracted next. Quadrilateral meshes are considered in general for any 2D mesh generation process. It is achieved by mapping an arbitrary triangle to an isosceles triangle and by dividing their triangular mesh elements into quadrilaterals with the help of Delaunay triangulation algorithm. Self-organizing maps-based kohonen algorithm is widely used technique to solve for the elements extraction relating to their respective density function in order to achieve a refined mesh. Few mesh refinement techniques are available based on the size of the elements, position of nodes a coarse mesh can be refined to a fine mesh under adaptive mesh refinement process. Further, FEM-based ANN technique will be studied carefully in depth to bring new and effective concepts out of it to solve many PDEs that cannot be tackled using analytical methods, and this FEM-based ANN approach can also be brought into artificial intelligence-based mathematics world in solving many robotic applications like making of a humanoid robot, self-driving car, biped robots, and many more.

References

1. R.D. Cook, D.S. Malkus, M.E. Plesha, R.J. Witt, Concepts and applications of finite element analysis, 4th edn, University of Wisconsin, Madison
2. J. Berg, K. Nystrom, A unified deep artificial neural network approach to partial differential equations in complex geometries, Department of Mathematics, Uppsala University S-751 06 Uppsala, Sweden
3. https://www.researchgate.net/profile/Nasir_Tamin/publication/46309172/figure/fig1/AS:307390479126531@1450299009461/Figure-1-A-coarse-mesh-two-dimensional-model-of-gear-tooth-All-nodes-and-elements-lie.png
4. O. de Weck, I.Y. Kim, Finite element method (MIT, 2004)
5. G.H. Paulino, D.B. Willett, Finite element methods. Department of Civil and Environmental Engineering University of Illinois at Urbana-Champaign
6. http://3.bp.blogspot.com/-rUQMZ1BuVnI/TiLwGJlGGOI/AAAAAAAAASw/fkaV3Z1aQFo/s1600/FEMShapes.gif
7. H. Jilani, A. Bahreininejad, M.T. Ahmadi, Adaptive finite element mesh triangulation using self-organizing neural networks. Tarbiat Modares Univ. Tehran Iran Adv. Eng. Softw. **40**, 1097–1103 (2009)
8. L. Manevitz, M. Yousef, D. Givoli, Finite-element mesh generation using self-organizing neural network. Univ. Hai Microcomput. Civil Eng. **12**, 233–250 (1997)
9. Y.H. You, X.Y. Kou, S.T. Tan, Adaptive meshing for finite element analysis of heterogeneous materials. Department of Mechanical Engineering, The University of Hong Kong, Pokfulam Road, Hong Kong

10. J. Jin, Regression model based automatic finite element mesh generation, A thesis in the Department of Electrical and computer engineering, Concordia University, Montreal, Quebec, Canada, February 2008
11. F. Belhabib, M. Ettaouil, Mesh refinement with finite elements and artificial neural networks. Int. J. Neural Netw. Adv. Appl. **2** (2015)
12. S. Devi, K.V. Nagaraja, T.V. Smitha, S. Jayan, 2D Higher order triangular mesh generation in irregular domain for finite element analysis using MATLAB. IOP Conf. Ser. Mater. Sci. Eng. **577**(1), 012132
13. ApurbaDas, https://www.researchgate.net/profile/Apurba_Das9/publication/323826818/figure/download/fig2/AS:742082914299904@1553937762056/a-Finite-element-discretization-of-8-x-8-mesh-on-plan-area-with-elements-b-node.png
14. https://clqtg10snjb14i85u49wifbv-wpengine.netdna-ssl.com/wp-content/uploads/2020/04/unstructured-mesh-and-its-adjacency-list.png
15. S. Devi, K.V. Nagaraja, T.V. Smitha, S. Jayan, Accurate higher order automated unstructured triangular meshes for airfoil designs in aerospace applications using parabolic arcs. Aeros. Sci. Technol. **88**, 405–420
16. P. Kannan, K.V. Nagaraja, An efficient automatic mesh generator with parabolic arcs in Julia for computation of TE and TM models for waveguides. IEEE Access **8**, 109508–109521 (2020)
17. T.V. Smitha, K.V. Nagaraja, An efficient automated higher-order finite element computation technique using parabolic arcs for planar and multiply-connected energy problems. Energy **183**, 996–1011 (2019)
18. H. Kukreja , N. Bharath, Kuldeep S.C., An introduction to artificial neural network. Int. J. Adv. Res. Innov. Ideas Edu. IJARIIE **1**(5). ISSN (O) 2395–439 (2016)
19. H. Pothina, K.V. Nagaraja, Artificial Neural Network and Math Behind It (Accepted)
20. S. Rusia, K.K. Pathak, Application of artificial neural network for analysis of triangular plate with hole considering different geometrical and loading parameters. Open J. Civ. Eng. **6**, 31–41 (2016)
21. https://cdn-images-1.medium.com/max/1600/1*pbk9xtz7WbBwYPVATdl9Vw.png
22. T. Guillod, P. Papamanolis, J.W. Kolar, Artificial neural network (ANN) based fast and accurate inductor modeling and design. Power Electronic Systems Laboratory, ETH Zurich, 8092 Zurich, Switzerland
23. S. Bhanu, The novel artificial neural network assisted models: a review, Canara Bank 8 February 2021
24. S.B. Maind, P. Wankar, Research paper on basic of artificial neural network. Int. J. Recent Innov. Trends Comput. Commun. **2**(1), 96–100. ISSN: 2321–8169
25. https://www.researchgate.net/profile/Adriano_Tech/publication/279224135/figure/download/fig2/AS:613966506106895@1523392430841/Model-of-an-artificial-neuron.png
26. K. Mehrotra, C.K. Mohan, S. Ranka, *Elements of artificial neural networks*, 144 illus (1996), 344 pp. ISBN 0-262-13328-8
27. T.V. Smitha, K.V. Nagaraja, Application of automated cubic-order mesh generation for efficient energy transfer using parabolic arcs for microwave problems. Energy **168**, 1104–1118 (2019)
28. D.G. Triantafyllidis, D.P. Labridis, A finite-element mesh generator based on growing neural networks. IEEE Trans. Neural Netw. **13**(6) (2002)
29. Ahmet, A. Ahmet, Neural Networks Based Mesh Generation Method in 2-D, Firat Universitesi, Muhendislik Fakultesi, Bilgisayar Muhendisligi, Elazig, Turkiye, 23119
30. A.A. Javadi, M. Mehravar, A. Faramarzi, A. Ahangar-Asr, An artificial intelligence based finite element method. ISAST Trans. Comput. Intell. Syst. **1**(2) (2009)
31. D.G. Triantafyllidis, D.P. Labridis, An automatic mesh generator for handling small features in open boundary power transmission line problems using artificial neural networks. Department of Electrical and Computer Engineering, Aristotle university of Thessaloniki, 540 06 Thessaloniki, Greece
32. D.A. Lowther, On automatic mesh generation using Kohonen map. IEEE Trans. Magn. **34**(5) (1998)

33. S. Yao, B. Yan, B. Chen, Y. Zeng, An ANN-based element extraction method for automatic mesh generation, Concordia Institute for Information Systems Engineering, Concordia University, 1455 de Maisonneuve West, CB-410–16, Montreal, Que., Canada H3G 1M8

An Ellipse Slotted Vivaldi Antenna for 5G Applications



Akshta Jagdale, H. Sairaam, Harshita Kulkarni, Lakshmi Suresh Nair, and Sanjeev Kumar

Abstract With the advancement in communication and digitization, the need of having a reliable hardware is extremely necessary. Radars and radar systems play a vital role in various fields like geographical studies, aviation, etc. One important part of these radar systems is an antenna. Antennas have been in use in several fields, right from aircrafts, ships, military applications and space shuttles to comparatively smaller systems like cars, a radio, mobile phones and many more. This paper introduces a particular type of antenna: tapered slot Vivaldi antenna (TSA) with ellipse slot. The presented unique Vivaldi antenna is specially designed for 5G applications. The design has FR4 as the substrate with a dielectric constant of 4.4 and a thickness of 0.8 mm. The dimensions of this design are 11 mm × 8 mm. From the simulated results, it can be seen that this antenna has a good return loss at two frequencies: 24.77 GHz and 44.88 GHz. The impedance bandwidth for these two frequencies is approximately 4 GHz and 14.5 GHz, respectively. The S11 value at 24.27 GHz is -31.75 dB and that at 45 GHz is -26.27 dB. The overall gain of this antenna is 4 dB. VSWR values at 24.77 GHz and 44.88 GHz are 1.0531 and 1.1021, respectively. The main advantage of this size is that it can easily fit in smaller appliances and hence can be used extensively for mobile phones.

Keywords Vivaldi Antenna · Ansys HFSS · FR4 (4.4 dielectric constant) · Ultra-Wideband · Ellipse-Slotted · S11 · VSWR

A. Jagdale (✉) · H. Sairaam · H. Kulkarni · L. S. Nair · S. Kumar
Department of Electronics and Telecommunications, Symbiosis International (Deemed) University, Pune, Maharashtra, India
e-mail: akshta.jagdale@sitpune.edu.in

H. Sairaam
e-mail: h.sairaam@sitpune.edu.in

H. Kulkarni
e-mail: kulkarni.harshita@sitpune.edu.in

L. S. Nair
e-mail: lakshmi.nair@sitpune.edu.in

S. Kumar
e-mail: sanjeevkumar@sitpune.edu.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_74

1 Introduction

The technologies around us have evolved in such a way that there is a growing demand for advancements in terms of speed, deliverability and performance. In today's wireless communication systems, there are a lot of requirements that need to be met apart from those delivered by 1G to 4G. Multimedia services are in great use and so the speed of transmission of these services are now required to be faster [1]. 5G is considered as the future generation which will focus on providing higher data rates, improved security, increased efficiency of energy and promotion of higher resolution. In such scenarios, coming up with a patch antenna design which has multiband characteristics can be beneficial. The patch antenna, as compared to other antenna, proves to be more beneficial as it costs low and offers moderate to high gain [2].

As reported in recent literature works, the most important and widely considered bands of 5G are 25 to 29.5 GHz and 31.8 to 33.4 GHz. A high value of gain in 5G is necessary to ensure high-radiated power. An antenna that is designed to work for 5G applications should essentially work at higher frequencies with a bandwidth of 6 to 7 GHz [3]. Tapered slot Vivaldi antenna can be a choice of antenna which will satisfy all the needed requirements for 5G communication. The tapered slot in this type of antenna is exponential and is found helpful in radiating the EM wave [4]. The operating frequency of an antenna in 30 GHz band covers the band for 5G communication and gives a high-spectral efficiency as well as high-signal speed and high-data transmission speed. Vivaldi antenna is used mainly because of its ease of fabrication and integration along with wider bandwidth [5]. It has been proven to be good for providing great impedance matching and on the other hand also fulfils the criteria of covering the S and L band that is necessary for 5G [6]. Vivaldi antenna is considered as a perfect choice for applications like that of a radar because of its high gain and wide bandwidth. Also, for wireless applications, Vivaldi antenna is preferred because of its properties like broad bandwidth, low-cross polarization and high-directive patterns. The good radiation pattern, VSWR and gain of a Vivaldi antenna when obtained over the UWB frequency band makes the antenna valuable for short range, low-power mobile electronics in ultra-wideband communication field [7]. An additional reason why it is preferable for radar applications is because the resolution of the radar is directly related to the wider bandwidth of the antenna [8]. For applications like IoT, this antenna poses as the best option when the gain obtained is 3dBi with an operating frequency of 5.8 GHz [9].

UWB stands for ultra-wideband communication. It is a short wideband communication technology with high speed (about 100 Mbps). It is beneficial because it provides wireless connectivity with a consistent high data rate. Enhancement of results like antenna radiation, front to back ratio (F/B ratio) and other antenna characteristics can be done using various techniques like inserting a parasitic radiating element in the aperture of the Vivaldi antenna (which will produce strong end fire direction), insertion of planar reflector at the back end and addition of corrugation at the end of the antenna, respectively [10].

As far as, the shape of slots of this tapered slot Vivaldi antenna is concerned, and the super elliptical equation is found to be used to control various parameters of the antenna, like tapering and the structure of the feedline which in turn gives us enhanced performance. This super elliptical slot shape is observed to have optimized the antenna features and has proven to decrease the lower cut-off frequency without dealing with the gain and design ratio properties [11].

The size of the antenna should be compact and it should be easily integrable. An antenna should show the required impedance matching and radiation across the given frequency band [12]. Even changing the dimensions of various parameters may cause difference in the results obtained like-on changing the flare length and width of the slot, the resonant frequency shifts to a lower value, thus improving the low-frequency transmission. Also, it is noticed that on increasing the substrate thickness of the antenna and the dielectric constant, the antenna size can be reduced and will also lead to achieving wider bandwidth, better radiation efficiency and gain in the band we are operating. For a microstrip type feeding technique, better results will be obtained by decreasing substrate thickness, decreasing dielectric value and increasing flare length as well as slot width [13].

In this paper, coplanar Vivaldi antenna is designed with multiple bandwidths along with high gains using high-frequency structure simulator (HFSS) software. The material used for substrate in this design is FR4, which has a relative permittivity of 4.4. FR4 substrate is chosen here because of its low-cost and better input impedance matching results. The proposed antenna is compact in size and shows operating frequencies of 24.2 and 45 GHz. The paper contents are: Sect. 2 focuses on the design methodology and design elaboration; Sect. 3 presents the simulated results and observations.

2 Antenna Design Methodology and Parameters

This section of the paper discusses the antenna design parameters along with detailed steps involved to achieve high gain and wider bandwidth. Figure 1 shows the top view of the proposed antenna design, and Fig. 2 shows the bottom view of the antenna with the feedline in green colour. In this figure, the dimensions of the antenna are shown in detail. The values of parameters of this ellipse slotted Vivaldi antenna are shown in Table 1.

The Vivaldi antenna is designed on the high-frequency structure simulator (HFSS) software. The steps followed for designing this antenna are as follows—A patch of the tapered slot Vivaldi antenna was designed using length of Vivaldi antenna 11 mm and width 8 mm. An equation-based surface was subtracted from the rectangle to make it taper slot. Ellipse shaped slots were subtracted on both side of taper slot, with major radius 1 mm, ratio 2 and at an angle 45o. From the radiation patch of Vivaldi antenna, two rectangular slots were subtracted, whose dimensions are 1.8 mm and rotated at 45o.

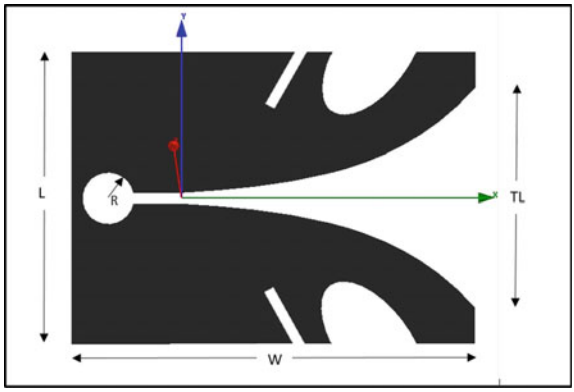


Fig. 1 Top view of radiating patch antenna

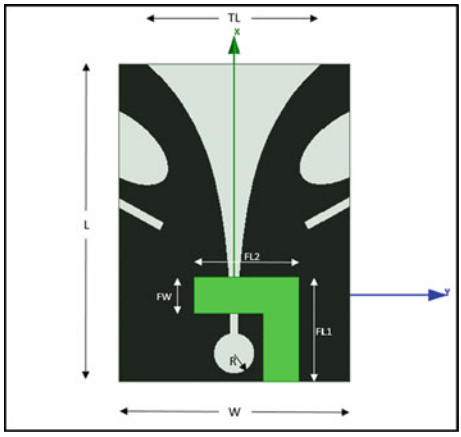


Fig. 2 Feedline of the antenna

Table 1 Parameters and dimensions of the proposed antenna

S. No	Parameters	Value	Description
1	Length (L)	11 mm	Length of antenna
2	Width (W)	8 mm	Width of antenna
3	Taper length (TL)	6.013 mm	Length of taper
4	Radius (R)	0.707 mm	Radius of circular slot
5	Material	FR4	Substrate material
6	Dielectric	4.4	Dielectric constant of substrate
7	Thickness	0.8 mm	Substrate thickness
8	Taper rate	375	Rate of tapering
9	Feedline width (FW)	1.25 mm	Width of feedline
10	Feedline length 1 (FL1)	3.625 mm	Vertical length of L-shaped feedline
11	Feedline length 2 (FL2)	3.65 mm	Horizontal length of L-shaped feedline

To complete the radiating patch, a circular slot with radius 0.707 mm was subtracted from the patch. The made patch needs to be supported by a substrate. A 0.8-mm thick FR4 substrate is used here with exact dimensions of the antenna (11 mm × 8 mm × 0.8 mm). The FR4 has a dielectric constant of 4.4. To feed the antenna, a microstrip feedline is introduced on the other side of the substrate with a width of 1.25 mm. Feed point is 0.675 mm above circular slot. Lastly, a lumped port on the YZ plane, between the patch and feedline, is introduced with dimensions 1.25 mm × 0.8 mm to assign excitation to the Vivaldi antenna.

3 Results and Discussion

Once the design was complete, it was simulated, and certain results were observed. The return loss (S11 parameter) at the frequency of 24.2778 GHz is −31.7504 dB, and the same at 44.8889 GHz is −26.2715 dB. This can be observed in Fig. 3.

The VSWR plot of the Vivaldi antenna shows values of 1.0531 and 1.1021 at the frequencies of 24.7778 GHz and 44.8889 GHz, respectively. This shows a good impedance matching occurring at both frequencies. Figure 4 shows the VSWR values.

Figure 5 under this description shows 2 plots together. One is 'Gain vs Frequency', and the other is 'Directivity vs Frequency'. The purple trace represents directivity, and the green trace represents gain of the antenna. It can be seen that these 2 traces follow each other very closely. The maximum value of gain observed here is approximately 4.5 dB, and maximum directivity is about 6 dB.

Figure 6 shown below represents E-plane radiation pattern, and Fig. 7 is the overlay of this radiation pattern on the antenna. This parameter helps in understanding the directivity of the radiation. E-plane shows the direction of electric field propagation. Figure 7 justifies that Vivaldi antenna is an end fire type of antenna.

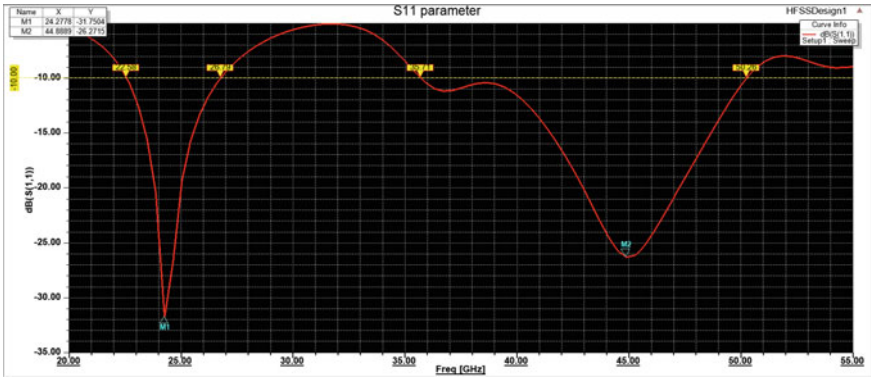


Fig. 3 S-parameter of the proposed antenna showing the multiband behaviour

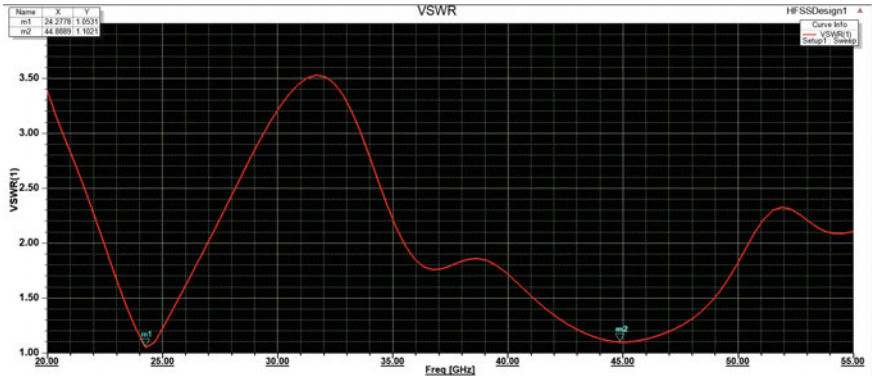


Fig. 4 VSWR of the proposed antenna showing the multiband behaviour

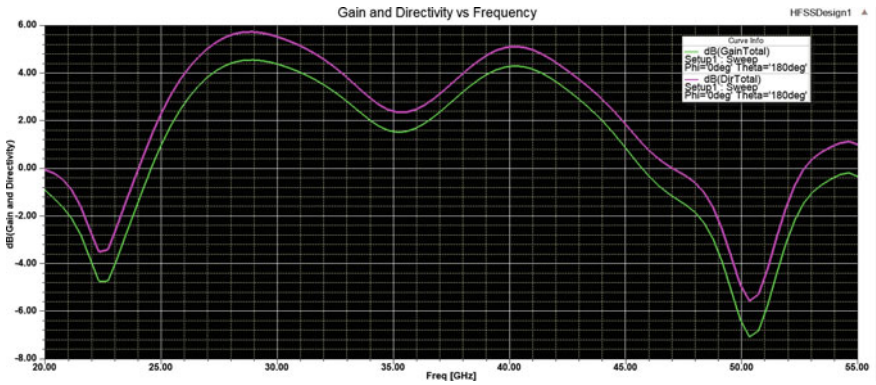


Fig. 5 Gain versus frequency and directivity versus frequency

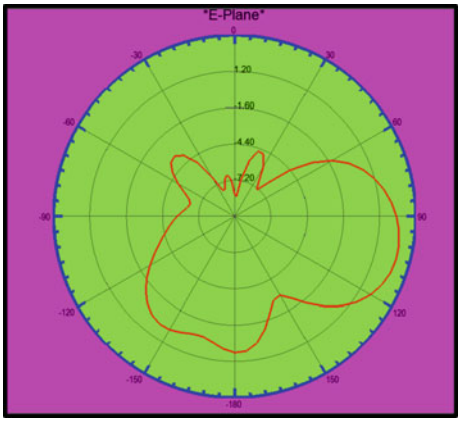


Fig. 6 E-plane radiation pattern

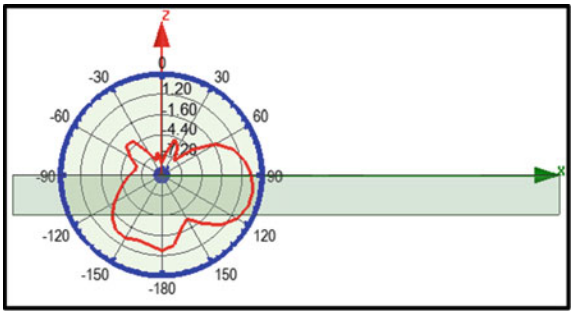


Fig. 7 E-Plane radiation pattern overlay on antenna

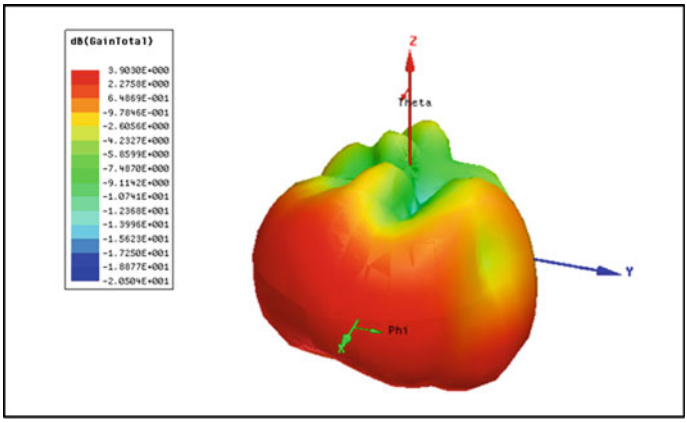


Fig. 8 Three-dimensional polar plot of the designed slot antenna

The bandwidth observed below -10 dB level shows us two different ranges as we have two good impedance matching. Here, 22.58 GHz to 26.79 GHz (4.21 GHz) and 35.71 GHz to 50.26 GHz (14.55 GHz) of bandwidth is observed, which shows why Vivaldi antenna are referred to as ultra-wideband antenna. The antenna is providing a gain of approximately 4 dB, and this can be used for 5G applications with higher data rates and improved efficiency. Figure 8 shows the 3D polar plot.

4 Conclusion

In this paper, the design and simulated results of a novel Vivaldi antenna for 5G applications were discussed. Based on these results, it can be inferred that this antenna is a multiple bandwidth antenna as the gain value is seen to be going below −10 dB, and major dip in this value is observed at two frequencies: 24.2 GHz and 45 GHz. The

bandwidth in case of both these dips is significant and can be used effectively. The overall obtained gain is about 4 dB, and a VSWR value of 1.05 and 1.1, respectively, is observed at both the assumed operating frequencies. Another inference that can be drawn from this is that the addition of elliptical and rectangular slots aid in improving the bandwidth as well as gain of the designed antenna. The size and dimensions of the feed and also of the radiation box play an important role in gaining better values for bandwidth, gain and other antenna parameters.

As 5G is about to roll out in the coming years, several factors will influence its implementation, including antenna. So, Vivaldi antenna can be a suitable candidate for 5G communications where antenna with wider bandwidth is appreciable.

References

1. A. Ahmed, A. Rahman, Y. Abdulmaqsoud, F. Amer, Design of Vivaldi antenna array with enhancement of radiation characteristics for 5G mobile applications. **3**, 74–80 (2016)
2. M. Almashhdany, O. Al-Ani, A. Sabaawi, M. Altaee, N. Hussein, F. Abdelreda, Design of Multi-band slotted mmWave antenna for 5G mobile applications. IOP Conf. Ser. Mater. Sci. Eng. **881**, 012150 (2020). https://doi.org/10.1088/1757-899X/881/1/012150
3. A. Dixit, S. Kumar, The enhanced gain and cost-effective antipodal Vivaldi antenna for 5G communication applications. Microw. Opt. Technol. Lett. **62**, 2365 (2020). https://doi.org/10.1002/mop.32335
4. H. Monga, Design and performance enhancement of Vivaldi antenna. Res. Dev. Mater. Sci. **3** (2018). https://doi.org/10.31031/RDMS.2018.03.000560s
5. A. Zhang, T. Huang, S. Zhu, Z. Wang, W. Yang, L. Haiwen, A miniaturized gain-enhanced antipodal Vivaldi antenna and its array for 5G communication applications. IEEE Access. **6**, 76282–76288 (2018)
6. F.-M. Paula, M.-A. Sergio, S.-V. Daniel, Design of a wideband Vivaldi antenna for 5G base stations (2019), pp. 149–150. https://doi.org/10.1109/APUSNCURSINRSM.2019.8888989
7. Y. Che, K. Li, X. Hou, W. Tian, Simulation of a small sized antipodal Vivaldi antenna for UWB applications. **1**, 1–3 (2010). https://doi.org/10.1109/ICUWB.2010.5615485
8. M. Perdana, T. Hariyadi, Y. Wahyu, Design of vivaldi microstrip antenna for ultra-wideband radar applications. IOP Conf. Ser. Mater. Sci. Eng. **180**. 012058 (2017). https://doi.org/10.1088/1757-899X/180/1/012058
9. M. Kumar, S. Agarwal, A. Sharma, A multi-application compact ultra-wideband vivaldi antenna for IoT, 5G, ITS, and RFID (2019). https://doi.org/10.1109/InCAP47789.2019.9134579
10. K. Sultan, H. Abdullah, E. Abdallah, M. Basha, H. El-Hennawy, A 60-GHz Gain Enhanced Vivaldi Antenna On-Chip (2018), pp. 1821–1822. https://doi.org/10.1109/APUSNCURSINRSM.2018.8608914
11. K. Simay, L. Abraham, C. Diego, A novel class of super-elliptical vivaldi antennas with enhanced radiation properties (2019), pp. 259–260. https://doi.org/10.1109/APUSNCURSINRSM.2019.8888948
12. Z. Djalal, M.F. Zahra, M.M. Sidi, New tapered slot vivaldi antenna for UWB applications (2012), pp. 1–4. https://doi.org/10.1109/ICM.2012.6471419
13. J. Shan, A parametric study of microstrip-fed Vivaldi antenna (2017)

Impact of Data Mining on HCC Prediction: Survey



Babitha Thamby and S. Sheeja

Abstract Liver diseases are common nowadays, and it is often described as silent disease since detection of such diseases is difficult since the affected person will not show any of the symptoms until the progressive stage. Researches show that over fifty million people globally are suffering from any type of hepatic diseases. Data mining has vital score in the diagnosis and prognosis of liver diseases using big data, machine learning (ML) and deep learning since detection procedures that are noninvasive have high-accurate results with ML support than clinical invasive procedures. Regarding this, study was done for the review of the benefits of applying these mining algorithms and their high contribution to the healthcare sector by its potential prediction capabilities and thus providing clinical decisions and a quality life style for the liver patients.

Keywords Data mining · Liver diseases · Machine learning · Prediction

1 Introduction

Liver is the body's largest internal organ doing the job of breaking down and detoxification of substances in the body. Its ultimate job is refining the stream of blood which is coming from the digestive tract, and supplying it to the remaining parts of the body. It stores glucose in order to make you remain nourished when you're not eating. Across the globe, most of the people are suffering from Chronic liver diseases [1]. The main risky considerations for the various liver sickness are hepatitis B or C viral infection, non-alcoholic fatty liver disease (NAFLD), heavy alcohol intake, habit of smoking, type 2 diabetes, obesity, exposure to chemicals or toxins and sometimes genetically. Various types of liver diseases include viral infections (hepatitis A, B, C), immune system related (autoimmune hepatitis, primary sclerosing cholangitis, primary biliary cholangitis), alcoholic fatty liver issues and non-alcoholic fatty liver disease (NAFLD) [2], non-alcoholic steatohepatitis (NASH), cirrhosis, inherited diseases, also tumor and cancer (Bile duct cancer, Liver cell adenoma and Liver

B. Thamby (✉) · S. Sheeja
Karpagam Academy of Higher Education, Coimbatore, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_75

Cancer). NAFLD is a common condition in the liver nowadays even in children [3]. NAFLD can progress into non-alcoholic steatohepatitis (NASH), type of fatty liver disease, which is aggressive and showing inflammation and may further develop scarring (cirrhosis) and sometimes even liver failure [4].

Among all liver cancers, hepatocellular carcinoma (HCC) [5], also called as hepatoma, is the very common type of liver cancer which is difficult to detect at the early stages with no or less symptoms [6]. Here, we are comparing the many ML algorithms that were applied broadly in prognosis and diagnosis of broad spectrum of liver diseases that were coming as a burden of NAFLD [7].

2 Prediction Analytics

There are invasive and non-invasive bio markers used in the prediction analysis of liver diseases. A biomarker is a patient characteristic which act as an indicator of a pathologic process or of a biological response to a treatment. The liver biopsy is the invasive procedure that was done in the case of prognosis to get more accurate results. Non-invasive methods showing reliability using two different methods [8]. The biological perspective based on either the quantitative biomarkers in samples of serum or by taking liver stiffness (LS) measurement [9]. Non-invasive biological markers were expanded and explored to assess fibrosis phase of NAFLD patients. This investigation call attention to recent considerations on the detection and different NAFLD-HCC levels constructed by some non-invasive procedures [10]. ML is a multidisciplinary field to implement computer algorithms for the high-prediction accuracy. We do it either by analysis or by probabilistic models from static as well as dynamic data.

By applying clinical data, it will possible. Machine learning has taken a big step in prediction of NAFLD related issues. Normally, algorithms are applied on the data like radiological imaging, liver pathology, electronic health records (EHRs), serum findings and from wearable sensors [11].

3 Methodology

Machine learning in healthcare is now has a prominent role, and it can help both patients as well as clinical experts in variety aspects. The common healthcare use cases for ML are clinical decision support, drug impacts and the development of care recommendations in clinical level. The performance of ML in automatic diagnosis and prediction has equal role that was given by the experienced radiologist. Various ML algorithms were used to detect HCC so that the progression of such diseases can be cured. Here, we are discussing about some of the popular ML algorithms, their predictive nature and performance [12]. They are:

3.1 Logistics Regression (LR)

It is a supervised classification method and was used in the research and other applications mostly. This method is able to deal with various quantities of numerical and absolute factors. It is a type of linear regression method but uses a logistic function. The method will give a binary output within a very short time. It provides both the appropriateness of a predictor and its association (positive or negative) [13]. If the number of findings or observations is lower than the number of features, logistic regression should not be used. Nonlinear problems will be difficult to handle since it has a linear decision surface.

3.2 Naive Bayes (NB)

The method based on Bayes' Theorem having an assumption of independence among predicting factors. In this method, the existence of a special attribute in a class is unrelated to the existing any other feature [14]. Each variable is independent.

3.3 Decision Tree (DT)

In this method, we split the data set based upon various conditions and generate a tree structure. Each node in the tree undergoes a test case for the value of some attribute. It is the one in the widely used supervised learning methods. It is used for both classification and regression tasks. We will create a model for predicting the value of a variable (target) by learning some simple decision rules concluded from the features of the data [15].

3.4 Support Vector Machine (SVM)

SVM constructs a hyper plane for classification and regression in a high-dimensional space. The ideal hyper plane will give the largest margin distance which separates the two object groups. It is a no probabilistic binary classifier. SVMs are only applied in diagnosis with low number of samples since the number of support vectors in large datasets will be more [16].

3.5 Random Forest (RF)

It is a process that operates among multiple decision trees for an optimum result by selecting the majority among those as our best value. It searches for the best feature among a random subset of features [17]. Random forest is a classifier that contains a number of decision trees on various subsets of the given dataset and will take the average value to improve the accuracy of prediction of the dataset.

3.6 K-Nearest Neighbor (KNN)

The method will assume the similarity between the new case or data and available data and assign the new case into the particular category that will be most similar to the categories available. We can say that similar things are close to each other. It calculates the distance between a pair of records.

Above six algorithms were analysed by their common working principles and the pros and cons were listed (see Table 1).

4 Literature Review

Classification algorithms have vital role in the prediction analysis of automatic medical health diagnoses. We have done a review of the articles presented in Google scholar and noted the performance of different algorithms in the diagnosis of HCC and other related liver diseases.

A study on Egyptian citizen with HCV related prediction of HCC shows that decision tree algorithm was effective for the diagnosis of HCC having sensitivity level of 83.5%, Precision (specificity) 83.3% by the usage of routine data [18] Study done by [19] (ROC) curve showed that it is reaching at 0.75 approximately. In the supervised models of machine learning, the statistics of ROC curve have reached the value of 0.852 by using the RF model and 0.833 by the adaptive boosting model. Hintay, Ba-Alwi [20] reported a comparative examination on the diagnosis of hepatitis disease. Naive Bayes, Logistic Regression algorithms were analyzed. Results of classification were taken in terms of time and precision. Analysis study was mainly done using WEKA. Naive Bayes exhibited accuracy level 96.52%. Logistic regression provided 83.6%. Naive Bayes was the best algorithm found when used rough set. Naive Bayes produced correctness (precision) 61.28% and SVM gave 79.66% when Gulia et al. [21] compared different methods to classify liver patients. RF, SVM as well as Bayesian Network were there for comparison. SVM expressed 71.35%, Random forest—71.87% and Bayes Net produced 69.13% accuracy. Vijayarani with Dhayanand [22] were used both support vector machine and Naive Bayes classification algorithms for the predictive liver disease. Using MATLAB data analysis was

Table 1 Advantages and disadvantages of various machine learning algorithms

Algorithm	Advantages	Disadvantages
Logistic Regression	Easy implement and train Can extend to multiple classes Fast Classification of unknown records and accuracy is good for simple data sets Provides both the direction of association (positive or negative)	Can't use when the number of observations is lesser than the number of features Constructs linear boundaries Only be used to predict discrete functions Nonlinear problems could not be solved
Naïve Bayes	Works fast and can save time solving multi-class prediction problems small amount of training data Easy to implement	Assumption of independent predictors Here assumes that all the attributes are mutually independent Problem of zero probability
Decision Tree	Normalization not required Implementation can be done without data scaling Impute the missing values is not necessary Takes less time to handle both categorical and numerical variables	Require more memory for calculation Even very small changes in the data will interpret large changes in the structure of the tree The time and space complexity is high Takes more training time
SVM	More accuracy in prediction Need small number of parameters and target estimation is fast	Comparatively takes more time to train on large data set Difficult to function on large sets of data
Random Forest	less prone to over fitting It can accept both categorical and continuous data values and automates missing values seen in the data Normalizing of data is not required	Computations are complex More computation time Large number of decision trees is used to determine the class
K-Nearest Neighbor	Classification is good if samples are huge Can be applied to data form of any distribution	Testing demands more memory No training; the work will be done in testing phase

done. Naive Bayes resulted 61.28% accuracy and SVM brought 79.66% accuracy. Another study [23] for prediction of HCC using computer tomography suggested that the SVM showed the highest accuracy over 88%. The study done by [24] for therapeutic outcome prediction using SVM, Decision Tree, Bayesian and Random forest. The SVM model had an accuracy of 82.1% over 8 features, while other algorithms were shown less accuracy. Another study [25] on ML algorithms to predict liver disease The accuracy of RF, NB and LR were 87.48, 82.65 and 76.96%, respectively. Another prediction using Alpha feto protein negative HCC prediction multicentre study was done [26]. Among three ML approaches, LR performed the best for identifying ANHCC in training group (LR showed 0.842 value in AUC, 95% CI

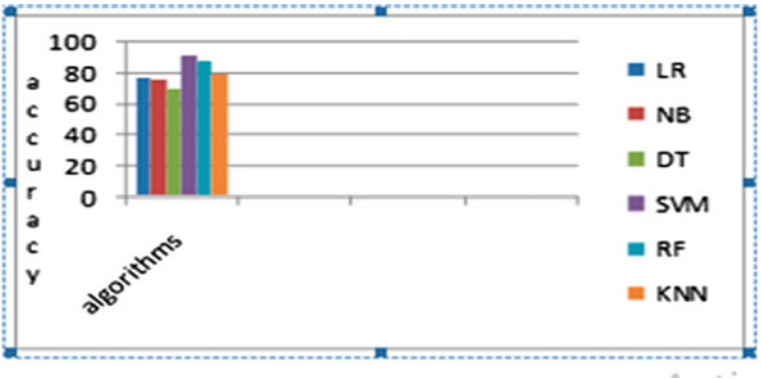


Fig. 1 Accuracy level of different ML algorithms

was 0.784–0.899; then RF showed AUC of 0.825, 95% CI was 0.766–0.885; also SVM had AUC of 0.610, 95% CI value 0.527–0.684). A high-diagnostic performance was showed by LR, in independent validation also (0.860 in AUC, 95% CI in 0.824–0.897).

A comparative study of SVM and random forest by [27] revealed that SVM and RF shows respective accuracy percentage of 90 and 100. Optimization study was carried out by [28] and it was observed that the evaluation values of performance were area under curve (AUC) for naive Bayes algorithm was 72.5% and k-nearest neighbor (KNN) had 63.19%. There are various other studies using relevant biomarkers in the prediction study of hepatocellular carcinoma and other liver disorders. Yet another study [29] showed that serum biomarkers in the chronic hepatitis B, LC and HCC diagnosis showed 94.28% specify and [30] showed that DT has more than 85% accuracy in HCC prediction. Ali et al. [31] also proves the capability of SVM in optimized manner (Fig. 1).

5 Conclusion

In the survey, we have gone through the risk of NAFLD and HCC and the need to find out a best method of algorithm for the early detection of liver diseases. Various prediction methods were analyzed and taken into study. It was found that more studies were done in this area by data mining algorithms and their modified versions by taking bio markers using non-invasive procedures than invasive as liver biopsy is not a best path for fibrosis findings since the cells which are affected may be unevenly distributed in the liver mass and tested fragments may not holding that cells. Here, we have analyzed the working method of six different machine learning algorithms on non-invasive markers and found that SVM algorithm is having more accuracy

rate compared to other algorithms, and it is used more in prediction analysis. The scope lies in the prediction using less non-invasive biomarkers with ML.

References

1. S. Mittal, H.B. El-Serag, Epidemiology of HCC: consider the population. J. Clin. Gastroenterol. **47**, S2 (2013)
2. Q.M. Anstee, H.L. Reeves, E. Kotsiliti, O. Govaere, M. Heikenwalder, From NASH to HCC: current concepts and future challenges. Nat. Rev. Gastroenterol. Hepatol. **16**(7), 411–428 (2019)
3. B. Cariou, C.D. Byrne, R. Loomba, A.J. Sanyal, Nonalcoholic fatty liver disease as a metabolic disease in humans: a literature review. Diabetes Obes. Metab. **23**(5), 1069–1083 (2021)
4. B.A. Neuschwander-Tetri, Non-alcoholic fatty liver disease. BMC Med. **15**(1), 1–6 (2017)
5. J.A. Flemming, J.D. Yang, E. Vittinghoff, W.R. Kim, N.A. Terrault, Risk prediction of hepatocellular carcinoma in patients with cirrhosis: the ADRESS-HCC risk model. Cancer **120**(22), 3485–3493 (2014)
6. F. Negro, Natural history of NASH and HCC. Liver Int. **40**, 72–76 (2020)
7. S. Myers, I. Neyroud-Caspar, L. Spahr, K. Gkouvatsos, E. Fournier, E. Giostra, N. Goossens, et al., NAFLD and MAFLD as emerging causes of HCC: a populational study. JHEP Rep. **3**(2), 100231 (2021)
8. European Association for Study of Liver, EASL-ALEH Clinical Practice Guidelines: non-invasive tests for evaluation of liver disease severity and prognosis. J. Hepatol. **63**(1), 237–264 (2015)
9. V.A. Piazzolla, A. Mangia, Noninvasive diagnosis of NAFLD and NASH. Cells **9**(4), 1005 (2020)
10. M. Yoneda, K. Imajo, H. Takahashi, Y. Ogawa, Y. Eguchi, Y. Sumida, A. Nakajima, et al., Clinical strategy of diagnosing and following patients with nonalcoholic fatty liver disease based on invasive and noninvasive methods. J. Gastroenterol. **53**(2), 181–196(2018)
11. T.H. Su, C.H. Wu, J.H. Kao, Artificial intelligence in precision medicine in hepatology. J. Gastroenterol. Hepatol. **36**(3), 569–580 (2021)
12. R. Shouval, O. Bondi, H. Mishan, A. Shimoni, R. Unger, A. Nagler, Application of machine learning algorithms for clinical predictive modeling: a data-mining approach in SCT. Bone Marrow Transplant. **49**(3), 332–337 (2014)
13. Logistic Regression, Retrieve from https://www.saedsayad.com/logistic_regression.htm. Last accessed 2021/06/08
14. S.R. Ghosh, S. Waheed, Analysis of classification algorithms for liver disease diagnosis. J. Sci. Technol. Environ. Inform. **5**(1), 360–370 (2017)
15. Decision Tree, Retrieve from https://dataaspirant.com/how-decision-tree-algorithm-works. Last accessed 2021/06/09
16. X. Wu, V. Kumar, J.R. Quinlan, J. Ghosh, Q. Yang, H. Motoda, D. Steinberg, et al., Top 10 algorithms in data mining. Knowl. Inform. Syst. **14**(1), 1–37 (2008)
17. L. Breiman, Bagging predictors. Mach. Learn. **24**(2), 123–140 (1996)
18. D.A.E.H. Omran, A.H. Awad, M.A.E.R. Mabrouk, A.F. Soliman, A.O.A. Aziz, Application of data mining techniques to explore predictors of HCC in Egyptian patients with HCV-related chronic liver disease. Asian Pac. J. Cancer Prev. **16**(1), 381–385 (2015)
19. Y.J. Lin, R.J. Chen, J.H. Tang, C.S. Yu, J.L. Wu, L.C. Chen, S.S. Chang, Machine-learning monitoring system for predicting mortality among patients with non-cancer end-stage liver disease: retrospective study. JMIR Med. Inform. **8**(10), e24305 (2020)
20. F.M. Ba-Alwi, H.M. Hintaya, Comparative study for analysis the prognostic in hepatitis data: data mining approach. Int. J. Sci. Eng. Res. **4**(8), 680–685 (2013)

21. A. Gulia, R. Vohra, P. Rani, Liver patient classification using intelligent techniques. Int. J. Comput. Sci. Inform. Technol. **5**(4), 5110–5115 (2014)
22. S. Vijayarani, S. Dhayanand, Liver disease prediction using SVM and Naïve Bayes algorithms. Int. J. Sci. Eng. Technol. Res. (IJSETR)**4**(4), 816–820 (2015)
23. M. Sato, R. Tateishi, Y. Yatomi, K. Koike, Artificial intelligence in the diagnosis and management of hepatocellular carcinoma. J. Gastroenterol. Hepatol. **36**(3), 551–560 (2021)
24. Z.M. Zou, D.H. Chang, H. Liu, Y.D. Xiao, Current updates in machine learning in the prediction of therapeutic outcome of hepatocellular carcinoma: what should we know? Insights Imag. **12**(1), 1–13 (2021)
25. C.C. Wu, W.C. Yeh, W.D. Hsu, M.M. Islam, P.A.A. Nguyen, T.N. Poly, Y.C.J. Li, Prediction of fatty liver disease using machine learning algorithms. Comput. Methods programs Biomed. **170**, 23–29(2019)
26. C. Huang, M. Fang, H. Feng, L. Liu, Y. Li, X. Xu, C. Gao, et al., N-glycan fingerprint predicts alpha-fetoprotein negative hepatocellular carcinoma: a large-scale multicenter study. Int. J. Cancer (2021)
27. V.V.P. Wibowo, Z. Rustam, S. Hartini, Q.S. Setiawan, J.E. Aurelia, Comparison between Support Vector Machine and Random Forest for Hepatocellular Carcinoma (HCC) Classification, in *2020 International Conference on Decision Aid Sciences and Application (DASA)* (IEEE, 2020), pp. 618–622
28. H. Hartatik, M.B. Tamam, A. Setyanto, Prediction for diagnosing liver disease in patients using KNN and Naïve Bayes algorithms, in *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)* (IEEE, 2020), pp. 1–5
29. J. Cui, X. Kang, Z. Dai, C. Huang, H. Zhou, K. Guo, Y. Liu, et al., Prediction of chronic hepatitis B, liver cirrhosis and hepatocellular carcinoma by SELDI-based serum decision tree classification. J. Cancer Res. Clin. Oncol. **133**(11), 825–834 (2007)
30. M.E. Khameneh, M.M. Sepehri, M. Saberifiroozi, Using data mining for identify patients at high risk to hepatocellular carcinoma in the cirrhosis liver: preliminary report. Govaresh **19**(4), 265–274 (2014)
31. L. Ali, I. Wajahat, N.A. Golilarz, F. Keshtkar, S.A.C. Bukhari, LDA–GA–SVM: improved hepatocellular carcinoma prediction through dimensionality reduction and genetically optimized support vector machine. Neural Comput. Appl. **33**(7), 2783–2792 (2021)

Implementation of UVM Agents for Hexagon Subsystem RTL



Keerti Umesh Sankangoudar, K. Sowmya Nag, and Anshul Sharma

Abstract Verification is a major bottleneck in the design of complex system designs, accounting for nearly 70% of the project development period. Directed test verification is currently a tedious, time-consuming, and repetitive task for verifying complex systems, and many uncovered scenarios will be left out. So, it is necessary to construct robust, scalable, and reusable SoC verification environment. Universal Verification Methodology (UVM) along with SystemVerilog work together to build a coverage-driven constrained random environment for verification. In this paper, UVM test bench is implemented for verifying the frequency generated from PLL, which in turn is used as the clock source for QDSP core, hence enhancing the reusability of verification components. PLLs (Phase Lock Loop) are an integral part in almost all SoCs, used as a frequency synthesizer. And the output of PLL is fed to the Clock Generator along with 2 different clock sources. Clock Generator is a mini clock macro used to generate the clock root which takes in 2 other raw clock sources. Clock Generator contains source muxing and clock divide (integer, half integer, fractional divide) ability.

Keywords UVM · SoC · PLL · DSP · UVC · Coverage-driven verification · Systemverilog

1 Introduction

SystemVerilog has a robust framework for generating random stimuli. The SystemVerilog testbench environment in Fig. 1 is based on class-object randomization, which means that random variables of a class-object are automatically

K. U. Sankangoudar (✉) · K. S. Nag
Department of ECE, R V College of Engineering, Bengaluru 560059, India

K. S. Nag
e-mail: sowmyanagk@rvce.edu.in

A. Sharma
DSP, Qualcomm India Pvt. Ltd, Bengaluru 560037, India
e-mail: anshrma@qti.qualcomm.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_76

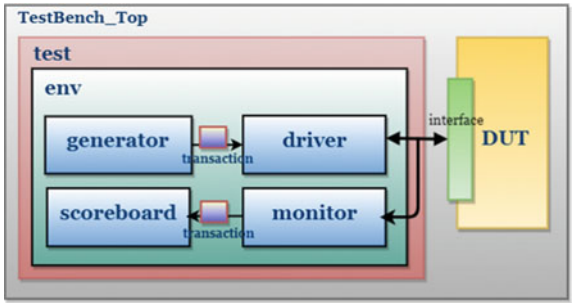


Fig. 1 SystemVerilog testbench environment

randomized by calling the object's predefined randomize process. Constraints help the randomization feature even further. These constraints determine the boundaries within which the randomization function operates. UVM is a structured technique that describes the standard practices in verification that enhances productivity by significantly reducing the product development cycle and is currently part of the IEEE 1800.2 [1].

Figure 2 depicts the SystemVerilog UVM testbench environment, which promises to increase verification efficiency by allowing teams to share tests and testbenches across projects. It is also a powerful methodology for using constrained randomization to achieve higher functional coverage goals and to explore combinations of tests without having to write each one separately [2].

RTL bugs are very difficult to find, and debug takes more time. There has been a huge demand to reduce time to market and verification time, UVM compliant testbench would serve the purpose. UVM Testbench detects bugs in the design if any at a very early stage of the project with a much minimal manual effort. UVM testbench can generate number of stimuli with less manual efforts and help to capture Functional coverage which is measure of verification. Thus, UVM compliant testbench is built to verify the frequency generated from PLL.

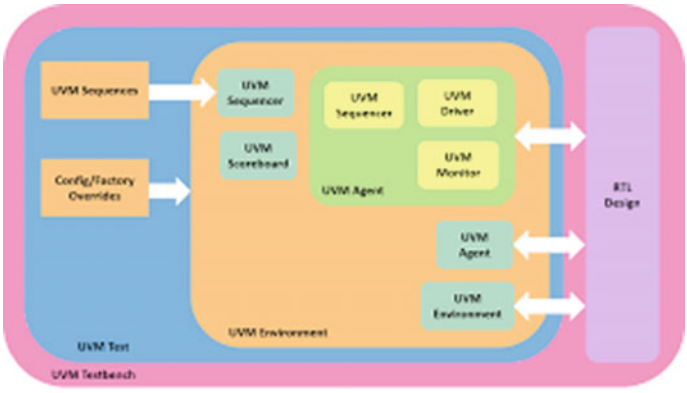


Fig. 2 UVM Verification testbench environment

The main importance of UVM-based environment is:

1. Modularity and Reusability—UVM methodology has modular components (Driver, Sequencer, Agents, Environment, etc.) that allow components to be reused from unit to multi-unit or chip level verification as well as across projects [2].
2. Separation of tests from testbenches—Testcases and the testbench environment are kept apart, that helps in reusability of stimulus across projects and units [3].
3. Simulator Independent—UVM is the methodology that is not a simulator dependent. UVM class library is supported by almost all simulators [4].
4. UVM's factory mechanisms make it easier to modify modules and creating each one with a factory allows them to be overridden in various tests or environments without having to change the underlying base code. Among the many different frequency synthesis methods, the digital PLL circuit is the most widely used in the wireless communications industry.

2 PLL and Clock Generator

The Hexagon DSP subsystem contains a digital PLL to generate QDSP6 core clock source. The PLL supports a Voltage-Controlled Oscillator (VCO) clock frequency slew, without the need to turn off the PLL output.

There is sequence of steps followed to switch the QDSP6 clock source from default clock frequency to PLL clock frequency and to change the target output frequency while the PLL is in RUN mode. These sequences change between the technology.

The PLL will slew from the original output frequency to the new target frequency without introducing any glitches. The block clocked by the PLL can continue to do computations while the PLL's frequency is changing. However, the lock time will likely be longer than if the target output frequency was changed while the PLL is in STANDBY mode.

The PLL circuit uses a negative feedback mechanism to perform frequency multiplication to produce the output frequency, f_{out}, in terms of the phase detector reference frequency, f_{ref}.

$$f_{\text{out}} = N \times f_{\text{ref}}$$

where N is integer value. The synthesizer's output frequency, f_{out}, can be tuned to the required by reprogramming the divider N. The VCO can be tuned around the frequency band of interest by adjusting the value N. In this paper, N is referred as pll_value.

Clock generator shown in Fig. 3 contains source muxing and clock divide (integer, fractional divide) ability, depending on the src_sel, particular clock source is selected as QDSP6_clk, as shown in Table 1.

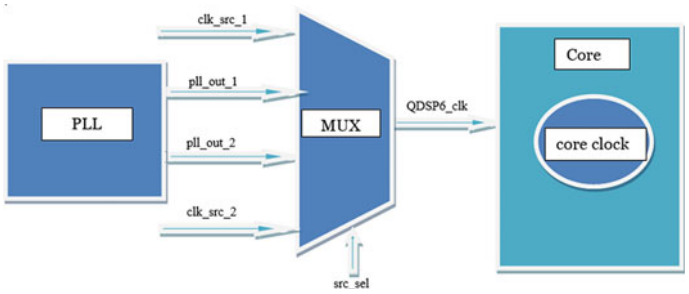


Fig. 3 PLL and clock generation unit

Table 1 Clock sources with their src_sel values

src_sel	QDSP6_clk
1	pll_out_1
2	pll_out_2
3	clk_src_1
4	clk_src_2

3 UVM

(1) UVM Base Class Library
The UVM testbench environment includes a large class library that aids in the development of well-designed, scalable, and reusable verification components. *uvm_component* [5, 6].
The UVM component class is the base class for all verification components that exists during the simulation.

(i) Sequencer
The UVM Sequencer acts as an arbiter by regulating the flow of UVM Sequence Item transactions produced by one or more UVM Sequences.

(ii) Driver
The UVM Driver receives UVM Sequence Item transactions from the UVM Sequencer and supplies it to the DUV through virtual interface.

(iii) Monitor
The UVM Monitor observes the pin level transitions on the DUV interface, converts the pin level transitions to high-level transitions and broadcast the captured information to components connected to the analysis port of the Monitor such as Scoreboard, Coverage collector.

(iv) Agent
The UVM Agent is a wrapper class that encapsulates a UVM Sequencer to deliver the stimulus to the Driver, a UVM Driver to receive and convert the high-level transactions into pin level actions, and a UVM Monitor to monitor the pin level transitions on the virtual interface.

The active agent includes driver, sequencer and monitor that drives the transaction whereas the passive agent is meant to monitor the transaction and responses.

(v) Scoreboard
The UVM Scoreboard collects transactions from all the Monitors. It usually receives transactions carrying inputs and outputs of the DUT through UVM Agent analysis ports, runs the input transactions through a reference model to produce expected transactions, and then compares the actual output versus the expected output.

(vi) Environment
The UVM Environment is a container class which may contain multiple agents for different interface and is a hierarchical component that groups together other verification components that are interrelated.

(2) *uvm_transaction*
uvm transaction class is extended from uvm object class and is a root base class for all UVM transaction. They are used to create data items. uvm sequence item is the base class from which all the transaction items are extended, which itself is extended from uvm_transaction.

(3) *uvm_sequence*
The uvm_sequence class provides the interfaces which are necessary to create streams of sequence items and/or other sequences.

(4) *uvm_sequence_item*
The sequence item is built up of data fields that are randomized to generate the stimulus.

(5) *uvm_phases*

- ***build phase***: The main purpose is to construct testbench components. All the build phase methods run in top-down style.
- ***connect phase***: The order of execution of this phase is in bottom-up manner. The TLM ports of components are connected in this phase.
- ***end of elaboration phase***: This phase executes after the connect phase completes. At this point, entire testbench is built and connected. UVCs can do final checks for proper connectivity.
- ***Start of simulation phase***: It executes at zero simulation time. At this point, elaboration phase has been completed and testbench is about to start the simulation. This phase executes in bottom-up manner.
- ***run phase***: Run tasks in all the universal verification components run in parallel. This is the only phase that consumes time, hence it is declared as task.
- ***extract phase***: The extract phase collects and processes the results of the simulation, which is obtained from Scoreboards and Functional Coverage Monitors.
- ***Check phase***: The check phase executes after the run and extract phase completes. This phase is used to check the correctness of the extracted data.

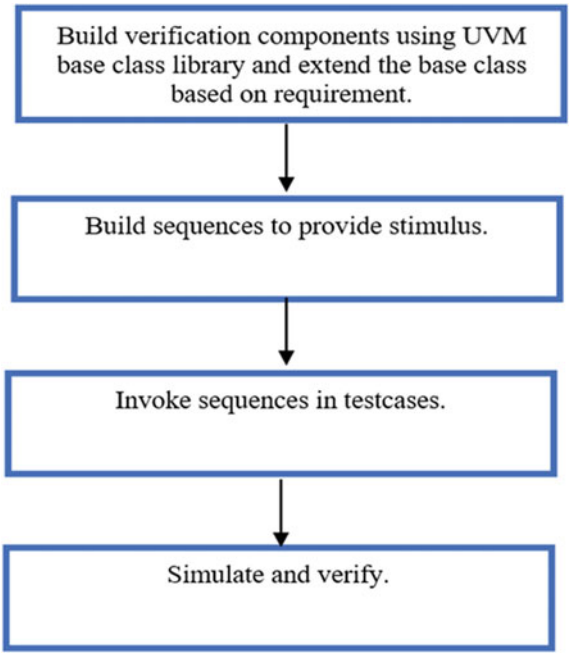


Fig. 4 Verification flow to build UVM PLL agent

- ***report phase***: The simulation results are displayed on the standard output or written to a file during the report phase. Analysis Components are the most common users of this phase.
- ***final phase***: The final phase is meant for the testbench to complete any outstanding task that is left out (Fig. 4).

4 UVM Testbench for PLL

In this section, all UVM verification components shown in Fig. 5 are built to verify the generated clock frequency against the expected clock frequency. PLL output clock frequency such as pllout_1 and pllout_2, clk_src_1 and clk_src_2 is fed to the MUX. Depending on the value of the select line particular input is selected as the QDSP6 core clock. The MUX enables dynamic clock switching among the clock sources without a glitch. It can also divide the clock frequency. Figure 4 shows the sequence of steps that is followed in order to build UVM agent for PLL.

The purpose of each UVM Component is explained below:

- **Env**

The pll_enviroment is a user-defined wrapper class which is derived from uvm_env. The pll_environment is a container component for grouping higher level components like pll_agent and pll_scoreboard.

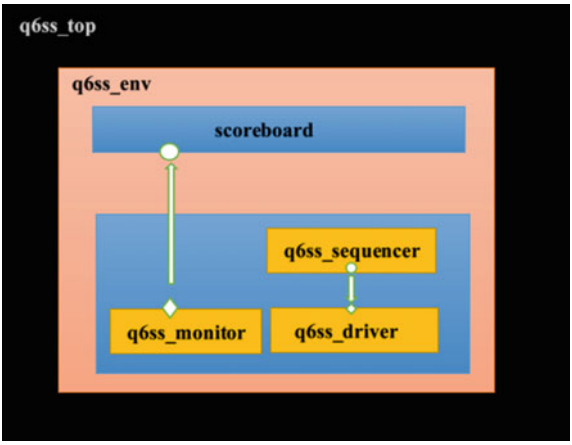


Fig. 5 UVM compliant testbench structure

- **Agent**

The pll_agent is a custom class which is inherited from uvm_agent. Agent being the component is registered with factory using a macro 'uvm_component_utils.

In the build_phase, since pll_agent is active, pll_sequencer, pll_driver and pll_monitor is created. In the connect phase, the driver seq_item_port is connected to the sequencer seq_item_export for any transaction between the driver and the sequencer. The pll_sequencer manages stimulus flow, a pll_driver follows sequence of steps to generate the frequency, and a pll_monitor to monitor the generated frequency.

- **sequence_item**

The class contains all the pll and clock generator-related configurations, which are randomized and constrained.

- **Driver**

The pll_driver class contains all the dummy pll-related functions and which is overridden by specific technology pll driver in the env to enhance the reusability of the verification components.

PLL specific driver contains the sequence of steps to be followed to generate the frequency. Since these depend on the technology, as the technology changes the existing driver can be overwritten by the new one in the pll_env. This makes the verification more efficient with maximum reusability.

- **Sequence_lib**

The data items that must be produced and sent/received to/from the driver are described by the sequences.

The various sequences are:

- Sequence to generate pll frequency by dynamically varying pll_l value.

- Sequence to exercise all valid clock sources.
- **Sequencer**

It is in charge of routing the data packets (sequence_item) generated in the sequence to the driver or vice versa.

- **Monitor**

In the run_phase of monitor, the following steps have been carried out,

(a) DSP Core and pll must be out of reset to proceed for frequency calculations.
(b) PLL and clock generator-related configurations like pll_value, src_div and src_sel is obtained from interface.
(c) clk_measure() task is called after PLL locks to the new frequency.
(d) clk_measure task

- Measure the time period and the rise time of the QDSP6 clock for 20 times (random) to obtain the accurate value.
- Calculates the average time period and average rise time of the QDP6 clock signal.

(e) Calculated time period and rise time is sent to the scoreboard for comparison of calculated versus expected clock frequency.

- **pll_scoreboard**

Sequence of steps to create the pll_scoreboard.

a. This class is inherited from uvm_scoreboard and is registered with the factory and function new is called.
b. Create the required TLM exports in build phase to receive transactions from other components.
c. TLM exports are created in the build phase to retrieve transactions from other UVCs.
d. Define the action to be taken when the data is received from the analysis port.
e. Perform checks.

Real checkers are not expected to check only during the check phase; they can also actively check during the run phase.

f. Connect the scoreboard's analysis port to other components in the environment. pll_scoreboard consists of write method, build, extract, and check phase. The scoreboard's write method will obtain the transaction packet from the monitor and determine the action to be taken when data from the analysis port is received.

- build phase: Creates and instantiates the required TLM exports to accept transactions from other components.
- extract phase: QDSP6 Clock frequency is calculated after receiving the t_period and rise time of the QDSP6 clock. Among all the calculated frequency for a particular pll_value, max is selected and sent to the check phase.

Table 2 Expected frequency versus calculated frequency

pll_value	Calculated frequency (clock_freq) MHz	Expected frequency (clock_freq) MHz
16'h32	966	960

- check phase: Compare the obtained frequency from extract phase with the expected frequency.

Calculation of Expected Frequency for PLL Outputs:

$$\text{Expected QDSP6 Clock Frequency} = \frac{\text{Standard Clock Frequency (19.2 MHz)} \times \text{pll_value (decimal)}}{\text{src_div}}$$

Calculation of Expected Frequency for Non-PLL Outputs:

$$\text{Expected QDSP6 Clock Frequency} = \frac{\text{Clock Source Frequency (MHz)}}{\text{src_div}}$$

Example If pll_value is 16'h32 which is 50 in decimal, So the Expected clock frequency = 19.2 MHz × 50 = 960 MHz Same is shown in Table 2.

5 Simulation Results

The maximum frequency range that the PLL Agent can generate with src_div = 1 ranges between 288 and 960 MHz. To get this frequency range, the constraints for sequence_items are mentioned in Table 3.

Table 4 shows the output for the sequence, meant to exercise all the valid clock sources. It shows the frequency change while transiting among various clock sources (pll_out_1, pll_out_2, clk_src_1, clk_src_2).

For example, src_sel = 1, the particular clock source, that is pll_out_1 is selected and fed to the clock generator block which acts as a mux. Since src_div = 'h3 which is mapped to the value 2. The pll_out_1 clock frequency is divided by the src_div which is the QDSP Clock.

Table 3 Constraints of sequence items

seq_items	Constraints
pll_value	pll_value inside {['hf:'h32]}
src_sel	src_sel inside {[3'h1:3'h4]}
src_div	src_div inside {['5h0:'5h1F]}

Table 4 QDSP6 clock frequency for different clock sources

src_sel	src_div	Clock source	Clock frequency (MHz)	QDSP6 frequency (MHz)
1	3(2)	Pll_out_1	966.18	480.877
3	A(5.5)	clk_src_1	576.037	90.900
2	1c(14.5)	Pll_out_2	519.211	35.801
4	0(1)	clk_src_2	846.024	200.000

- Constraints for exercising all clock sources with randomized pll_values are listed below.

```
'uvm_do_on_with(req,p_sequencer.m_pll_rcg_sequencer_h,{req.src_sel == 'h1;}).
'uvm_do_on_with(req,p_sequencer.m_pll_rcg_sequencer_h,{req.src_sel == 'h3;}).
'uvm_do_on_with(req,p_sequencer.m_pll_rcg_sequencer_h,{req.src_sel == 'h2;}).
'uvm_do_on_with(req,p_sequencer.m_pll_rcg_sequencer_h,{req.src_sel == 'h4;}).
```

In Fig. 6, since src_sel = 1, pll_out_1 clock source with frequency 966.18 MHz is divided by 2 since src_siv = 'h3 which results in 480.77 MHz which is nothing but the QDSP6 clock frequency.

Calculation of Expected frequency for PLL outputs:

$$\text{Expected QDSP6 Clock Frequency} = \frac{\text{Standard Clock Frequency (19.2 MHz)} \times \text{pll_value (decimal)}}{\text{src_div}}$$

$$\text{Expected QDSP6 Clock Frequency} = \frac{19.2\,\text{MHz} \times 50)}{2} = 480\,\text{MHz}$$

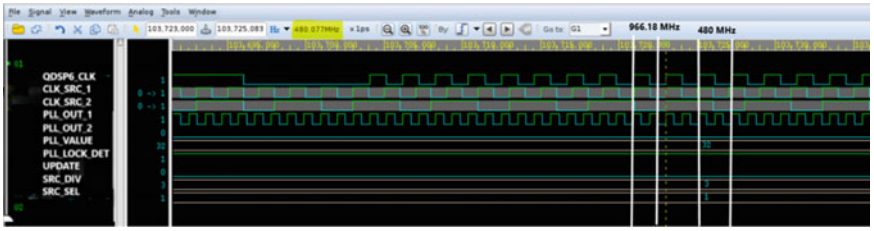


Fig. 6 QDSP6 clock frequency change w.r.t src_sel

6 Conclusion and Future Scope

Universal Verification Methodology (UVM) along with SystemVerilog work together to build a coverage-driven constrained random environment for verification. In this work, to enhance the reusability of verification environment, UVM testbench is implemented for verifying the frequency generated from PLL.

As PLL depends on the technology, whenever the PLL technology changes from one project to another, by making use of UVM compliant testbench the whole setup remains the same, only the existing driver is overwritten by the new driver. Thus, UVM makes verification more efficient with maximum reusability. Based on the study of the UVM typical verification platform and UVM methodology to achieve reusable method, this paper builds a reusable verification platform of PLL.

Currently, the pll_environment has pll_agent along with scoreboard. UVM configuration database can be used to set more controllable for verification components.

References

1. T.M. Pavithran, R. Bhakthavatchalu, UVM based testbench architecture for logic sub-system verification, in *IEEE International Conference on Technological Advancements in Power and Energy* (2017)
2. S. Rosenberg, K. Meade, *A Practical Guide to Adopting the Universal Verification Methodology (UVM)*, 2nd edn. (Cadence Design Systems, San Jose, 2010)
3. S. Jain, P. Govani, K.B. Poddar, A.K. Lal, R.M. Parmar, Functional verification of DSP based On-board VLSI designs, in *International Conference of VLSI Systems, Architectures, Technology and Applications (VLSI-SATA)* (2016)
4. J. Bromley, If SystemVerilog is so good, why do we need the UVM? Sharing Responsibilities between Libraries and the core language, in *Proceedings of the 2013 Forum on specification and Design Languages FD* (2013)
5. K. Salah, A UVM-based smart functional verification platform: concepts, Pros, Cons, and Opportunities, in *9th International Design and Test Symposium (DTS)* (2014)
6. W. Ni, J. Zhang, Research of reusability based on UVM verification, in *IEEE International Conference on ASIC* (2015)

Hybrid Intrusion Detection System for Detecting DDoS Attacks on Web Applications Using Machine Learning

Madhura Shekhar Potnis, Sanjyot Kedar Sathe, Purva Govind Tugaonkar, Gayatri Laxmikant Kulkarni, and Shilpa Shrikant Deshpande

Abstract Due to tremendous rise in the use of microservices and smart devices, there has been an increase in distributed denial of service (DDoS) attacks. Distributed denial of service is the attack where the perpetrator aims to make a network resource or machine unavailable to its users for its services. The detection of these attacks is not very effective due to manual configuration errors and predefined rule sets. This paper proposes a hybrid web intrusion detection system (HWIDS) which detects DDoS attacks. The system focuses on detection of five different types of hypertext transfer protocol (HTTP) based application layer DDoS attacks and unknown variants of these known attacks. An ensemble learning technique is used to combine the advantages of multiple algorithms. The results show that the ensemble learning model has an accuracy of 95.96% and false negative rate of 4.10% for detecting known attacks. The system has an accuracy of 93.48% and false negative rate of 6.52% in detecting unknown attacks. As given by the result statistics, the system detects known attacks and unknown variants of known attacks with high accuracy and no human intervention, providing an advantage in curbing the adverse effects of the security breach.

Keywords Anomaly detection · Application layer · Distributed denial of service (DDoS) · Ensemble learning · Machine learning · Signature detection · Web application

M. S. Potnis (✉) · S. K. Sathe · P. G. Tugaonkar · G. L. Kulkarni · S. S. Deshpande
Department of Computer Engineering, Cummins College of Engineering for Women, Pune, India
e-mail: madhura.potnis@cumminscollege.in

S. K. Sathe
e-mail: sanjyot.sathe@cumminscollege.in

P. G. Tugaonkar
e-mail: purva.tugaonkar@cumminscollege.in

G. L. Kulkarni
e-mail: gayatri.l.kulkarni@cumminscollege.in

S. S. Deshpande
e-mail: shilpa.deshpande@cumminscollege.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_77

1 Introduction

Digital technology has progressed at a very fast pace, reaching around half of the developing World's population in just two decades [1]. This has consequently led to an increase in distributed denial of service (DDoS) attacks. Over the last decade, the world has seen a significant growth in the size and frequency of DDoS attacks. GitHub was a victim to a large DDoS attack, of size 1.3 TBPS, in February 2018 [2]. The detection of these attacks is not very effective due to manual configuration errors and predefined rule sets for attack detection.

The ineffectiveness in detecting the attacks not only wastes processing power and time of the systems but also businesses lose massive money due to such attacks. Recent studies suggest that DDoS attacks are rising, mainly hypertext transfer protocol (HTTP) based application layer attacks as they are highly scalable [3]. Use of machine learning algorithms will significantly reduce the inaccuracy in detecting and mitigating the DDoS attacks.

Recently, various machine learning (ML) algorithms have been applied to detect DDoS attacks. However, every algorithm has its own vantage points and shortcomings. Instead of a single algorithm, multiple algorithms may be used for detection of DDoS attacks by combining the advantages of each algorithm.

Research indicates that detecting zero day [4] or unknown attacks has always been a challenge for prevalent intrusion detection systems (IDS). Much work needs to be done in improving the detection of attacks.

Keeping these improvement areas in mind, this paper presents a hybrid web intrusion detection system (HWIDS) which detects DDoS attacks on web applications by using an ensemble machine learning model. The system uses a hybrid approach for detection, that is, it uses anomaly based as well as signature-based detection methods. The system is also tested for the detection of attacks previously unknown to the system. These unknown attacks are further stored to retrain the ML models to detect these in future.

In the rest of this paper, the HWIDS is discussed in detail. Section 2 describes the related work and a summary of relevant literature. Section 3 describes the architecture of the HWIDS. Section 4 discusses the implementation aspects of the HWIDS. Section 5 summarizes the results obtained. Section 6 concludes the paper.

2 Literature Review

After an extensive study of available literature, work related to detecting DDoS attacks, ML techniques for detection of DDoS attacks and intrusion detection systems was found. Between January 2014 and December 2018, the authors of the paper [5] studied 12 detection methods of application layer DDoS attacks. This paper emphasized the importance of choosing the right parameters for the detection of HTTP DDoS attacks. Munivara et al. [6] presented a broad classification of various

DDoS attacks and various defensive techniques. Several detection and mitigation techniques such as soft-computing based, statistical based, data mining based and knowledge based have been reviewed with their advantages and disadvantages.

Karanjeet et al. [7] surveyed the literature available to recognize application layer HTTP-GET flood DDoS attacks. They aimed to provide state-of-the-art protection mechanisms against such attacks. They concluded that there are challenges in detection of different types of DDoS attacks. These challenges need to be identified and overcome in every strategy. The origin of DDoS attacks along with some of the detection methods were introduced by authors in [8]. They also introduced the methods for prevention of these attacks. Most of the methods focused on attack traffic detection along with filtering near the target.

Chonka et al. [9] presented intelligent decision prototype (IDP). The pre-marking decision (PMD) mechanism provided is used for evaluation of a packet. The packet is evaluated before it is marked for traceback purposes. In the paper [10], the authors, Wankhede and Kshirsagar aimed to detect DoS attacks effectively using machine learning and neural network (NN) algorithms such as Random Forest and Multilayer Perceptron (MLP), respectively. The results showed that, Random Forest algorithm provides higher accuracy than the MLP algorithm. It classified traffic as benign or attack and does not classify the type of attack further.

The paper [11] offered a comparison of the performances of different supervised machine learning classifiers. The classifiers are Random Forest, Gaussian Naïve Bayes (GNB), K nearest neighbor and Support Vector Machine (SVM). They concluded that the best performing classifier to detect DDoS attacks is the Random Forest classifier. In [12], the authors proposed a solution for a DoS prevention system based on various machine learning techniques. In the experimental results, it is shown that more than 99.7% of four different types of DOS attacks are successfully detected: brute-force attacks, flooding attacks and spoofing.

The paper by Nancy Agarwal and Syed Zeeshan Hussain [13] presented a framework for intrusion detection in web applications. It also compared the framework to the features of some current systems. In the paper [14], a comparison of hybrid intrusion detection systems (H-IDS) was carried out. The objective in the paper was to compare the performances. The authors isolated the weaknesses of the systems, such as drawbacks associated with single classifier models, which include the inability to detect all classes of attacks, which leads to misclassification.

In [15], the author proposed a H-IDS which used signature-based as well as anomaly based methods for detection. In that, anomaly detection (using Gaussian mixture models) and signature detection (using SNORT) were done in a parallel fashion. The results from both detectors are then combined to give final output. The performance for detecting the attacks over the binary set of data of ML based anomaly intrusion detection system (AIDS) models is reviewed and tested by the authors of [16]. The paper proposed the use of various supervised and unsupervised ML algorithms such as ANN, k-NN, RF, DT, CNN, SOM, SVM, EM, NB. These algorithms are used for development of viable ML AIDS.

It can be inferred from the survey of available literature that a better system is needed to detect DDoS attacks more extensively. Hybrid IDS has not been developed

for web applications particularly. Identifying unknown variants of known attacks is an area that has not been explored much. The proposed HWIDS takes into consideration these shortcomings and aims to overcome them. The use of a combination of machine learning algorithms (both supervised and unsupervised) in an ensemble model combines advantages of the individual ML algorithms, while detecting the DDoS attacks.

3 System Architecture

This section describes the architecture of the system and a brief description of each module in the system. Figure 1 shows the system architecture for implementing the intrusion detection system. It consists of four tiers—data tier, middleware tier, application programming interface (API) tier and presentation tier.

The data tier consists of a relational database for storing login details of users, details of security incidents and unknown attack samples (once unknown attack has been detected). It also has the datasets (CSV files) and trained ML models for the anomaly detection module and the signature detection module.

The middleware tier has an authentication service and representational state transfer (REST) services for attack classification, generation of alerts, attack details and fetching report. It also consists of schedulers. The schedulers are used to schedule tasks that execute at a certain time or periodically at a fixed interval. The packet capture scheduler captures HTTP packets periodically. The retraining scheduler

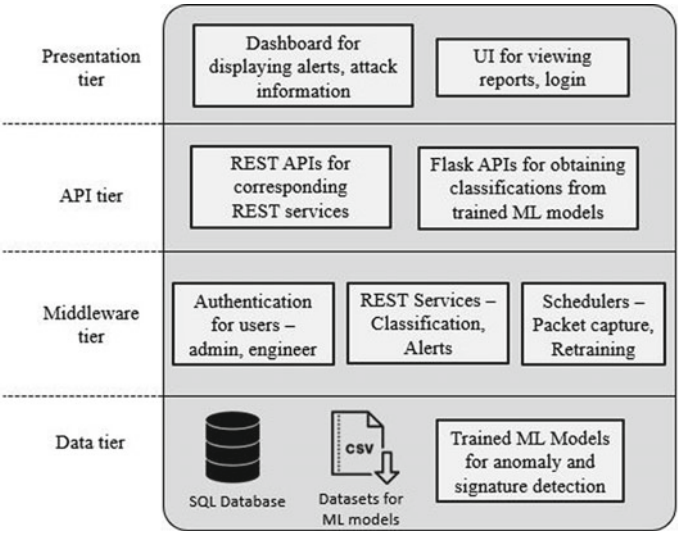


Fig. 1 System Architecture of the HWIDS

retrains the ML models after periodic intervals of time (say, per week) to update the system with information of unknown attacks that have now been detected.

The API tier consists of REST APIs (one for each REST service) and Flask APIs to access the trained models for anomaly and signature detection.

The presentation tier consists of the dashboard and the user interface of the system.

For ease of implementation, the system is divided into five modules. The first module is the network traffic capture module. It is responsible for capturing samples of network traffic, processing them and making it ready to feed to the classification model. Random samples of simulated network traffic are captured. The statistical variables which are present in the dataset are calculated from the packet information (such as mean, median, variance of source port, destination port, transmission control protocol (TCP) flags, Internet Protocol (IP) length). This processed sample is now fed to the ML model for classification.

The system implements a hybrid approach to intrusion detection. Anomaly detection and signature detection are done sequentially. The second module is the anomaly detection module. It classifies the traffic as anomalous or benign. For building the anomaly detection model, the dataset is first split into training and testing sets. Multiple binary classification algorithms are implemented on the training sets and validated using the testing set. The best performing algorithm is selected for the classification model.

The third module is the signature detection module which identifies the type of attack being carried out (such as HTTP Flood, HTTP Slow Read). For the signature detection module, an ensemble of classifiers is used to give better accuracy in classification. An ensemble learning model can produce an optimal result by combining the advantages of the base classifiers. A soft voting classifier combines the results of the base classifiers used in the ensemble.

The fourth module consists of the dashboard. It gives a visual representation of the threats detected, types of attacks identified, detection time. It also displays alerts or notifications in case of a detected attack.

The fifth module consists of the database and the middleware. The middleware consists of REST Services, schedulers (packet capture scheduler, model retraining scheduler), authentication services. The database is a relational database for storing login details of users, details of security incidents and unknown attack samples.

4 Implementation

In this section, details regarding implementation of the system are discussed in brief. We developed a prototype of the HWIDS using Python and MySQL for the backend, Spring framework and Java Persistence API (JPA) for the middleware and Hypertext Markup Language (HTML), Cascading Style Sheets (CSS) for the user interface. The dataset used for building the ML models in the anomaly detection and signature detection modules was created by the authors of [17].

It is a customized dataset, created by extracting the normal traffic instances of the ISCXIDS2012 dataset. DDoS simulation software was used to synthesize the attack instances in a controlled environment. The dataset contains instances of User Datagram Protocol (UDP) attacks, TCP attacks, and HTTP attacks. Since the proposed system operates in a web app environment, we have considered only the HTTP attacks instances and the normal traffic instances from the dataset. The dataset contains HTTP attacks like HTTP slow read, HTTP slow body, HTTP slow range, HTTP slow headers and HTTP flood attacks.

For the anomaly detection module, normal traffic instances and attack instances labeled as 'benign' and 'attack' are used. For the signature detection module, the attack instances, with the labels indicating type of attack such as HTTP flood, HTTP slow are used. Both these subsets of the dataset have class imbalance. To correct the imbalance in the datasets, synthetic minority oversampling technique (SMOTE) is used. Normalization and label encoding are the other data preprocessing techniques used to bring data to a common scale and represent categorical values in numerical format, respectively. Recursive feature elimination with cross validation (RFECV) technique is applied to select the optimal number of features which will give the highest accuracy for the ML models. For RFECV, the Decision Tree algorithm is used as the base classifier.

For the anomaly detection module, the Logistic Regression algorithm is used for classification as it gives the highest accuracy from among the explored algorithms (SVM, Random Forest and Logistic Regression).

For the signature detection module, Random Forest, Decision Tree, Gradient Boosting and AdaBoost algorithms are used. Using these four models as base classifiers, an ensemble learning model is created to provide greater accuracy. A soft voting classifier combines the results of the four classifiers using a weighted average technique [18]. According to the accuracy obtained for each of the base classifiers, weights are assigned to each base classifier. The weights are used to calculate a weighted average of the probabilities predicted for each class by each base classifier. The class with the highest weighted average is selected as the output by the ensemble learning model. Figure 2 gives a diagrammatic representation of the ensemble learning model used in the intrusion detection system.

Machine learning for business operations enhances the security with fast and effective monitoring and detection and prevention of cybersecurity breaches. In IDS, employing other techniques than machine learning require more time for detection, giving the proposed method an advantage. The system can monitor and detect DDoS security breaches without any human intervention, better than a security expert.

5 Results and Analysis

To evaluate the performance of the ensemble model, we have used accuracy, precision, recall and false negative rate (FNR) [17] as the evaluation metrics. We first

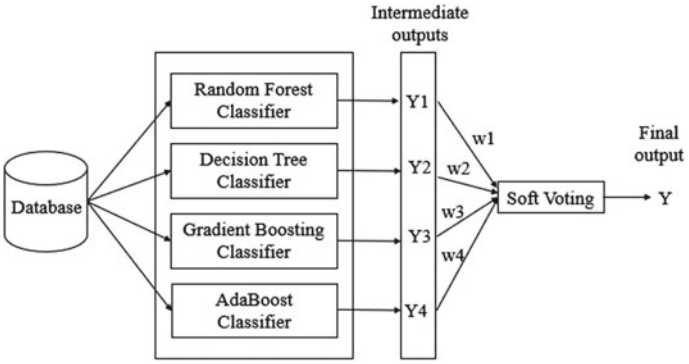


Fig. 2 Ensemble learning model for HWIDS

Table 1 Results for individual classifiers

Algorithm	Accuracy	Precision	Recall	FNR
Random forest (%)	93.08	92.88	93.44	6.55
Decision tree (%)	86.74	86.61	86.48	13.51
Gradient boosting (%)	95.67	95.43	95.52	4.47
AdaBoost (%)	94.81	95.84	94.66	5.33

Table 2 Results for ensemble learning model

Accuracy	Precision	Recall	FNR
95.96%	95.84%	95.89%	4.10%

calculate the values of the metrics for the individual classifiers in the ensemble model. These results are given in Table 1.

Next, we calculate the values of the performance metrics for the ensemble model. These results are given in Table 2. From the comparison of results in Tables 1 and 2, it is clearly seen that the ensemble model outperforms the individual classifiers.

For any intrusion detection system, the ability to detect previously unknown attacks is a crucial advantage. For any ML model, it is very difficult to detect unknown attacks which are vastly different from the attacks that the system has been trained on. However, using machine learning, we should be able to detect unknown variants of the known attacks. In our case, since the HWIDS is developed for web applications, most of the attacks are expected to be variants of HTTP attacks. To test our system for unknown attacks, we trained the ML model using instances of HTTP flood, HTTP slow body, HTTP slow headers and HTTP slow range. We then tested the system on instances of HTTP slow read attack, as it was an unknown attack for the system. The model was able to detect the attack with 93.48% accuracy. The detailed results for testing the system against previously unknown attacks are summarized in Table 3.

Table 3 Results for detection of unknown attacks

Accuracy	Precision	Recall	FNR
93.48%	99.83%	93.47%	6.52%

The constant threat of DDoS attacks is detected using the proposed HWIDS, with superior results, reducing the after-effects and loss. From the statistics, the proposed system outperforms the systems previously mentioned in literature, with respect to accuracy and false positive rate.

6 Conclusion

This paper has presented a hybrid web intrusion detection system (HWIDS) that detects DDoS attacks on web applications. We used multiple binary classification algorithms for anomaly detection. The signature detection module was developed by creating an ensemble of multiple multiclass classification algorithms. The key thought behind our proposed system is to utilize ensemble learning to accumulate the benefits of various algorithms. The proposed method is feasible and efficient. The ensemble learning model gave an accuracy of 95.96% in identifying the attacks.

In the ensuing work in the area of intrusion detection, the main objective is to enhance the training data quality, optimize the process of feature extraction and strengthen the detection of unknown attacks. The accuracy of the ensemble model may be improved in future by using further optimization techniques. The system can also be tested against more HTTP attack variants which are unknown to the system. In future, this system can be extended to develop an intrusion prevention system (IPS) to mitigate the DDoS attacks detected by the HWIDS.

References

1. United Nations, The impact of digital technology, https://www.un.org/en/un75/impact-digital-technologies. Last accessed 2021/05/24
2. S. Pande, A. Khamparia, D. Gupta, Deepak, D. Thanh, DDOS detection using machine learning technique. https://doi.org/10.1007/978-981-15-8469-5_5 (2020)
3. D. Moustis, P. Kotzanikolaou, Evaluating security controls against HTTP based DDoS attacks, in *Fourth International Conference Information, Intelligence, Systems and Applications (IISA)* (2013), pp. 1–6
4. H. Al-Rushdan, M. Shurman, S. H. Alnabelsi, Q. Althebyan, Zero-day attack detection and prevention in software-defined networks, in *2019 International Arab Conference on Information Technology (ACIT)* (2019), pp. 278–282
5. G.A. Jaafar, S.M. Abdullah, S. Ismail, Review of recent detection methods for HTTP DDoS attack. J. Comput. Netw. Commun. **2019** (2019). Article ID 1283472
6. K.M. Prasad, A. Rama Mohan Reddy, K. Venugopal Rao, DoS and DDoS attacks: defense, detection and traceback mechanisms—a survey. Glob. J. Comput. Sci. Technol. (2014)

7. K. Singh, P. Singh, K. Kumar, Application layer HTTP-GET flood DDoS attacks: research landscape and challenges. Comput. Sec. (65), 344–372 (2017)
8. Z. Khan, O. Baig, M.K. Asif, DDoS attacks and countermeasures in cyberspace, in *2015 2nd World Symposium on Web Applications and Networking (WSWAN)* (IEEE, 2015)
9. A. Chonka, W. Zhou, J. Singh, Y. Xiang, Detecting and tracing DDoS attacks by intelligent decision prototype, in *2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom)* (2008), pp. 578–583
10. S. Wankhede, D. Kshirsagar, DoS attack detection using machine learning and neural network, in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)* (2018), pp. 1–5
11. N. Bindra, M. Sood, Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset. Automa. Control Comput. Sci. (53), 419–428 (2019)
12. Z. He, T. Zhang, R.B. Lee, Machine learning based DDoS attack detection from source side in cloud, in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* (2017), pp. 114–120
13. N. Agarwal, S.Z. Hussain, A closer look at intrusion detection system for web applications. Sec. Commun. Netw. **2018** (2018). Article ID 9601357
14. F.L. Bello, K. Ravulakollu, Amrita: analysis and evaluation of hybrid intrusion detection system models, in *2015 International Conference on Computers, Communications, and Systems (ICCCS)* (2015), pp. 93–97
15. Ö. Cepheli, S. Büyükçorak, G. Karabulut Kurt, Hybrid intrusion detection system for DDoS attacks. J. Electr. Comput. Eng. **2016** (2016). Article ID 1075648
16. Z. Kamil, Y. Robiah, N. Bahaman, S. Mostafa, M. Foozy, C. Feresa, Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset. IEEE Access **9** (2021)
17. F.S.de Lima Filho, F.A.F. Silveira, A. de Medeiros Brito Jr, G. Vargas-Solar, L.F. Silveira, Smart detection: an online approach for DoS/DDoS attack detection using machine learning. Sec. Commun. Netw. **2019** (2019). Article ID 1574749
18. X. Gao, C. Shan, C. Hu, Z. Niu, Z. Liu, An adaptive ensemble machine learning model for intrusion detection. IEEE Access **7**, 82512–82521 (2019)

Geospatial Technology and Analytical Hierarchy Process (AHP)-Based Discrimination of Groundwater Potential Zones in Vijayawada–Mangalagiri Region, Andhra Pradesh

Koduganti Sai Sudha Manasa and P. Geetha

Abstract Groundwater is one of the principal sources that contribute to the total annual supply. Understanding the groundwater potential zones is significant for water management and planning for any city. Situated in Andhra Pradesh, the Vijayawada–Mangalagiri region is majorly known for its industrial and agricultural activities. However, the rapid urbanization, inappropriate land use methods, increased anthropogenic activities, and poor irrigation practices led to the depletion of groundwater during the last few years. This research aspires to discriminate the groundwater potential zones using the combination of geospatial technology and analytical hierarchy process (AHP) which augment the source of groundwater. Different thematic layers such as digital elevation model (DEM), drainage density, slope, soil type, land use/land cover (LULC), and rainfall pattern were prepared and analyzed by employing primary and secondary resources. The weighted overlay analysis has been performed on various thematic layers based on their importance using AHP. A groundwater potential map with five zones has been classified as poor, fair, good, very good, and excellent.

Keywords GIS · AHP · Groundwater · Overlay analysis

1 Introduction

Water has a pivotal role to play in the development of a country like India which drives an influential section of the economy is directed by agricultural and industrial activities [1]. The water need in India is immense for the domestic and irrigation sector and needs special attention to stop water scarcity. Harder than ever, access

K. S. S. Manasa (✉)
Center for Wireless Networks and Applications (WNA), Amrita Vishwa Vidyapeetham, Amritapuri, India

P. Geetha
Center for Excellence in Computational Engineering and Networking (CEN), Amrita Vishwa Vidyapeetham, Coimbatore, India
e-mail: p_geetha@cb.amrita.edu

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_78

to safe water is crucial to maintain a healthy life balance for Indian families. More than 30% of the urban population and 90% of the rural population in India depend on groundwater for their drinking and household necessities [11]. The rate of water consumption during the summer season rises every year, and it is crucial to replenish the groundwater [17]. Groundwater being an incredible wealth to us has significance for its fresh quality. Groundwater flows below the land surface between the spaces of rocks, sand, and soil. It moves at different rates according to the geological formations and forms aquifers. Over the years, the extensive demand for groundwater has kept growing and is unlikely to conclude in the future [3]. Groundwater is advantageous over surface water in terms of immense quality, pollution-free, and large-scale spread [16]. Misuse of water has increased rapidly due to the uncertainty of the monsoon, which seriously affects the surface and groundwater resources [19]. Groundwater has been subsequently declining throughout the district with overexploitation, groundwater contamination, industrialization, and exponential population growth. Recent studies show that there is a huge demand for pure water for drinking, agriculture, etc., purposes due to the depletion of groundwater availability in our country [18]. Highly populated cities like Vijayawada–Mangalagiri, Andhra Pradesh, in recent years require finding new groundwater zones to serve the increasing population due to inadequate and unreliable municipal water supplies. To ensure the present-day standing of groundwater potential and sufficient quantity of recharge, potential zones of groundwater are to be identified where unnatural recharge approaches can be accustomed to raise the recharge extent [4]. Groundwater potential zones map assists as effective tools for accurate ground-based hydro-geological surveys which helps in suitable sites for bore wells/dug wells. Geospatial technology-based tools are helpful for the collection, storage, retrieval, and spatial data management for any application. The principal factors considered that affect the potential zone discrimination are drainage density, soil, elevation, slope, LULC, and rainfall. All these factors were assigned a satisfactory weight based on AHP to obtain a groundwater potential zone. These factors determine groundwater occurrence, hydrological properties, and geological formation [5].

2 Study Area

One of the fundamental requirements of human beings is having accessibility to fresh, potable drinking water [22]. Encircled by the hills of Eastern Ghats and canals, the Vijayawada–Mangalagiri region in Andhra Pradesh sprawls on the banks of the Krishna River. Telugu is the predominant language spoken by the residents of the study area [21]. Having a tropical climate, the annual mean temperatures range from 23.4 to 34 °C. The summers have more rainfall when compared with winter, and the annual rainfall ranges from 900 to 1100 mm. The broad range of land use practices in the study area includes settlements, agriculture, barren land, and forests. The major soil types in the region are loam, clay loam, sandy clay loam, and clay. Figure 1 represents the study area map.

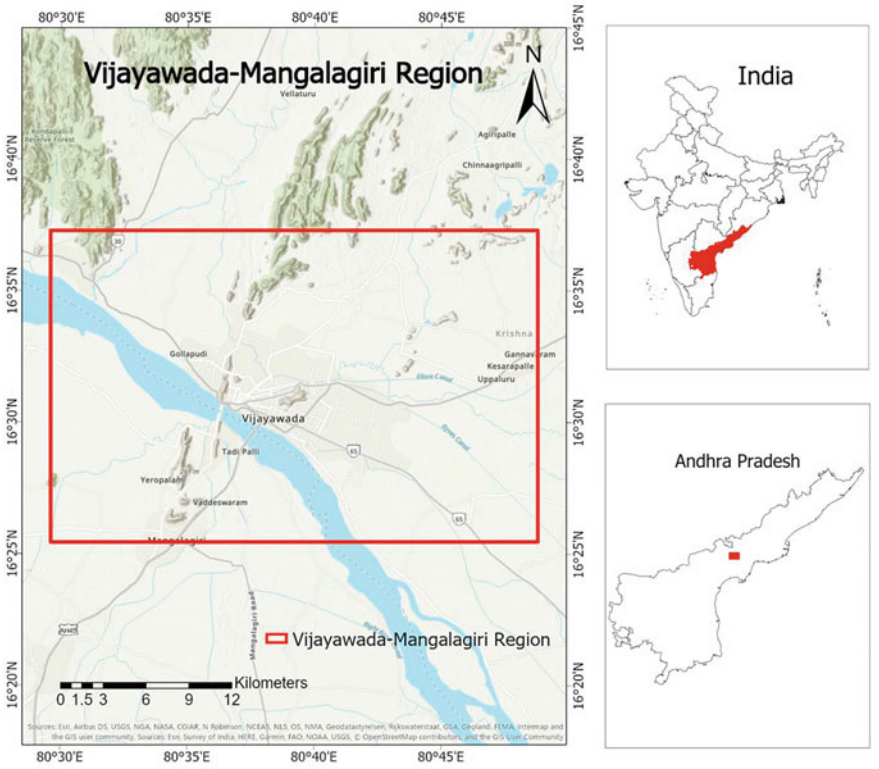


Fig. 1 Study area map

3 Data Requirements and Methodology

The study was pursued by taking into consideration various layers say drainage density, elevation, slope, soil, land use/land cover (LULC), and rainfall. These data sets have been composed of various primary and secondary sources and are redefined in the geospatial environment to create the database. The shapefile layer of India was obtained from Diva GIS, an online repository for GIS data. Digital elevation model (DEM) is extracted from the Aster Global DEM V3 to prepare slope, elevation, and drainage density layers. Cloud-free Sentinel-2 data of 10 m resolution has been chosen for performing random forest classification for land use/land cover extraction using Google Earth Engine. The rainfall data in grid format has been downloaded from Climate Research Unit (CRU).

The methodology involves the collection and preparation of various remotely sensed data layers which were processed using ArcGIS software. Understanding potential zones of groundwater by geospatial technology has numerous benefits, especially defining the features spatially [20]. A geo-database has been created for

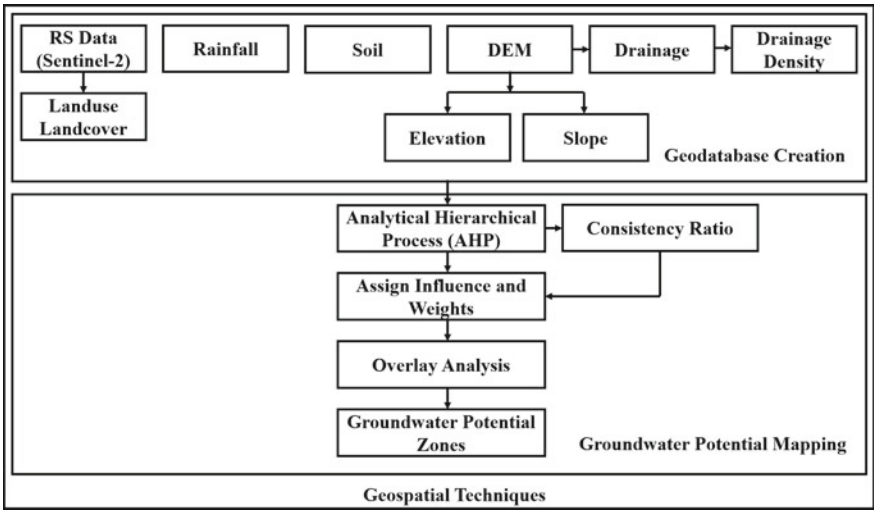


Fig. 2 Methodological flowchart

all the layers and georeferenced to the UTM zone 44N. Supervised classification has been performed for classifying different features in the study area using Sentinel-2 data. An automatic drainage map has been generated from the DEM. All the layers were assigned ranks and weights based on the multicriteria decision-making technique [6]. While calculating the weights, the number of layers was given as 6, and the pairwise comparisons were made to calculate the priorities based on the analytical hierarchy process. Table 2 shows the importance of values [7]. It helps to identify and repair logical inconsistencies. The pairwise comparison results are presented in a matrix form, and the first normalized right eigenvector of the matrix yields the weighting. The eigenvalue determines the consistency ratio [8]. The obtained matrix is said to be consistent if the consistency ratio is below 0.1. After assigning the determined weights, the layers were subjected to weighted overlay analysis. The scale preference for each class is decided by how important the layer and its class with the attribute are. Figure 2 represents the methodology flowchart followed in this research.

4 Analysis of Results

The potential zones of groundwater having a direct or indirect impact are based on the six parametric layers investigated for the study. Based on the overlay analysis, the effect of one layer on to the other layer was determined by assigning suitable weights [13] (Table 1).

Table 1 Satty's relative importance scale

Value	Indication	Description
1	Similar importance	Contribution of two parameters is same
3	Average importance	One parameter is chosen slightly over the other
5	Strong importance	Strongly supports only one parameter
7	Very strong importance	One parameter dominates the other
9	Extreme importance	Highest degree of dominance of one parameter over the other
2,4,6,8	In-between values	When settlement is essential

4.1 Drainage Density and Soil Map

Drainage density plays a vital role in understanding groundwater contamination and accessibility. The drainage density influences the rate of infiltration and runoff. The digital elevation model (DEM) collected from Aster Global DEM V3 with the 30-m spatial resolution has been employed to acquire the study area drainage density map. The drainage density was achieved by computing the flow direction and flow accumulation of the region and thereby clustered into five classes. From the drainage density map, it was observed that the elevated drainage density is due to less infiltration and does not endorse the potential zones of groundwater, and the depressed drainage density is due to high infiltration and indicates groundwater potential zone. Figure 3 represents the study area drainage density map. Soil types play a crucial role in the water quantity that can infiltrate into the subsurface and thereby affect the recharge of groundwater [9]. The main constituents regarded for the estimation of infiltration rate are hydraulic properties and texture of the soil [8]. The water quantity approaching the water table relates to the scope of the aloof lying underneath the soil. Figure 4 represents the soil map of the study area. The Vijayawada–Mangalagiri region includes different soil types such as loam, clay loam, sandy clay loam, and clay.

4.2 Elevation and Slope Map

The elevation and slope maps of the study area were derived from Aster Global DEM V3 with a 30-m spatial resolution. The elevation signifies the undulations of the ground surface available for sink storage. The study area elevation ranges from 8 to 326 m of mean sea level. Figure 5 represents the study area elevation map. The slope is a vital terrain feature that signifies the ground surface steepness [10]. The slope of the region affects the rate of infiltration and surface runoff. A steeper slope indicates higher runoff [11]. During rainfall, large slopes offer less recharge as the water flows swiftly down a steep slope. The study area slope ranges from 0 to 57.11

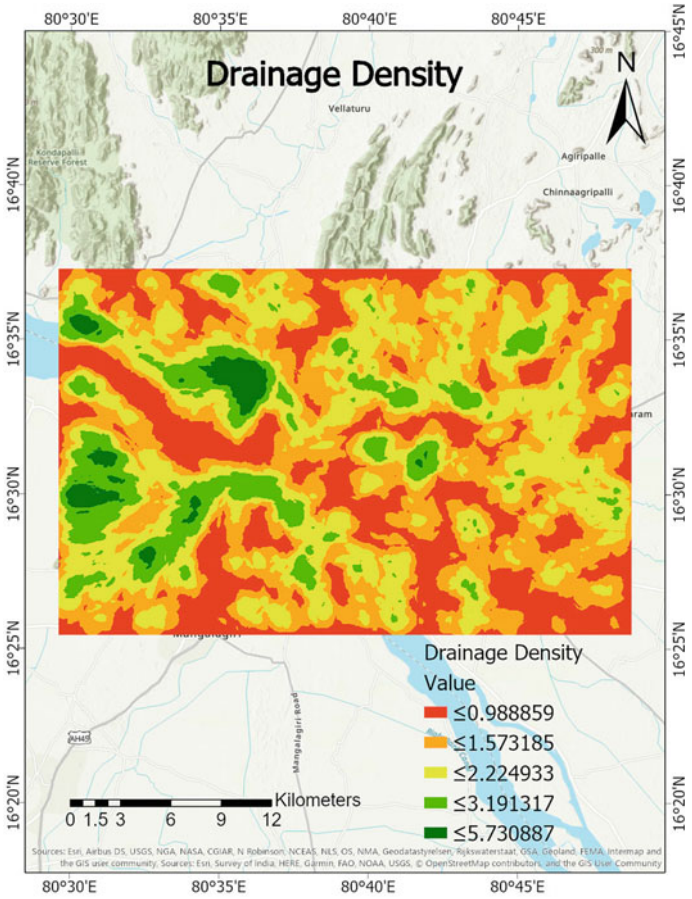


Fig. 3 Drainage density map

degrees, classified and represented in five classes based on the slope value. Figure 6 represents the slope map of the study area.

4.3 Rainfall and Land Use/Land Cover Map

Rainfall is the principal and dominant factor of groundwater recharge. The rate of infiltration depends on the amount and period of rainfall [12]. The rainfall data of 2020 has been used for the current study. The annual rainfall ranges from 948 to 1075 mm. The rainfall spatial distribution map was developed using the Kriging interpolation technique. The rainfall data set has been reclassified into five categories based on the maximum and minimum values ranging from very low (948–980

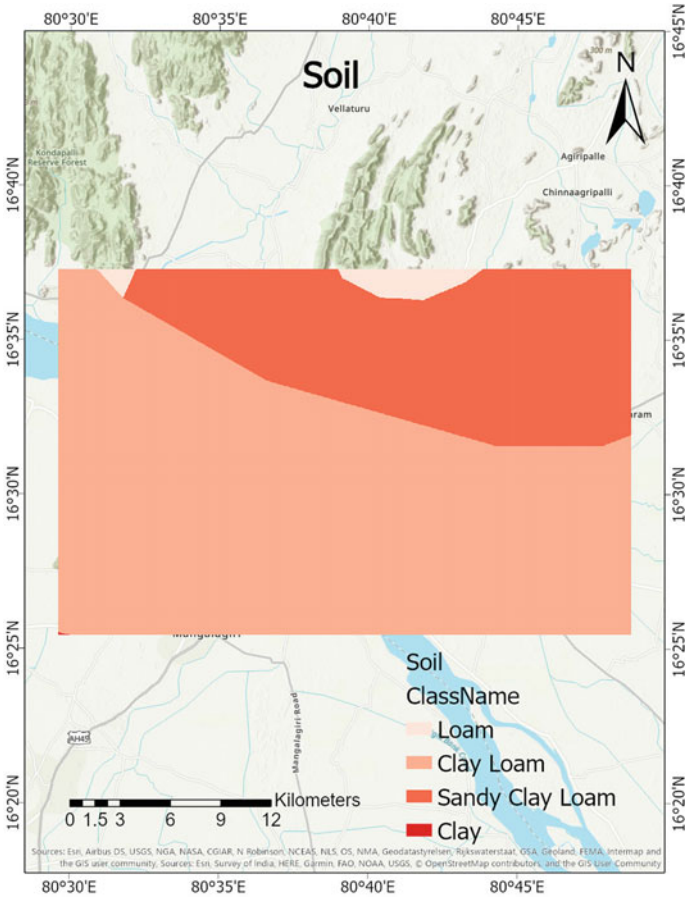


Fig. 4 Soil map

mm), low (980–1000 mm), moderate (1000–1019 mm), high (1019–1041 mm), and very high (1041–1075 mm). Short span and high amounts of rainfall indicate more surface runoff and less infiltration. Higher weights are assigned for high rainfall, and lower weights are assigned for low rainfall. Figure 7 represents the study area interpolated rainfall map. The land use/land cover provides the necessary information regarding groundwater demands along with surface water, infiltration, soil moisture, etc. [14]. The study area has been classified into five major classes which include water, agriculture, settlements, barren land, and scrub forest. The land use/land cover types in the study area are delineated from Sentinel-2 satellite data with a 10-m resolution. The highland area is comprised primarily of scrub forests. The midlands and lowlands are dominated significantly by agricultural land and settlements. The agricultural land and scrub forest carry extensive water proportions of water than the settlements and barren land. So, the weights were assigned based on the available

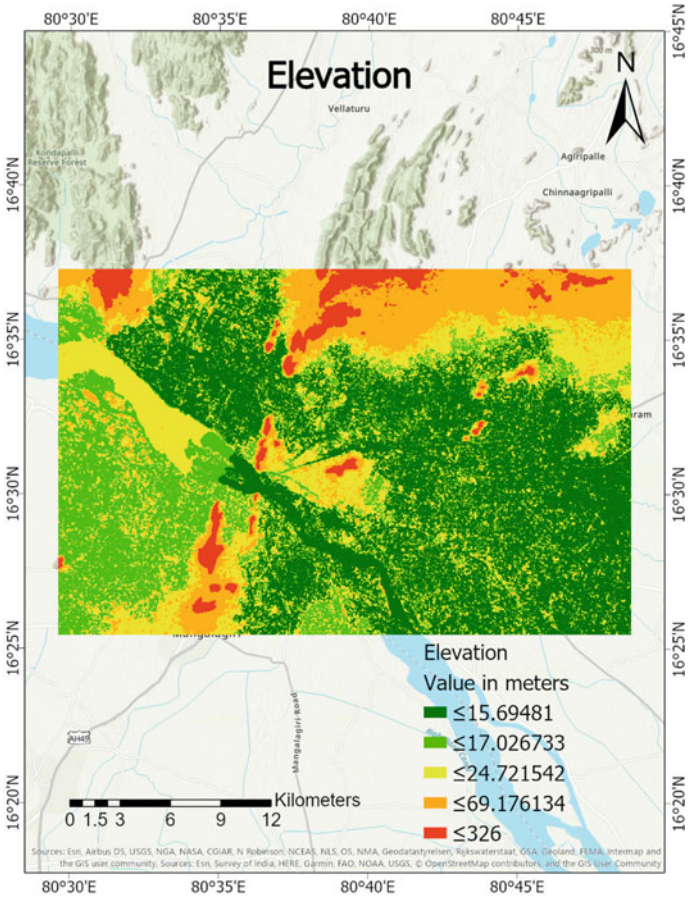


Fig. 5 Elevation map

water quantity for recharge concerning the topography. The high weight is assigned to the water and agriculture, and the low weight is assigned for the settlements, barren land, and scrub forest. Figure 8 represents the study area land use/land cover map.

4.4 Analysis of Groundwater Potential Zones

The six data sets were generated in the geospatial environment, and the suitable weights have been determined by the analytical hierarchy process (AHP) technique. The weights were later attributed based on the weighted overlay analysis, one of the powerful decision-making tools that solve multicriteria issues [15]. The weights for each thematic layer were selected based on Saaty's scale (1–9) of relevant importance.

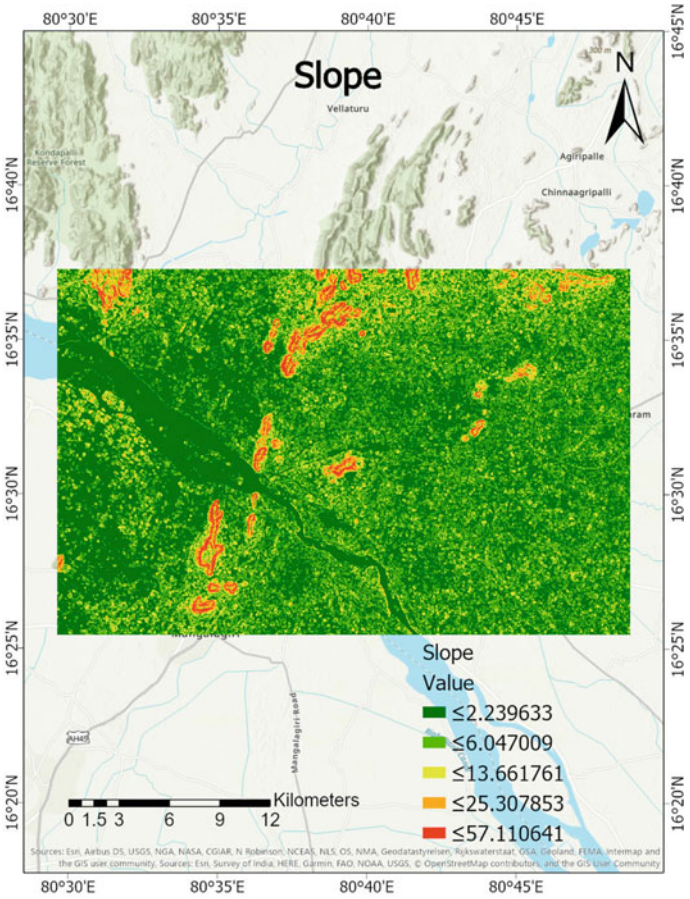


Fig. 6 Slope map

Table 2 AHP-based decision matrix

Class	DD	Rainfall	Slope	Elevation	Soil	LULC
DD	1	1	5	5	5	5
Rainfall	1	1	5	5	5	5
Slope	0.20	0.20	1	1	1	1
Elevation	0.20	0.20	1	1	1	1
Soil	0.20	0.20	1	1	1	1
LULC	0.20	0.20	1	1	1	1

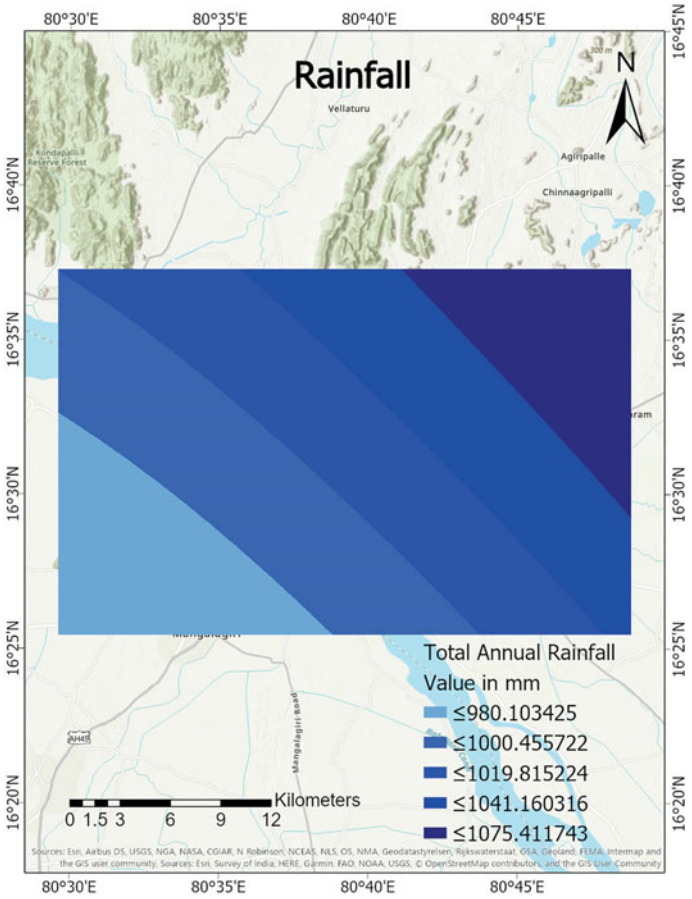


Fig. 7 Rainfall map

AHP scale ranges from 1—similar importance, 3—average importance, 5—strong importance, 7—very strong importance to 9— extreme importance (2,4,6,8 values are in-between values). The raster values are reclassified to a common agreement scale based on the importance of the layers by inputting the values in integer format. All the six thematic layers were correlated concerning each other in a pairwise comparison matrix form [8]. The high weight represents a thematic layer with a high influence, and the low weight represents a thematic layer with a little influence on groundwater potential. The result achieved was categorized into five classes ranging from very poor potential zone to very good potential zone as shown in Fig. 9. Most of the study area has a smooth terrain which confers the possibility of groundwater recharge. Initially, the principal eigenvalue (λ) was computed by the eigenvector method, and consistency index (CI) was determined from following Eq. 1, where RI = random consistency index value, n = number of parameters used in the study = 6

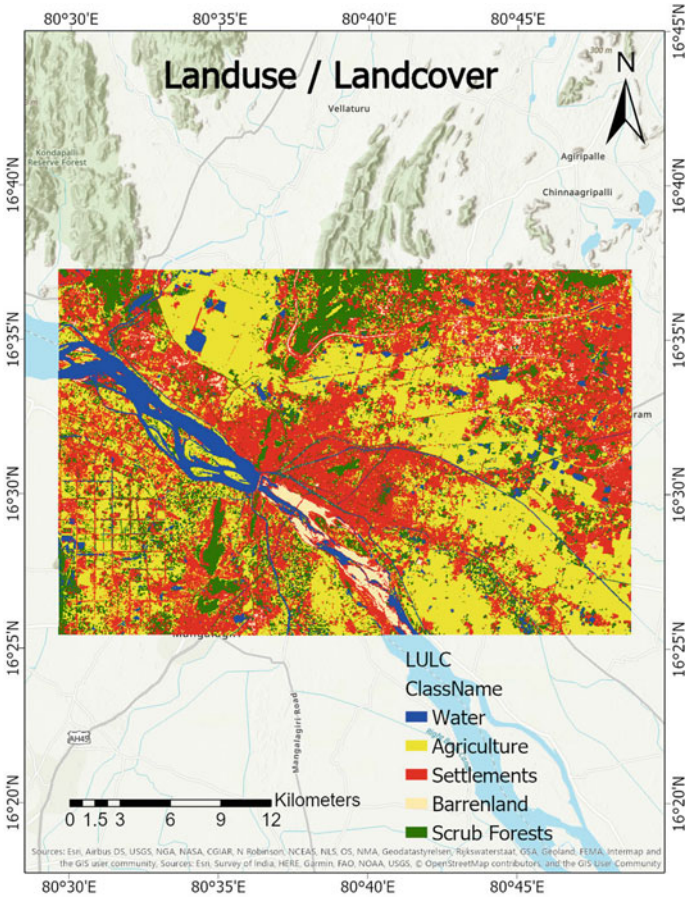


Fig. 8 Land use/land cover map

$$\mathrm{CR} = \mathrm{CI}/\mathrm{RI} \tag{1}$$

$$\mathrm{CI} = (\lambda \max - n)/(n - 1) \tag{2}$$

The consistency ratio acquired is 0% which indicates the perfect consistency level in pairwise comparison [7]. To generate the potential zones of groundwater in the Vijayawada–Mangalagiri region, all the six thematic layers were used based on Eq. 3:

$$\mathrm{GPZM} = Dd_{\mathrm{w}}Dd_{\mathrm{r}} + R_{\mathrm{w}}R_{\mathrm{r}} + S_{\mathrm{w}}S_{\mathrm{r}} + E_{\mathrm{w}}E_{\mathrm{r}} + So_{\mathrm{w}}So_{\mathrm{r}} + Ll_{\mathrm{w}}Ll_{\mathrm{r}} \tag{3}$$

where GPZM is groundwater potential zone map, Dd is drainage density, R is rainfall, S is slope, E is elevation, So is soil, Ll is land use/land cover, r is rank assigned, and w is weight.

Table 3 Groundwater Potential Zone Priorities

Category	Assigned weight	% Priority	Domain	Rank
DD	1	36	0-0.98	1
			0.98-1.57	2
			1.57-2.22	3
			2.22-3.19	4
			3.19-5.73	5
Rainfall	1	36	948–980 mm	1
			980–1000 mm	2
			1000–1019 mm	3
			1019–1041 mm	4
			1041–1075 mm	5
Slope	3	7	0–2.23	5
			2.23-6.04	4
			6.04–13.66	3
			13.66-25.30	2
			25.30–57.11	1
Elevation	3	7	8–24	5
			24–51	4
			51–101	3
			101–174	2
			174–326	1
Soil	3	7	Loam	1
			Clay loam	2
			Sandy clay loam	3
			Clay	4
LULC	3	7	Water	5
			Agriculture	4
			Settlements	3
			Barren land	1
			Scrub Forest	2

4.5 Decision Matrix

The groundwater potential zone discrimination using AHP involves assigning of principal eigen vector of the decision matrix which is shown in table 2. In tables 2 and 3, DD is drainage density and LULC is land use/land cover (Table 4).

Table 4 Area covered by groundwater potential zones

Class	Area (km)
Poor	5.5584
Fair	193.796
Good	389.406
Very Good	144.204
Excellent	0.0099

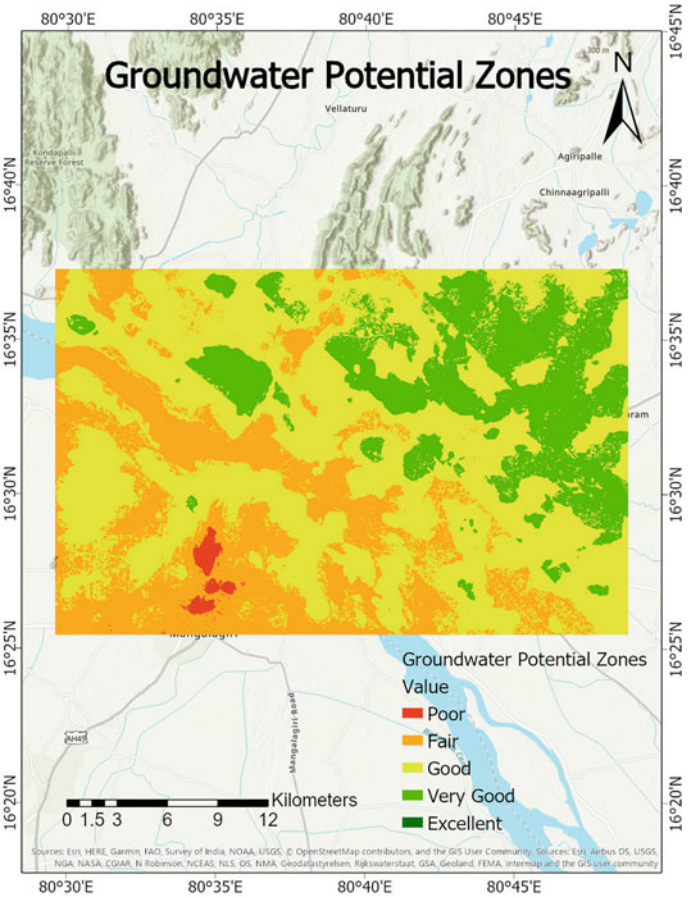


Fig. 9 Groundwater potential zones map

5 Conclusion

The geospatial technology involving remote sensing and GIS helps in deriving spatial and visual results more prominently. The present study discriminates the potential zones of groundwater using geospatial technology and analytical hierarchy process (AHP) in the Vijayawada–Mangalagiri region of Andhra Pradesh. A total of six thematic layers such as digital elevation model (DEM), drainage density, soil type, slope, land use/land cover (LULC), and rainfall pattern were used in this study, and appropriate weights are assigned to all the layers. The output map shows five categories of groundwater potential zones as poor, fair, good, very good, and excellent. The very good and excellent zones are situated in and around the Vijayawada city, and the poor zone is situated in and around Mangalagiri. This shows that special attention in the Mangalagiri region needs to be given to recharge the groundwater. Poor and excellent groundwater potential zones cover less than 1% of the total area. Fair groundwater potential zone covers an area of 26.44%, good groundwater potential zone covers an area of 53.12%, and very good groundwater potential zone covers an area of 19.67%. The potential zones map of groundwater in the current research contributes insights into decision-makers for groundwater management and planning agricultural and industrial activities.

References

1. R.K. Jaiswal, S. Mukherjee, J. Krishnamurthy, R. Saxena, Role of remote sensing and GIS techniques for generation of groundwater prospect zones towards rural development-an approach. Int. J. Remote Sens. **24**(5), 993–1008 (2003)
2. C.R. Fitts. *Groundwater science* (Elsevier, 2002)
3. S. Shahid, S.K. Nath, J. Roy, Groundwater potential modelling in a soft rock area using a GIS. Int. J. Remote Sens. **21**(9), 1919–1924 (2000)
4. M. Nagarajan, S. Singh, Assessment of groundwater potential zones using GIS technique. J. Indian Soc. Remote Sens. **37**(1), 69–77 (2009)
5. M. Mokarram, G. Roshan, S. Negahban, Landform classification using topography position index (case study: salt dome of Korsia-Darab plain, Iran). Model. Earth Syst. Environ. **1**(4), 1–7 (2015)
6. T.L. Saaty, *Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World* (RWS Publications, 1990)
7. L.T. Saaty, Decision making with the analytic hierarchy process. Int. J. Serv. Sci. **1**(1), 83–98 (2008)
8. L.K. Singh, M.K. Jha, V.M. Chowdary, Assessing the accuracy of GIS-based multi-criteria decision analysis approaches for mapping groundwater potential. Ecol. Indicat. **91**, 24–37 (2018)
9. S. Das, Delineation of groundwater potential zone in hard rock terrain in Gangajalghati block, Bankura district, India using remote sensing and GIS techniques. Model. Earth Syst. Environ. **3**(4), 1589–1599 (2017)
10. S.J. Riley, S.D. DeGloria, R. Elliot, Index that quantifies topographic heterogeneity. Intermountain J. Sci. **5**(1–4), 23–27 (1999)
11. S. Prafull, J.K. Thakur, S. Kumar, Delineating groundwater potential zones in a hard-rock terrain using geospatial tool. Hydrol. Sci. J. **58**(1), 213–223 (2013)

12. K. Ibrahim-Bathis, S.A. Ahmed, Geospatial technology for delineating groundwater potential zones in Doddahalla watershed of Chitradurga district, India. The Egypt. J. Remote Sens. Space Sci. **19**(2), 223–234 (2016)
13. X. Li, W. Wang, F. Li, X. Deng, GIS based map overlay method for comprehensive assessment of road environmental impact. Trans. Res. Part D Transp. Environ. **4**(3), 147–158 (1999)
14. P. Kumar, S. Herath, R. Avtar, K. Takeuchi, Mapping of groundwater potential zones in Killinochi area, Sri Lanka, using GIS and remote sensing techniques. Sustain. Water Resour. Manage. **2**(4), 419–430 (2016)
15. R. Yousef, H.R. Pourghasemi, N.S. Neisani, O. Rahmati, Application of analytical hierarchy process, frequency ratio, and certainty factor models for groundwater potential mapping using GIS. Earth Sci. Inf. **8**(4), 867–883 (2015)
16. M. Kaviarasan, P. Geetha, K.P. Soman. GIS-based ground water quality monitoring in Thiruvannamalai District, Tamil Nadu, India, in Proceedings of the International Conference on Soft Computing Systems (Springer, New Delhi, 2016), pp. 685–700
17. G.P. Kumar, P. Geetha, G.A. Shanmugasundaram, *Real Time Water Utility Model Using GIS: A Case Study in Coimbatore District, in Intelligent Systems Technologies and Applications* (Springer, Cham, 2016), pp. 115–123
18. M. Kaviarasan, P. Geetha, K.P. Soman, Multivariate statistical technique for the assessment of ground water quality in Coonoor Taluk, Nilgiri District, Tamilnadu. India. Ind. J. Sci. Technol. **8**, 36 (2015)
19. V. Aiswarya, A.S. Mahesh, Quality assessment of ground water in pre and post-monsoon using various classification technique. Int. J. Recent Technol. Eng. (IJRTE) **8**(2), 5996–6003 (2019)
20. P. Geena, S.E. John. Delineation of ground water potential zones using GIS and remote sensing–a case study from midland region of Vamanapuram river basin, Kerala, India, in *AIP Conference Proceedings*, vol. 1952, no. 1 (AIP Publishing LLC, 2018), p. 020028
21. Geography of Vijayawada. www.mapsofindia.com
22. G.E. Takem, D. Chandrasekharam, S.N. Ayonghe, P. Thambidurai, Pollution characteristics of alluvial groundwater from springs and bore wells in semi-urban informal settlements of Douala, Cameroon. Western Africa. Environ. Earth Sci. **61**(2), 287–298 (2010)

IoT Application for Spruce Fire Detection in Rwanda

Eric Hitimana, Gaurav Bajpai, Richard Musabe, Louis Sibomana, and Jayavel Kayalvizhi

Abstract In Rwanda installing, fire extinguishers are mandatory in all buildings. The number of staff trained in its efficient usage is still insufficient. Many are not aware of the fire extinguisher handling. Although alerting a fire outbreak detection on a real-time basis is still a big challenge. Furthermore, as people delay informing fire brigades, the administrative procedures also delay resulting in several people having fire injuries with valuable asset damage. Developing a system that detects fire smartly, records the building's occupants sending alert information to the fire brigade with other stakeholders on a real-time basis is the motivation of this paper. This paper presents a system based on the Internet of Things (IoT) that detects spruce fire in a building. The IoT system consists of various sensors that measure important factors like recording the number of occupants in the buildings through an Infrared proximity sensor. The smoke sensor sends the notification updates to the fire brigade's dashboard providing an alert in case of fire. The actuators are initialized for a quick exit from the spruce fire. The developed system helps to evacuate buildings' occupants against fire outbreaks on real-time information. This reduces the number of casualties, decreasing the extent of property damage to save resources during the fire outbreaks.

Keywords Spruce fire detection · IoT · IR · MQTT · Smoke sensors

E. Hitimana (✉)
African Center of Excellence in the Internet of Things, University of Rwanda, Huye, Rwanda
e-mail: e.hitimana@ur.ac.rw

G. Bajpai (✉) · R. Musabe
Department of Computer and Software Engineering, University of Rwanda, Huye, Rwanda
e-mail: gaurav.bajpai.2014@ieee.org

L. Sibomana
National Council for Science and Technology, Rwanda Government, Kigali, Rwanda
e-mail: lsibomana@ncst.gov.rw

J. Kayalvizhi
Department of Information Technology, SRM Institute of Science and Technology, Chennai, India
e-mail: kayalvij@srmist.edu.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_79

1 Introduction and Background

Rwanda is a fast-growing economy with increasing infrastructure development. Its cities are gradually expanding with city dwellers [1]. This leads to an increase in fire risks as more buildings are constructed. There are a growing number of people with inadequate knowledge of fire safety measures, regulations, and laws. This results in high exposure to fire hazards leading to increased vulnerability. The firefighting equipment installed in the building could handle small fire incidences. Most buildings are unequipped with upgraded fire safety equipment. Sensitization of the population on fire safety-related matters is irregular. Building codes for geographical identification based on fire safety regulations are not fully reinforced.

Real-time information is critical to fire emergency response for recovery measures. The collation, assessment, verification, and dissemination of information require an appropriate information management system. This system's decision-making provides external information that allows members of the public to make informed decisions to ensure their safety. Fire outbreaks have increased in recent times with 326 fires registered across the country from 2010 up to 2019. Investigation on causes of the fire outbreaks found [2] that 61, 22, 9, 4, 3, and 1% were due to short circuits causes, arson, road incidents, hazardous domestic activities, and chemical explosion. Fire outbreaks cause loss of life with property damage. Early detection of fire sources with effective countermeasures is an issue in fire prevention [3]. Efforts to develop fire management systems worldwide by applying information communication technology (ICT), are being conducted in practice. The utilization of ICT includes cloud computing with the IoT. The main characteristics of the smart city are integrating scalability, interoperability, limited power consumption, multi-modal access, and robustness [4].

The main objective of this research is to develop a highly efficient system that detects a fire and records the building occupants by notifying the stakeholders in real-time. This also provides users privacy by detecting them using an Infrared proximity sensor. The remaining part of this paper has related works in Sect. 2, proposed methods in Sect. 3, research design in Sect. 4, results and discussions in Sect. 5 concluding with Sect. 6.

2 Related Works

The building monitoring system using Raspberry pi, radio-frequency identification (RFID) technology, temperature sensor, and video monitoring compromises privacy [5]. It is capable of motion and disturbance detection at entry points along with a security alarm system having alerts containing pictures also has privacy concerns. However, this system avoids static individuals as people sleeping or in places that have no cameras such as toilets. It has been observed that cameras do not provide privacy [6]. A non-intrusive approach for indoor occupancy detection enhances smart

environments by focusing on the detection, localization, and identification of people. Many techniques to detect human presence by using wearable devices and cameras also suffer from intrusiveness issues.

The development of an algorithm for the detection of carbon dioxide (CO_2)-based occupancy was implemented. It detects CO_2 concentration monitored in buildings to assess the indoor air quality. It has a drawback of detecting the concentration of CO_2 or other gases in places as cooking areas. The use of different methods for inferring occupancies such as data streaming and video streaming [7] to handle ingesting along with analyzing with the IoT sensors. Different platforms such as Intel Edison, Raspberry Pi, Arduino with sensors parameters including vibration, light, CO_2, temperature, humidity, with live video streams also has issues of privacy. The reasons can be to improve space utilization, locate people during an emergency, or understand flows within buildings over time [8].

Personal detection techniques and emergency evacuation assistance were developed [9] to minimize the loss of mishaps. However, some corporations also trained employees to be emergency response coordinators (ERCs) recording manual entries of occupants. Nowadays, emergency evacuation is linked to an electronic attendance providing baseline number of actually in the building. Also scanned ID of a person to detect movement. This assumes that moving machinery is not interfacing too. The system has the drawback to detect static people or visitors. Counting all people in the whole building or people based on some predefined zones [10] is to know total occupants. The zones are defined using heating ventilation, and air conditioning (HVAC) zones, offices, or Wireless Fidelity (Wi-Fi) access point coverage areas. The granularity of the zones differs case by case.

The IoT connection control has four common methods: internet control (Wi-Fi), area network control (WebSocket), Bluetooth, and serial port. It has nodes connected with multi-hop to transmit and reinforce continuous monitoring in real-time [11]. Mainly fire alarm systems use wireless sensor networks (WSN) [12]. The key characteristics of an IoT setup include the following: (1) instrumentation, (2) interconnectivity, (3) intelligence, and (4) facilitation of smart services through instrumentation and networking technologies. The IoT enables various devices that are attached with microsensor chips. Earlier, fire detection used visual analysis through video and image processing techniques to detect fires [13]. Nowadays, advances in sensor microelectronics are used in fire detection technology monitoring [14].

Traditionally, single-point heat along with smoke detectors was widely used for limited areas. In large rooms with high-rise buildings, smoke particles and heat takes a longer detection time. Detection of fires preferably uses video-based fire [15]. They can also perform high-rise building fire monitoring along with outdoor fire detection [16]. These detections use visual characteristics of fire, including color, texture, geometry, flicker, with motion [17]. Since smoke is translucent, the edges of the high-frequency image frame lose clarity as an indicator of smoke. The distinction between different types of smoke is through the examination of changes in background tones, smoke pixels, blurred backgrounds, with illumination segmentation. Establishing a sensor-based safe cooking kitchen environment requires in-depth risk analysis. Kitchen disaster risk consists of three factors: fire, burn, and intoxication.

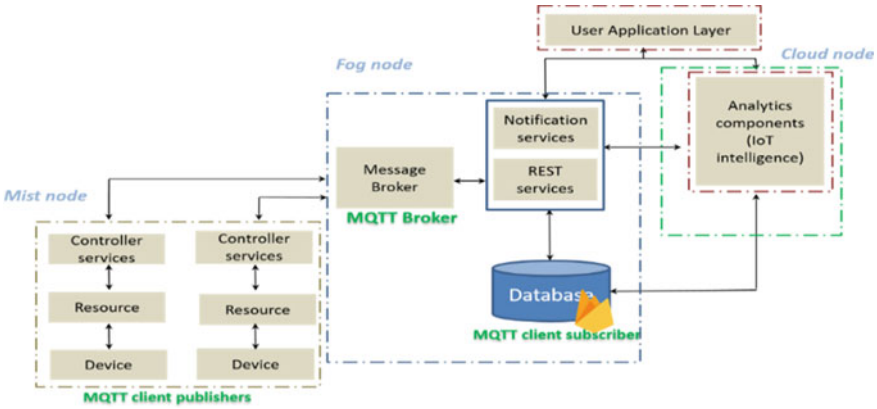


Fig. 1 The architecture of the system overall diagram

The sensor-based fire detection technology is highly accurate. It is easy to install the hardware and deploy the software. Integrating sensor and vision-based visual fire detection algorithms for fire color modeling with motion detection sensor seem to be an appropriate combination. Although it increases system overhead increasing complexity.

3 Proposed Methodology

In the system, the proximity sensor will detect building occupants. This is recorded in the dashboard sending messages through a short message service (SMS). Also, a buzzer and light-emitting device (LED) shall be activated for exiting the building. In case of smoke in a building heave smoke sensors that will provide a warning light alert (Fig. 1).

The proposed system will enhance the accuracy of detecting building occupants by using an IR proximity sensor. It will ensure the privacy of people by knowing the location of each person in the building without using the camera. Consequently, the system provides an alert to deliver real-time information to the fire brigade. This reduces the number of casualties during a fire outbreak.

4 Research Design

IoT-based applications use sensors for sensing the environment. NodeMCU Amica is an ESP8266 Wi-Fi Module-based development board. Proximity level is reported as the distance from the sensor to the closest visible surface. A smoke sensor can detect smoke by alerting through a sound alarm while LED gives an alert to the building

occupancy. A piezo buzzer is a tiny speaker connected directly to an Arduino. LED is a semiconductor that illuminates when charged.

The use case identifies the users that are called actors for implementation. Figure 2a describes the actors of the proposed model. The system is implemented to notify concerned users. Sound alerts to notify the occupant of the threat to evacuate. Also, the LED will be blinking to direct the evacuation path to be followed during an event. Light indicators with sound alarm notifications are for occupants in range of the threat. However, the remote administration units will get SMS notifications for action to be foreseen. The information assimilated through data sent on the dashboard generates analytics that is visualized promptly through dashboard management. Furthermore, the fire brigade will log in for rescue during an event. The activity diagram in Fig. 2b shows the data workflows with activities followed by actions made according to the choices taken.

The sequence diagram of the proposed system describes sequenced interactions as shown in Fig. 3 among classes in terms of the exchange of tasks over time. This sequence diagram contains seven (7) objects having different names.

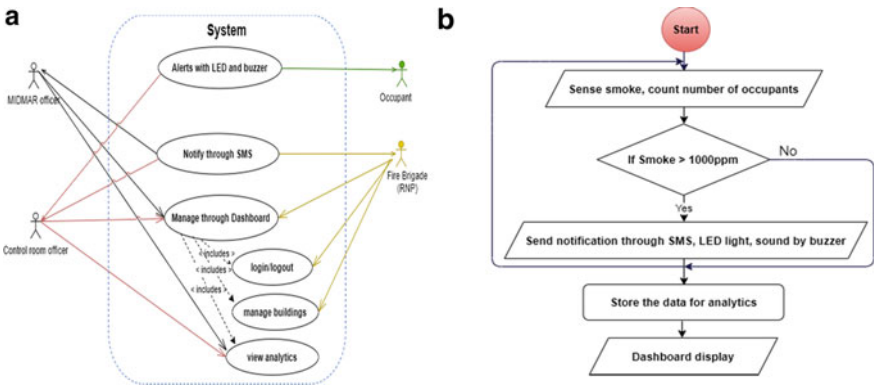


Fig. 2 **a** Use case. **b** Activity diagram

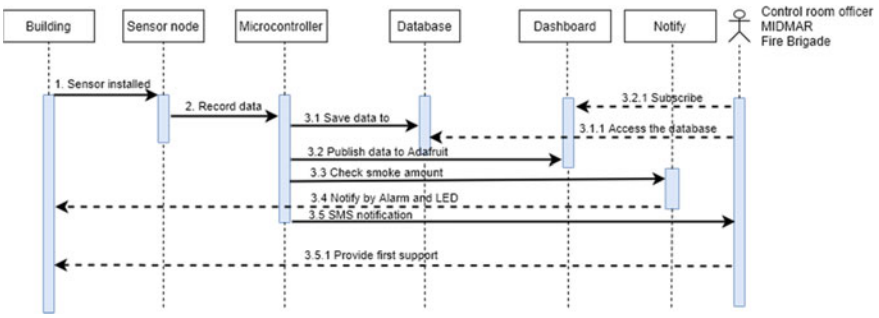


Fig. 3 Sequence diagram of the proposed system

5 Results and Discussion

This research used IoT techniques to develop smart fire detection. Creating the system architecture integrating the microcontroller, sensor elements, and actuators, to send notifications through SMS to concerned stakeholders. Further, the data is stored in Firebase DB as shown in Fig. 8 later to display events on the dashboard for rescue and evacuation of occupants in the building. This leads to data visualization through the Adafruit IO platform. The proposed model follows in Fig. 4.

The system implementation contains six parts described in the IoT framework structure shown in Fig. 4. It has an application layer, management layer, services, communication, security, and the device layer (Fig. 6).

The information systems collect data, store, and distribute them. Here, the client occupancy is detected with two sensors, proximity sensors, and smoke sensors in every room in the building. This assists to calculate the exact number of people on-site. The smoke sensor detects the presence of CO_2 concentration if greater than 1000 ppm. The Global System for Mobile Communications (GSM) module is used to alert the user by sending an SMS. In this research, the notification is sent from the microcontroller directly to administrators for the ERCs. The users access that real-time information by subscribing to the MQTT broker. MQTT allows them to subscribe to the system. MQTT is a lightweight publish/subscribe protocol. It allows administrators to publish and receive the message as the client after subscription.

In this research, the input from sensors is kept in a firebase like the number of people in a building from the proximity sensor including the amount of smoke from the smoke sensor. Consequently, in case of a fire outbreak, the fire brigade will receive records of real-time information for occupants trapped. This database always records the comment and the content of the comment that is received from the microcontroller as shown in Fig. 5. The system administration module contains a dashboard to display data. This provides real-time information that is recorded in firebase. Administrators feed information statistics to ERCs. The research proposes to include a control room manager for each building. The fire brigade unit's focus is to quickly rescue victims depicted on the dashboard. It also archives the record for

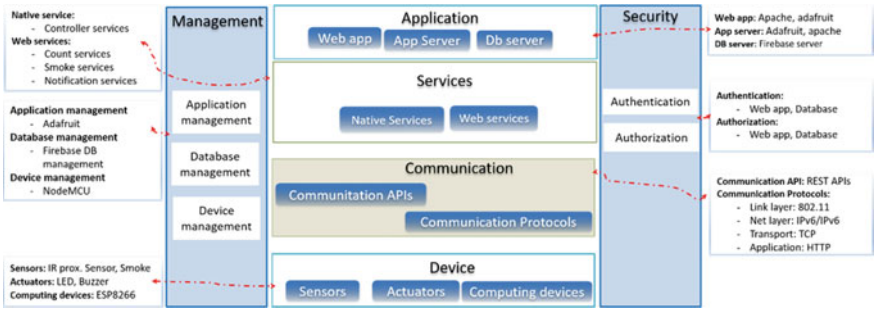


Fig. 4 Process diagram of the proposed model

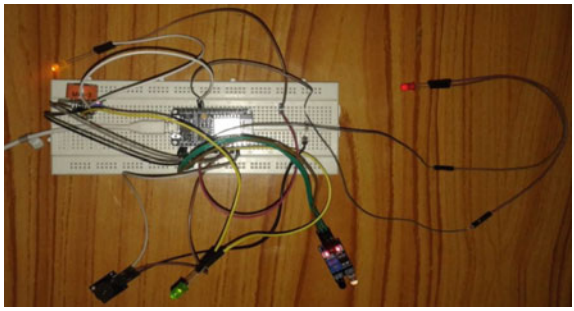


Fig. 5 A system setup

predictive analysis. Adafruit IO platform is a cloud service used to manage traffic information in real-time. The administrators view real-time data online by using any PDA (Personal Digital Assistance) devices as depicted in Fig. 7.



Fig. 6 Firebase stored data

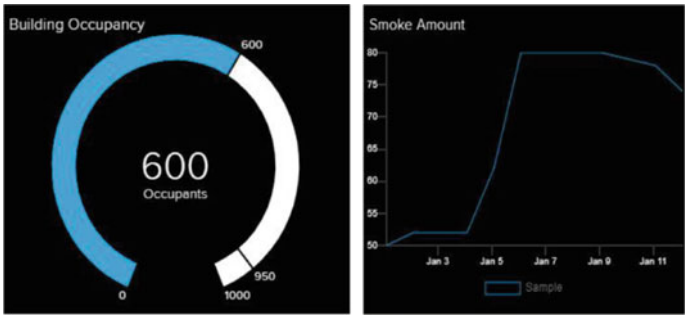


Fig. 7 Sample data for building occupants and smoke display dashboard

Table 1 Sample dataset generated by the system

Building ID	Room OD	Sensor node ID	Number of occupants	Smoke quantity	Time	Status
50	21	34	1	65	1:02:50	Normal
50	21	34	1	65	1:02:52	Normal
50	21	34	1	65	1:02:54	Normal
50	21	34	1	65	1:02:56	Normal
50	21	34	2	75	1:02:58	Normal
50	21	34	2	75	1:03:00	Normal
50	21	34	2	75	1:03:02	Normal
50	21	34	2	75	1:03:04	Normal
50	21	34	2	89	1:03:06	Normal
50	21	34	2	100	1:03:08	Fire
50	21	34	2	106	1:03:10	Fire

Table 1 shows all information accumulated from the system, such as building Id, Room Id, NodeSensorId, building occupancy, smoke quantity, time, and its status. The system analyzes the status of any spruce fire detection for ease of ERC's automatically.

6 Conclusion

This research detects spruce fire in buildings. The main objective was achieved to avoid casualty with less damage to properties caused by fire outbreaks. The system implemented was deployed to send a notification to the institutions in charge such as the fire brigade, and building control to notify them.

Future research work should focus on android applications for notifying using email over the cloud instead of using SMS notification. Moreover, advanced prediction methods could be used for predictive analysis.

References

1. MINEMA, National contingency plan for fire incidents, March 2019. http://minema.gov.rw/fileadmin/user_upload/MATRIX_PLAN_final.pdf
2. M. Ignatius,*Fire Outbreaks on the Increase Again?* (The New Times, 10 August 2016)
3. [Online]. Available https://www.newtimes.co.rw/section/read/202470. Last accessed 25 September 2020
4. J. Dutta, S. Roy, C. Chowdhury, Unified framework for IoT and smartphone-based different smart city-related applications. Microsyst. Technol. **25**, 83–96 (2019). https://doi.org/10.1007/s00542-018-3936-9

5. A. Bruno, P. David, C. Marilia, A non-intrusive approach for indoor occupancy, in *Polo II-Pinhal de Marrocos*, Coimbra (2018). https://doi.org/10.3390/s18113953
6. H. Wei-Ling, J. Ji-Yun, H. Chein-Shiun, L. Chiu-Kuo, S. Yan-Chyuan, Application of Internet of Things in a kitchen fire prevention system. Appl. Sci. **9**, 3520 (2019). https://doi.org/10.3390/app9173520
7. E. Shilpa, M. Hymavathi, T.U. Begum,Analysis of IoT based occupancy monitoring technique for energy efficient smart buildings. Int. J. Innov. Res. Comput. **IV**(10), 2–3 (2016)
8. A. Dey, et al., Namatad: inferring occupancy from building sensors using machine learning, in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 12–14 December 2016. https://doi.org/10.1109/WF-IoT.2016.7845462
9. N. Bekiaris-Liberis, J. Ming,Sensing by proxy: occupancy detection based on indoor CO_2, in *The 9th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM'15),* July 2015
10. A. Prasad, E. Wisam, T. Ramakrishna, Person detection techniques for an IoT based emergency, in *MOBIQUITOUS 2016: Adjunct Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services*, November 2016, pp. 77–82. https://doi.org/10.1145/3004010.3004019
11. B.S. Çiftler, S. Dikmese, İ Güvenç, K. Akkaya, A. Kadri, Occupancy counting with burst and intermittent signals in smart buildings. IEEE Internet Things J. **5**(2), 724–735 (2018). https://doi.org/10.1109/JIOT.2017.2756689
12. N. Prabakaran, R.J. Kannan, Sustainable lifespan of WSN nodes using participatory devices in a pervasive environment. Microsyst. Technol. **23**, 651–657 (2017). https://doi.org/10.1007/s00542-016-3117-7
13. W. Li, W. Zhang, Sensor selection for improving the accuracy of target localization in wireless visual sensor networks. IET Wirel. Sens. Syst. **2**, 293–301 (2012). https://doi.org/10.1049/iet-wss.2012.0033
14. T. Celik, H. Demirel, H. Ozkaramanli, M. Uyguroglu, Fire detection using the statistical color model in video sequences. J. Vis. Commun. Image Represent **18**, 176–185 (2007). https://doi.org/10.1016/j.jvcir.2006.12.003
15. Z. Liu, A.K. Kim, Review of recent developments in fire detection technologies. J. Fire Prot. Eng. **13**, 129–151 (2003). https://doi.org/10.1177/1042391503013002003
16. J.P. Dukuzumuremyi, B. Zou, D. Hanyurwimfura, A novel algorithm for fire/smoke detection based on computer vision. Int. J. Hybrid Inf. Technol. **7**, 143–154 (2014). https://doi.org/10.14257/ijhit.2014.7.3.15
17. L. Rossi, M. Akhloufi, *Dynamic Fire 3D Modeling Using a Real-Time Stereovision System.* (Springer, Dordrecht, the Netherlands, 2010), pp. 33–38. https://doi.org/10.1007/978-90-481-3656-8_8.
18. T. Celik, Fast and efficient method for fire detection using image processing. ETRI J. **32**, 881–890 (2010). https://doi.org/10.4218/etrij.10.0109.0695

Achieving Sustainable Village Development Through Geo-information Application



Sonal Mobar Roy, N. S. R. Prasad, and B. Srinuvas

Abstract According to Census 2011, India has majority of the populations residing in six lakh and above villages. With over seventy-five years of development, the government still strives to help the masses cross the threshold of poverty through its various interventions. However, the rural people are still to get access to basic amenities including drinking water, a proper house, a secure livelihood, education and social security. In this study, the authors study Burgula Panchayat that also has tribal thandas (hamlets) and is near the capital city of Hyderabad. The authors use survey method and Open Data Kit to collect data and GIS application to map the assets and create thematic maps for visualisation of data. An interactive Performance Management Dashboard is created to monitor and analyse the pace of development with enhanced citizen engagement. An attempt has been made by the authors to map already existing development entities and to identify the gap areas and suggest for future village development plans.

Keywords GPDP · GIS · GPS · Sustainable · Mapping · Rural · Spatial planning

1 Introduction and Background

Even after seventy-four years of attaining Independence, India struggles to provide the fruits of development to the masses whose lives are riddled with poverty. Creation of rural employment to mitigate economic delinquency has been on the cards of all the governments that have risen to power. Due to vast diversity in the country, given the various topographical, geographical, physical, economic or social and agro-climatic zones, planning is a big challenge per se. Spatial planning in rural areas is found to be completely absent. Spatial planning in rural areas means, arranging the land use that is critical to the economic development of aspirations of the rural people.

S. M. Roy (✉) · N. S. R. Prasad · B. Srinuvas
National Institute of Rural Development and Panchayati Raj, Hyderabad 500030, India
e-mail: sonalmobarroy.nird@gov.in

N. S. R. Prasad
e-mail: nsrprasad.nird@gov.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_80

Spatial planning refers to the methods and approaches which affect the distribution of diverse populations and activities across places and spaces and topology, for habitat environment, having basic infrastructure of communication and transport and access to basic provisions of life and sustenance. Spatial planning can be done with the help of the latest geospatial technology tools like GIS, remote sensing and GPS.

Moreover, the spatial plans are prepared for cities and towns popularly known as Master Plans and Development Plans. These are notified under the respective State Town and Country Planning Acts and Urban Development Acts. These Acts in their title include Country Planning; however, the same has been overlooked, and there is no cognisance of preparing Master/Development Plans for rural areas nor much attention has been given by the local governments to design focussed interventions for the same. However, over the period of years, it is evident that stress has never been laid on preparing spatial plans for rural areas and taking into account the vast rural population of the country who have been deprived of the access to basic facilities. Herein lies the importance of preparing a template for a spatially integrated version of the GPDP, namely the Gram Panchayat Spatial Development Plan (GPSDP).

Gram Panchayat Development Plan aka GPDP is to be prepared by the gram panchayat (local body) for the basic services within the functions devolved to them as per state laws. Participation of people is the key factor in the success of GPDP. This is mandated under the seventy-third Amendment Act that has paved way for democracy and laid stress on decentralised governance. The Fourteenth Finance Commission award has created an opportunity for responsive local governance at institutional level of the gram panchayat, and the guidelines issued by Ministry of Finance instruct that proper plans, i.e. Gram Panchayat Development Plan be developed. Main role is played by the community, especially the gram sabhas. They need to ensure compliance to the mandates of social justice and economic development as laid out in Article 243G, while they list out the priorities.

It helps to transform GPs into institutions of local self-governance and to concretise the GP's identity as development institution. From a vantage point, the process of participatory planning for a Gram Panchayat Development Plan envisages providing a better service delivery and looks forward to enhance citizenship. It plans for volunteerism and facilitates space for an alliance of people's institutions and groups and strengthens the decentralisation of powers and improves governance at the local level. The Rural Area Development Plan Formulation and Implementation Guidelines (RADPFI 2017) emphasise the need for the preparation of rural spatial plans, integrated with the overall development. The RADPFI guidelines aim to provide direction for the preparation of spatial plans for gram panchayat (GP) and also mentions the required alterations and additions in the existing statutory provisions of planning. The need for the RADPFI guidelines arises from the fact that there are 6.49 lakh villages in the country, and 68.84% of the total population resides in the rural areas (Gram Panchayat Spatial Development Plan, SPA, Bhopal 2018).

2 GIS and Its Importance

Geographical information system (GIS) is a computer system built to capture, store, manipulate, analyse, manage and display all kinds of spatial or geographical data (Krzysztof 2019). By relating seemingly unrelated data, GIS can help individuals and organisations better understanding of spatial patterns and relationships. Moreover, GIS is adopted as a tool for analysing and integrating the spatial and non-spatial data in the project. It is used as an information database, analytical tool and as a decision support system (DSS). Disparate data that may include data from remote sensing, data from census records and topographical sheets can be placed on one platform through GIS usage. Remote sensing has emerged as an inevitable tool for watershed development, and it helps to generate solutions to facilitate sustainable development. An approach of GIS and remote sensing adds more benefits to delineate the target areas for the apt preparation of action plans. Most of the government interventions are increasingly using technology to support last mile delivery of public services. While improving accountability, the use of technology ensures that benefits reach those who are most deserving.

2.1 Integrated Spatio-economic Planning Framework for Rural Settlements

Spatial data analysis is a multidisciplinary activity that covers a diverse set of entities that include land and water resources, geography, urban planning, hydrology and earth sciences. These datasets may be derived from text, maps, charts, organisations, aerial photographs, satellite images and ground information. The management and analysis of such large volumes of spatial data require a computer-based system called geographic information system (GIS) which can be used for solving complex geographical, hydrological and planning problems (Garg 2008). Any time access to records, easy retrieval of data and visualisation through maps make it user-friendly and interactive. Anytime and anywhere verification of records is, thus, enabled by GIS. Increased legitimacy and acceptability of the PRIs among its stakeholders is, therefore, achieved (Guidelines for preparation of GPDP by MoPR 2018).

3 Objectives

The main objective of the authors is to assess the pace of development in Burgula Panchayat. The authors make an attempt to assess the available land and water resources using remote sensing data map, to map thematic information by interpreting the satellite imageries and also from available resources. The thematic layers include land use and land cover, drainage, watersheds, roads and slope to prepare the

thematic layers based on the socio-economic data available in Mission Antyodaya. This would finally help the authors to generate the action plans for infrastructure, water resource development, etc. Moreover, the authors aim to map thematic information by interpreting the satellite imageries and also from available resources. This will help in identifying the penetration of the intervention along with exploring the gap areas for future planning and to generate the action plans for infrastructure, water resource development, etc.

4 Methodology

Both qualitative and quantitative approaches were used in this study. Burgula Village, Rangareddy District in Telangana, was selected for Gram Panchayat Spatial Development Plan. The GPSDP incorporates the spatial layers corresponding to attributes like physical features, land holding and land ownership of revenue lands, land use and land cover, overall physical and social infrastructure, built environment parameters like housing typology. It also integrates the non-spatial attributes like socio-economic condition and governance dimensions. The data collection included intensive primary survey, data from Census 2011 and Mission Antyodaya data. The data are collected through crowd-sourcing approach in collaboration with local youth through an NGO and PRI members. Open Data Kit (ODK) forms were used to collect data including pictures and videos and geo-tagging the same. Other data collection tools such as interview schedules, questionnaires and government officials working at village level and in collecting household level data were made use of. Household surveys are conducted to gather data for mapping the whole village along with ODK. The ODK forms helped in generating Excel sheets and maps and subsequently converting raw data into insights. Visualisation dashboards were finally created.

5 Case of Burgula Panchayat

Burgula is a village in Farooqnagar Mandal in Mahbubnagar District of Telangana State, India. It belongs to Telangana region. When re-organisation of Telangana State took place, Burgula Village Farooqnagar Mandal was re-organised from Mahbubnagar to Ranga Reddy District. It is located 39 km towards north from district headquarters Mahabubnagar and 8 km from Farooqnagar. Burgula is bounded by Farooqnagar Mandal towards north, Keshampeta Mandal towards east, Kothur Mandal towards north and Nawabpet Mandal towards west. Telugu is the local language. The total population is approximately 5993, and the total number of houses are approximately 1452. The female population is 48.6%, village literacy rate is 52.7%, and the female literacy rate is 21.1%. The authors discuss the case of Burgula Panchayat in this paper. It was one of the panchayats that was identified by NIRDPR under Village

Development Plan and has seen a very good participation of local panchayat leaders in carrying out government interventions for development.

6 Results

Gram panchayats are entitled to provide basic services and take up development works related to the functions devolved to them. As per the eleventh Schedule of the Constitution of India, there are 29 subjects where gram panchayats could work to ensure economic development and social justice. Sector and indicator-wise gap analysis is provided below in web portal. The eleventh scheduled of the constitution created by the seventy-third Amendment contains 29 subjects on which the panchayats shall have administrative control. The study team took all the 141 indicators in these 29 sectors and created a real-time interactive dashboard for easy monitoring, evaluation and dissemination of data that include agriculture, land improvement, minor irrigation, animal husbandry, fisheries, social forestry, minor forest produce, small-scale industries, Khadi, village and cottage industries, rural housing, drinking water, Fuel and fodder, roads, rural electrification, non-conventional energy, poverty alleviation, education, vocational education, adult and non-formal education, libraries, cultural activities, markets and fairs, health and sanitation, family welfare, women and child development, social welfare, welfare of the weaker sections, public distribution system and maintenance of community assets. The authors have attempted to map the same through GIS and remote sensing and corroborating data with first-hand ethnographic approach. In the following paragraphs, selected indicators are being discussed that reflect the pace of development in the Burgula GP. Apart from that, the screenshots reflect the distribution of development interventions across the six villages.

1. **Agriculture and Irrigation**: Under the sector of agriculture, eight parameters have been covered. As per Fig. 1, it can be seen that government seed centre is moderately available at only one village, i.e. Kasireddyguda, and other villages are devoid of such major facility. Irrigation is one of the most important factors in agriculture. In Burgula Panchayat, the land is mostly dry and not suitable for agricultural practices. As is evident from Fig. 2 above, soil testing centre services are available at Kadiyalakunta Thanda, Kasireddyguda and Chintaguda. However, Kundal Kunta Thanda is devoid of any such facility.
2. **Drinking Water**: Water is a basic need for all living beings. The government ensures that door-to-door supply of portable drinking water is made available. From Fig. 3, it can be deduced that piped tap water is available in all the villages of the gram panchayat.
3. **Roads**: All-weather roads form the spine of the economy of the country. It is of the utmost importance that infrastructure, especially roads are developed all across the country to make transportation easy and commutable. As can be seen from Fig. 4, three villages, namely Burgula, Kasireddyguda and Narella

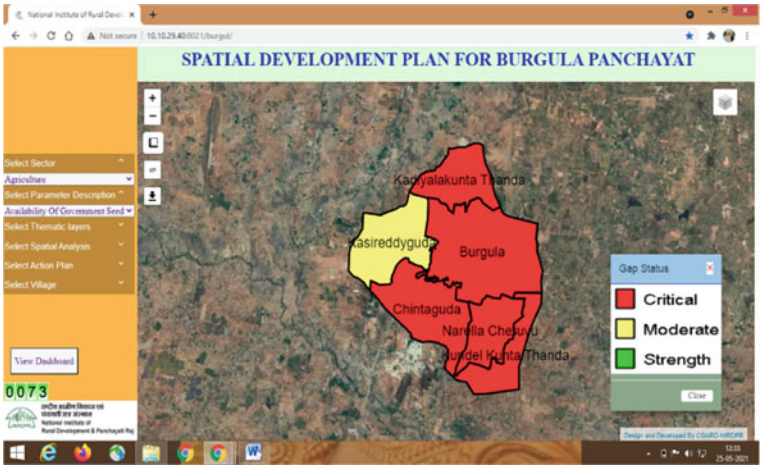


Fig. 1 Availability of government seed centres

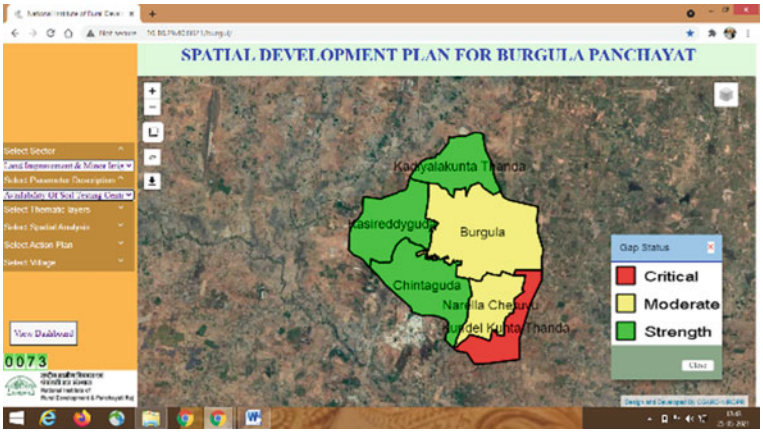


Fig. 2 Availability of soil testing centres

Cheruvu are connected with all-weather roads, while the tribal villages on the outskirts of the gram panchayat are yet to be connected and are left in silos.

4. **Public Distribution System and Primary School**: Over the years, PDS has become an important part of government's policy for management of food economy in the country. The basic aim is to provide essential commodities like rice, wheat, sugar, and edible oil and kerosene at subsidised prices. According to Fig. 5, it can be seen that Burgula does not have a public distribution service. However, the same is available in Kasireddyguda, Chinatguda and Narella Cheruvu.



Fig. 3 Availability of piped tap water



Fig. 4 Availability of all-weather road

The key factor in development is education. It is essential that all the citizens are educated and skilled to be able to lead their lives in a better fashion. Under Right to Education Act, 2003, all children from 6 to 14 years of age are entitled to receive free and compulsory education. Figure 6 depicts that a primary school is available in all villages of the gram panchayat. All the people residing in Burgula Panchayat can avail the benefits of primary schools in their respective villages.

5. **Health and Sanitation**: Public health depends on the condition of health and sanitation of that place. It is essential that people have access to a Primary Health Centre and have proper drainage facilities and waste disposal system in place. It is seen from Fig. 7 that a Primary Health Centre is located at Burgula only,

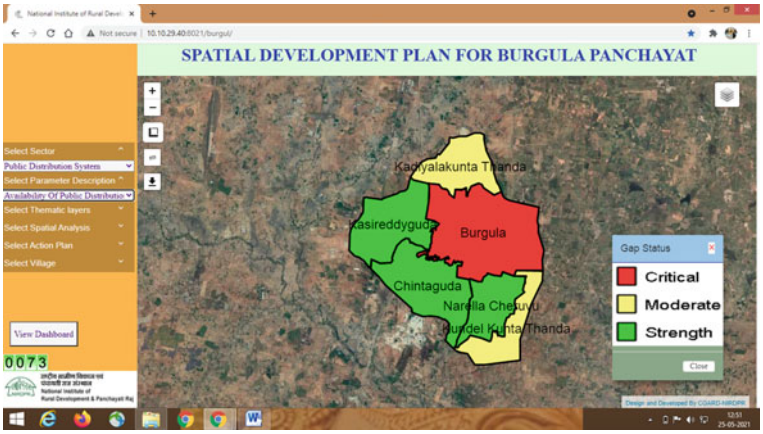


Fig. 5 Availability of public distribution system



Fig. 6 Availability of primary school

and other villages are devoid of having a centre. The people of these villages have to commute and access services at Burgula.

6.1 Thematic Layers

The authors also came up with thematic maps for a better understanding of village development plan. These included assets, cadastral maps, drainage pattern, groundwater prospects, land use and land cover, MGNREGA assets, roads, railway lines, settlements, built-up growth and watershed areas. Mapping these has helped in understanding the needs and gaps areas of the village.

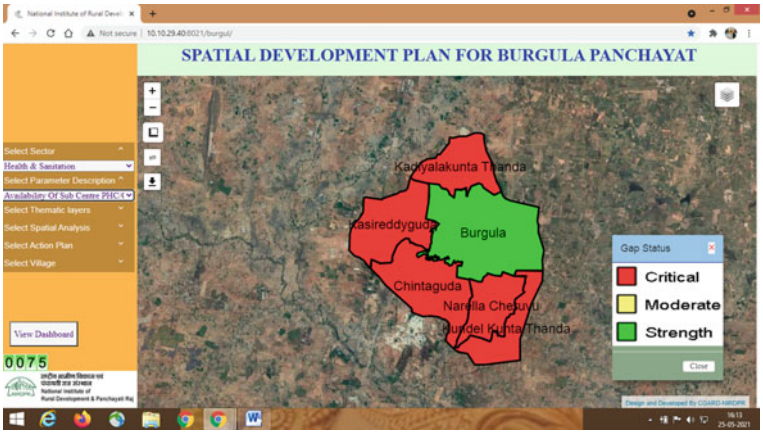


Fig. 7 Availability of a Primary Health Centre (PHC)

As per Fig. 8, the thematic layer shows the coverage of each primary school in each village of Burgula Panchayat. It is to be noted that under Sarva Shiksha Abhiyaan and Right to Education Act, 2003, all children aged 6 to 14 years of age have to receive free and compulsory education. To have proper access to schools, norms allow for a primary school to be in radius of 3 km from village, a middle school to be in 5 km radius and a high school to be in 10 km radius. There are various thematic layers available on the dashboard to show land use and land cover in Burgula Panchayat. All the villages are mostly covered in cropland, followed by plantation and some barren lands. Various groundwater prospects can be seen in another thematic layer that shows that the ground water recharge conditions are poor to moderate in most of the areas in the study area. The good groundwater conditions are confined to valley



Fig. 8 Thematic layer showing primary schools covering an area in each village



Fig. 9 Interactive performance management dashboard

fills in the study area. Another thematic layers shows MGNREGA assets created at Burgula Panchayat, followed by a layer showing community assets. These include drought proofing, individual land works, land development and assets created in rural sanitation. It can be drawn from the thematic map that a good number of assets have been created under the MGNREGA programme, and people seem to quite aware of the benefits drawn from the assets, thus, created.

6.2 Interactive Performance Management Dashboard

The authors came up with an interactive performance management dashboard that enables the users to check the pace of development at Burgula Panchayat. With the help of first-hand data collected through ODK, a database was created. This was collaborated with satellite imagery. The spatial maps helped in mapping the indicators. Various interactive pie charts show the distribution in relation to religion, community, ownership of house, type of house, having a bank account, having a ration card, etc. The dashboard enables the users including the public and government functionaries to monitor the development process related to all 141 indicators mentioned above. The data help in projecting and planning and allocation of resources in a better manner. Moreover, the visual maps help the uninitiated to understand the pace of development and contribute further in the village development plan (Fig. 9).

7 Discussion and Conclusion

Having a sustainable model of development is an essential requirement today. From the MDGs to the SDGs, the government has not left any stone unturned to cater to

the marginalised section of the society and ensures access to the fruits of development. In this study, the authors have made an attempt to map a panchayat, engage the community members, assess their needs and help them understand the process of development through GIS-based application and benefits drawn from its usage. It helps to create decision support system that guides in execution and implementation of activities that are ideated and planned. For making a village development plan, it comes in handy for the common people to see the visual maps in different colours and assess the performance across the villages. The authors also came up with the thematic maps as mentioned above. They facilitate taking queries and generating responses on the maps for easier visualisation. This helps in internalisation of the output and a responsive engagement with the user. Through these maps, all the works done at the village level and any convergence plans that have led to developing assets can easily be monitored. The interactive dashboard created by the authors helps in performance analysis and management. Performances of all GPs based on selected indicators across each district/block-wise can be visualised on thematic maps. This will help every GP to know about the best performance on any selected indicator, which has been already achieved in the district. Moreover, the GIS-based management dashboard provides senior management, bureaucrats, consultants and scholars with the status of on-going plans/schemes. On the other hand, the interactive dashboard leads to enhanced citizen engagement. Two-way interaction with users may result in reducing old school paper work and maintenance of records and exhausting manpower and chaotic over the counter service delivery. The authors have made an attempt to provide cost-effective solution for utilisation of resources and maximising of benefits.

References

1. Burgula data retrieved from http://www.onefivenine.com/india/villages/Mahbubnagar/Farooqnagar/Burgula on 2nd October 2018
2. Census of India, Census of India, Office of the Registrar General and Census Commissioner, New Delhi (2011)
3. P.K. Garg, Spatial planning of infrastructural facilities in rural areas around Roorkee, Uttarakhand, India, in *FIG Working Week 2008*, Stockholm, Sweden (2008)
4. Guidelines for preparation of GPDP by MoPR (2018). https://www.panchayat.gov.in/gpdp-guidelines-by-mopr
5. N. Krzysztof, Chapter 2: Territory, space, place and beyond. (Springer Science and Business Media, LLC, 2019)
6. Rural Area Development Plan Formulation and Implementation Guidelines 2017 retrieved from www.panchayat.gov.in ›asset_publisher› document retrieved on 20th May 2021
7. SPA Bhopal, Gram panchayat spatial development plan Barkheda Salam Gram Panchayat (2018)

An Analytical Overview of the State-Wise Impact of COVID-19 in India



Rupal Lohani, Vidya Suresh, Eric George Varghese, and S. Thara

Abstract The rise of coronavirus has exposed a trivial response to this major community disaster. The National Disaster Management Authority (NDMA), headed by the Prime Minister of India, is the main body for COVID-19 in India. It has been widespread in India despite the efforts of suppressing it. Due to its high transmission rate, India has taken several countermeasures and clinical trials to study the mutations and other antibodies. This study aims to visualize the main cause of the difference in the severity of cases among the states of India, taking into consideration the factors that mobilized the spread, along with the actions undertaken by the Indian government to control the spread of the virus. This paper introduces the data set and provides a comprehensive overview of related data visualization tools, existing techniques, and systems for analyzing the results. Finally, we have enabled the presentation of data with graphics, making comparisons more understandable, to help allocate resources (worldwide) to the states in India that are in need.

Keywords COVID-19 · State-wise · Data visualization · India · Lockdown · Trend analysis · Cure rate · Death rate · Active cases

1 Introduction

SARS-CoV-2 commonly referred to as COVID-19 is a respiratory virus that has taken the world by a storm and globally changed the world's infrastructure. Virulence of COVID-19 was first detected in India's state of Kerala in January 2020.

R. Lohani (✉) · V. Suresh · E. G. Varghese · S. Thara
Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India
e-mail: rupallohani@am.students.amrita.edu

V. Suresh
e-mail: vidyasuresh@am.students.amrita.edu

E. G. Varghese
e-mail: egvarghese@am.students.amrita.edu

S. Thara
e-mail: thara@am.amrita.edu

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_81

Since then, it has been spreading uncontrollably all over India. The earliest clusters of locally acquired cases emerged in Chennai with a total of 124 total cases toward the end of March 2020 and surrounding eastern coastal districts of Tamil Nadu state [1]. The rise of these cases raised concern for the Indian government and thereby surveillance of the intensity of COVID-19 was initiated with airport screening, especially for travelers from China. Indian states have neglected public health and lack of surveillance and monitoring of the spread of the COVID-19 virus affected several sectors of the economy [2]. Since India is a developing country, a complete market shutdown throttles the economy to the highest degree.

The Government of India implemented several lockdowns and restrictions to keep the spread minimal, resulting in a heavy blow to the economy, making it difficult to implement further precautions [3]. Another factor of the widespread propagation of the virus was the lack of awareness. Civilians did not realize the intensity and went about their normal routine, accelerating the spread until the virus was widespread. The virus descended on every state in India, albeit few states could control the pace and keep it minimal, whereas the rest of the states were confronted with unmanageable proliferation. The various sectors of the Indian economy were unevenly affected due to the different levels of the spread of COVID-19. With the steep rise of cases in recent times, there is an acute shortage of hospital beds. COVID-19 patients under emergency care are in great need of plasma donations [4]. The objective is to visually illustrate which states in India need help and present the data comprehensively. This will aid in a global effort to provide resources to the states that are in need the most. This study aims to identify the severity of cases throughout Indian states through

- The identification of the source of COVID emersion in India
- Prominence COVID cases per state
- Death versus recovery rates, monthly COVID cases per state/union territory
- Correlation between state/union territory population size.

2 Related Works

Several other papers that have been published about COVID-19 focus more on the effect from a social and economic standpoint and the resulting impacts and advancements made from it, mentioned in the paper “CoV2eX: A Covid-19 Website with Region-wise Sentiment Classification using the Top Trending Social Media Keywords”. Talks about an algorithm take in the most used keywords found on social media since the initial lockdown to find out the general populaces emotions in a given region [5]. Another similar paper “Comparative study of Twitter Sentiment On COVID-19 Tweets” uses natural language processing and machine learning algorithms such as logistic regression to analyze “tweets” from Twitter [6]. Rather than focusing on a region such as the previous paper, this one focuses mainly on keywords taken from Twitter that are COVID-19 related. These papers focus on the psycholog-

ical impacts of COVID-19, whereas our paper focuses on the impacts of COVID-19 on the human body such as the cure and death ratio.

The papers regarding technical advancements for the community from the damage of COVID-19 focus on economy and environment. From an economic view of COVID-19 impacts, "Local E-Shop Management System for Pandemic Situation" focuses on the welfare of small business and the creation of a management system for the growth of small business [7]. "Geo located alert via bottom-up IoT model in times of COVID-19, and other disasters" focus on the improvement of ad hoc IoT devices. It talks about a need for improved software during natural calamities especially during the virus [8]. The paper "Detailed View on Repurposed Drugs, Tracking of Vaccines, and Brief View on Prophylactic Nanomedicines as an Alternative Approach and Patient Care for COVID-19" mentions about the advancements that have been made in the pharmaceutical department such as drugs that have been reutilized to serve a different purpose, vaccine tracking, and the development of nanomedicines to prevent COVID-19 [9]. These papers talk about advancements that have been made for the complications that have been caused because of the COVID-19 pandemic, but they do not provide a model where it shows a prediction of how it will benefit the number of cases. The paper that has been created by our team provides a prediction model where it will show an estimate for the reduction of cases post lockdown.

3 Methodology

In the approach to investigate COVID-19 cases in India, several data analytical tools were built to derive a statistical report on the causal variables of COVID-19 in each state of India. Data visualization is just more than plotting numbers. It takes several implementations and rethinking the numbers on which data analysis is based. Before we focus on the implementation, we have reviewed information about the data set and efficient graphical tools.

3.1 Data Set Desciption

To ensure data validity, the "Covid_19_india" and "StatewiseTestingDetails" data sets [10] were collected in real time from Kaggle, an online trusted platform . The time frame of the data delineates the trend of COVID-19 cases in India, starting from the first case on January 30, 2020, to May 8, 2021. This data set was selected primarily due to its variables as it closely examines important factors that have influenced the number of cases in each state and can provide forecasts of potential case trends. State-wise incidences, such as death rate, recovery rate, and the number of confirmed cases, highlight the impact of the COVID-19 pandemic, through visual trends. Such visual trends will be conveyed in a graphical representation of the collected data.

Furthermore, a comparative analysis between foreign nationals and native Indians will help indicate the accurate causal factor of the emergence of the virus in India.

3.2 Tools Used

Python provides a vast set of analytical tools that have been utilized to analyze the data set. We have considered Pandas for data preparation, Matplotlib, seaborn or Plotly for data visualization. Statistical analysis was carried out using the IBM SPSS [11] on the early phase of COVID-19.

4 Analysis

A graphical representation of the data will relay an informative delineation of the COVID-19 pandemic trends through the various states in India. Preliminary screening of COVID-19 conducted by the Central Indian Ministry of Health included visitors from China and subsequently expanded to include other international travelers. Foreigners who returned to India were the most significant cause of the increase of India's COIVD-19 cases [12].

The visualized graphs clearly show that the states that were most affected were the states that have major metropolitan cities. COVID-19 prominence in Fig. 1 is arranged in ascending order and expresses the comparative number of cases in different states within India. The number of cases shows Maharashtra's variance in the number of confirmed cases to be the largest compared to Karnataka's next highest.

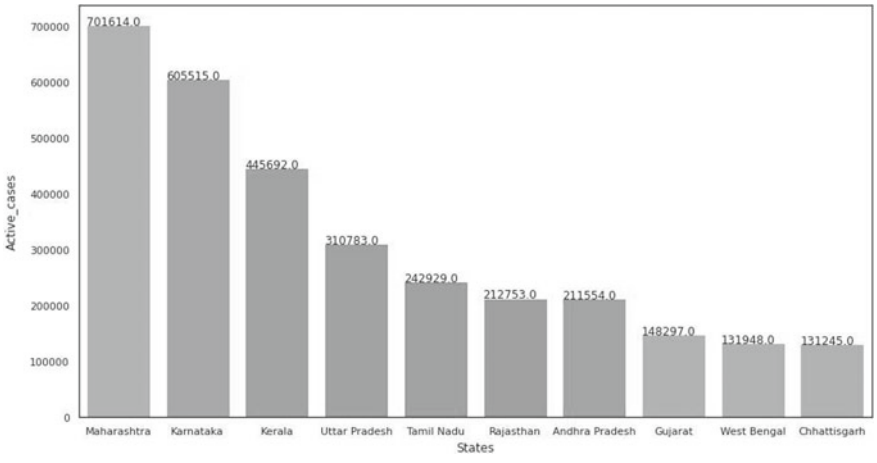


Fig. 1 Bar graph representing the number of active cases per state as of May 8, 2021 [13]

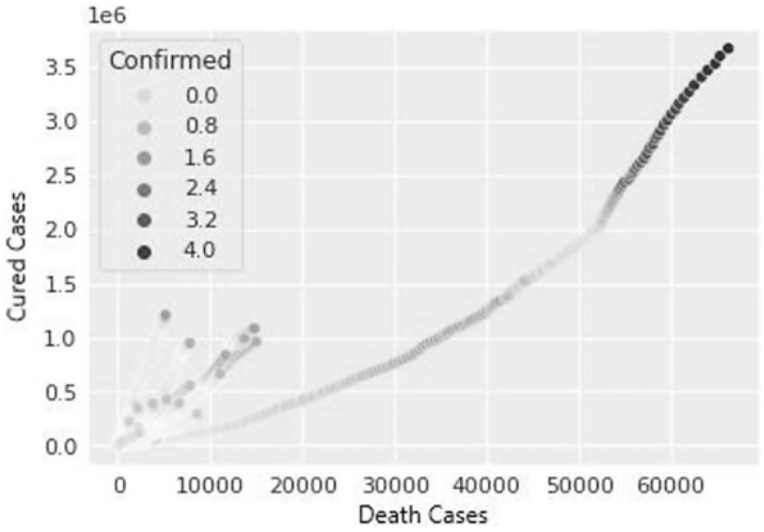


Fig. 2 State-wise scatter plot of death cases versus cured cases over confirmed cases

Table 1 Median value across states [13]

States	Cured	Deaths	Confirmed	Active cases
Delhi	257224	5472	287930	11068
Kerala	87354	489	122214	24892
Maharashtra	1188083.5	38894.5	1473200	83433.5
Tamil Nadu	572438	9881.5	627899.5	12145.5

As seen in Fig. 2, the relationship between the death and cured cases implies a contrasted relationship against the active cases. The variance in the states clearly shows that though Maharashtra leads the country with the greatest number of COVID-19 cases, the state leads the country with the greatest number of cases cured.

The line plot in Fig. 3 expresses the growth of COVID-19 cases over the course of one year in Maharashtra, Kerala, New Delhi, Karnataka and Tamil Nadu with most COVID-19 cases. When examining regional differences, there were no significant differences between North Indian and the South Indian states. Exponential increases of COVID-19 were experienced from August 2020 to October 2020. The next spike in cases was experienced from late March 2021 and identified as the second wave. Although Maharashtra has consistently had the highest incidence of COVID-19 cases, in May 2020, Maharashtra's COVID-19 cases grew exponentially.

Though the state may have the highest number of cured cases, the state also leads the country with the highest death count with a margin of approximately 60,000. A comparative statistical testing between the states of Tamil Nadu, Maharashtra, and Kerala implies that the three states have the highest overall impact on India's

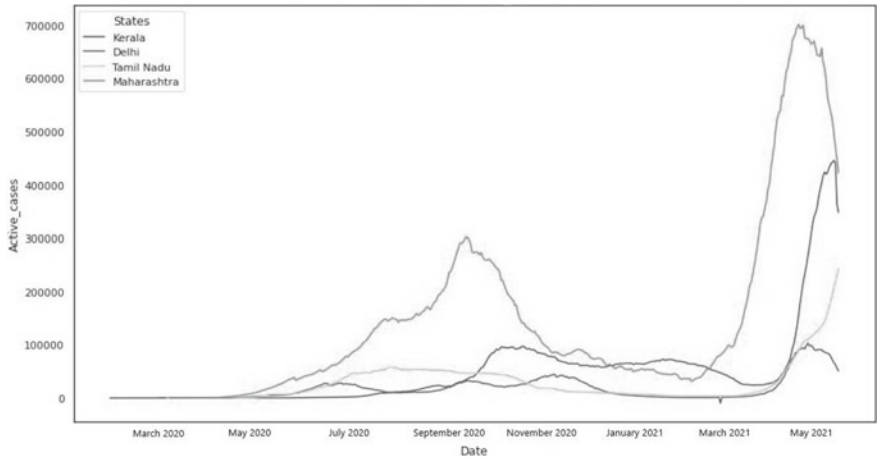


Fig. 3 Number of active cases per state [13]

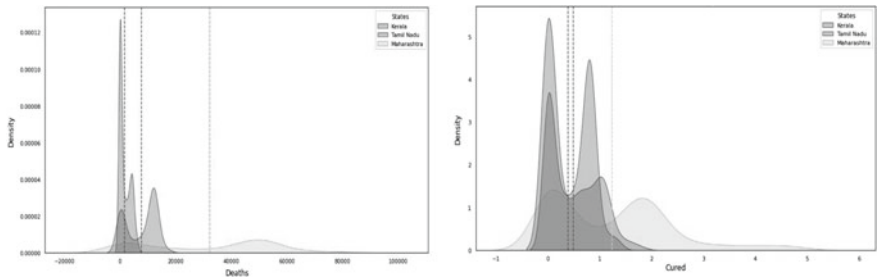


Fig. 4 Significant differences in death and cure rates [13]

COVID-19 rates. All three states Kerala, Tamil Nadu and Maharashtra have significant differences plotted (Fig. 4) in cure rate and death rate compared to overall impact.

5 Evaluation

India's situation is rapidly changing, and the country requires accurate executive approaches and monitoring plans. The course of evaluation for the research paper was to provide an overall analysis of the states that were the most affected. It was achieved by plotting different visual graphs and studying the statistical growth of the death rate, cure rate, and active cases over the course of the year. The data sets "Covid_19_india" and "StatewiseTestingDetails" share quality data from the states and union territories of India at daily level. The observations convey that almost all

states share the same trend in COVID-19 cases. Further performing the analysis, (in Table 1) we can evaluate Maharashtra having median around 83 K cases yet has a high range of cured value as well. But we cannot conclude rate by count, hence proportionality tests are evaluated (in Table 2) and each state shows a significant difference in their cure and death rates. Specifically, the evaluation criteria taken were the cured and death counts from the major states contributing in COVID-19 cases during the first wave and after sudden increase in the COVID-19 daily spike.

6 Discussions and Conclusions

Analyzing the COVID-19 death rates versus recovery rates enables researchers to decipher and predict morbidity rates. Examining the source of COVID-19 infection in India may contribute to the understanding of how to restrain the spread of the virus. The analysis depicted the variance of COVID-19 from the start of March 2020 to the present date. In the start of the pandemic, the virus was not nearly as contagious as it is now. The bar graph (Fig. 1) of the active number of cases gives an overview of the most affected states of India as of date through which we have analyzed the trend of the four most affected states with Maharashtra (7016140 active cases) being the most affected state. The two attributes of data—cured and deaths—were considered for a proportionality test (in Table 2), and it was concluded that for the three states, it proved a significant difference in cure and death rate. The statistical hypothesis can be stated that Maharashtra would be having the highest number of cure rate and death rate due to the state having the highest number of active cases. But, it was proven wrong when the proportionality test was done. Tamil Nadu had the highest cure rate out of the three states leading with 0.89% while Maharashtra only had 0.85%. The reason for this may be due to the recent lockdowns that India has been partaking in. Tamil Nadu's cure rate was predicted and expected that the lockdown is to bring down the increasing impact rate. Also, the effect of lockdown can be seen at the end of lockdown days (in Fig. 5). The line remained stagnant before March 2021, but after the implementation of lockdown and also arrival of vaccine deployment in India, the number of cure cases boosted up and the prediction model described the exponential rise of cured cases.

Understanding the alternative reasons for COVID-19 spikes can help mediate social gatherings, and identifying cases monthly may allow for determining key festivals or activities that involve large social gatherings that may be the cause for

Table 2 Proportionality test [13]

States	Cured	Death
Tamil Nadu, Maharashtra	0.89, 0.85	0.01, 0.01
Tamil Nadu, Kerala	0.89,0.78	0.01, 0.00

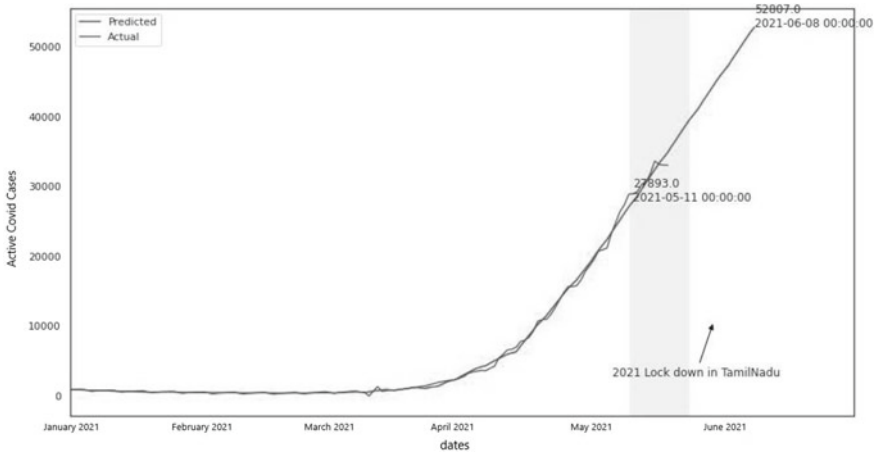


Fig. 5 Prediction model of active cases in Tamil Nadu post lockdown [13]

the COVID-19 spikes. By mapping the prevalence of COVID-19 cases per state, researchers focus more on how to reduce their intensity in those specific areas. It also allows for the distribution of resources to be promptly supplied to the places more in need. COVID-19 cases do not directly correlate to population size. The major states that were most affected were the states that have major metropolitan cities. The rest of the country experienced exponential spikes of COVID-19 cases from August 2020 to October 2020. If the government was more vigilant toward receiving international passengers, then this situation could have been under better control than it is now. In the current lockdown underway since March 25, 2020, the incidence of cases is anticipated to be significantly reduced. Currently, with the recent development of increased availability of COVID-19 vaccines, salutary recovery rates have been evident in the worst-affected states of Maharashtra, Kerala, Tamil Nadu and New Delhi. However, there are some limitations on how much this study can achieve; the lack of data available to the open public, which is being used for the study, limits the conclusions drawn. It is possible to extend the project with better data in the future once they are released.

References

1. S. Arunkumar, G. Sriram, C. Gnanadesikan, A review of covid 19 in tamilnadu with regression and correlation co-efficient. *Materials Today: Proceedings* (2020)
2. S. Udhaya Kumar, D. Thirumal Kumar, B. Prabhu Christopher, C. Doss, The rise and impact of covid-19 in india. Front. Med. **7**, 250 (2020)
3. V. Barbate, R.N. Gade, S.S. Raibagkar, Covid-19 and its impact on the indian economy. Vision **25**(1), 23–35 (2021)

4. A. Kumar, K. Rajasekharan Nayar, S.F. Koya, Covid-19: challenges and its consequences for rural health care in india. Public Health Pract. **1**, 100009 (2020)
5. A. Rajmohan, A. Ravi, K.O. Aakash, K. Adarsh, A.D. Raj, T. Anjali. Cov2ex: a covid-19 website with region-wise sentiment classification using the top trending social media keywords, in *2021 6th International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (IEEE, 2021), pp. 113–117
6. A.J. Nair, G. Veena, A. Vinayak, Comparative study of twitter sentiment on covid-19 tweets, in *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)* (IEEE, 2021), pp. 1773–1778
7. R. Nair, S.J. Yadhati, K.V. Vaisakh, et al., Local e-shop management system for pandemic situation (2021)
8. H.O. Lekshmy, T.R. Krishnaprasad, G. Vishwanath Gupta, K. Namitha. Geo located alert via bottom up iot model in times of covid-19 and other disasters, in *IOP Conference Series: Materials Science and Engineering*, vol. 1128 (IOP Publishing, 2021), p. 012001
9. K.S. Nair, S. Kamath, A. Rajan, S. Thomas, D. Aswin, S.M. Zachariah, Detailed view on repurposed drugs, tracking of vaccines, and brief view on prophylactic nanomedicines as an alternative approach and patient care for covid-19. Int. J. Appl. Pharm. 19–26 (2021)
10. Covid-19 in india | kaggle. https://www.kaggle.com/sudalairajkumar/covid19-in-india. Accessed on 06 Oct 2021
11. Spss Software—india | ibm. https://www.ibm.com/in-en/analytics/spss-statistics-software. Accessed on 06 Oct 2021
12. N. Jahan, P. Rubeshkumar, M. Karuppiah, I. Sambath, M. Sendhilkumar, K. Ilangovan, R. Ongesh, M. Sakthivel, R. Mohankumar, P. Ganeshkumar et al., Entry and initial spread of covid-19 in india: epidemiological analysis of media surveillance data, india, 2020. Clinical Epidemiol. Glob. Health **9**, 347–354 (2021)
13. Covid analysis & prediction | kaggle. https://www.kaggle.com/gcmadhan/covid-analysis-prediction. Accessed on 06 Oct 2021

An Analysis of FIPP Clauses with Respect to Data Lifecycle Phases and Privacy Properties



Asmita Manna, Anirban Sengupta, and Chandan Mazumdar

Abstract Introduction of data protection regulation and acts by different countries, especially guidelines like Fair Information Privacy Principle (FIPP), has made it almost mandatory for enterprises to implement data privacy protection throughout their information infrastructure. Data privacy is mostly managed either as confidentiality issue, risk management issue, or as policy/control implementation issue. If privacy is considered a control implementation issue, there must be a correspondence between privacy requirements/clauses with the control components. A scrutiny of privacy controls and privacy regulations reveals that privacy of personal data can be protected if specific privacy properties of data items are protected throughout the journey of the data in enterprise infrastructure. In this paper, an analysis of correspondence among FIPP clauses, data lifecycle phases, and privacy properties are presented. This analysis would help data controllers to identify and implement privacy controls more accurately and enable them to streamline data compliance activities.

Keywords Data lifecycle · E-Gov security · FIPP clause · Privacy controls · Privacy compliance · Privacy properties

1 Introduction

Over the last few years, different enterprises have been collecting, storing, and processing more and more personal data from individuals to provide customized and improved services. Increased usage of online transactions, IoT devices, social networking, etc. also results in a substantial amount of digital footprint left behind by an average person. With access to such high amount of personal data, it is easy to invade privacy of individuals. Therefore, different countries, including India [1], have incorporated or drafted data protection laws considering the security of their

A. Manna (✉)
Pimpri Chinchwad College of Engineering, Pune 411044, India

A. Sengupta · C. Mazumdar
Jadavpur University, Jadavpur, Kolkata 700032, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_82

citizens. Other than that, different organizations have come up with their own sets of guidelines for protecting the privacy of individuals. Such a guideline for promoting fair information practice in electronic marketplace, called 'Fair Information Practice Principle' (FIPP) [2], has been proposed by the United States Federal Trade Commission.

Fair Information Practice Principles are a set of principles and practices that defines how an enterprise should conduct collection, storage, processing, and transfer of data such that the security and privacy of customers are maintained. According to FIPP, activities related to personal data should comply with eight core principles: Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguard, Openness, Individual Participation, and Accountability.

In an enterprise, privacy is generally enforced by applying controls on different assets of the information infrastructure. A closer look at such privacy controls suggested by International Standardization Organization [3–5] and National Institute of Standards and Technology [6] reveals that not all controls are applicable throughout the journey of data within the enterprise. Instead, different controls are applicable for different phases of the data lifecycle and to protect one or more specific privacy properties of data.

As the controls are applicable to specific data lifecycle phases and privacy properties, the FIPP principles should also be decomposed as per privacy properties and lifecycle phases. In this paper, an analysis of relationships between each FIPP principle and data lifecycle phase is presented. Rest of the paper is organized as follows. Section 2 discusses existing research; Sect. 3 explains the FIPP clauses, data lifecycle, and privacy properties; Sect. 4 presents the analysis of FIPP clauses with respect to data lifecycle phases and privacy properties; finally, Sect. 5 identifies future work and concludes the paper.

2 Related Work

Many researchers have channelized their research toward implementing privacy in enterprise infrastructure. In this section, an analysis of some works which have considered data lifecycle for implementing privacy principles is presented.

In the privacy by design approach, Cavoukin [7] mentioned that privacy must be continuously protected throughout the lifecycle of the data and there should not be any gap in either protection or accountability. However, no direct relationship between data privacy and lifecycle phases has been identified in this paper.

Bamberger and Mulligan [8] tried to find out the privacy best practices for providing guidance to policymakers. They argued that privacy is framed as a part of risk management and they also concluded that privacy governance is about creating governance structures. This is one of the first works toward implementing data governance.

The Abstract Personal Data Lifecycle model [9], proposed by Alshammari and Simpson, is an abstract model for personal data lifecycles. This model identifies

the main operations, which are performed on personal data during its lifecycle and it also identifies distinct activities for each operation. Overall, this model helps to analyze functional requirements. However, the privacy clauses considered here are not specific to any privacy guideline or standard.

In [10], authors tried to analyze the relationship between the principles of the Brazilian General Data Protection Law—GPDL [11] and the stages of the data lifecycle. They concluded that the stages of the data life cycle map directly to the legal clauses. Hence, the data lifecycle model can be utilized for formulating a process that systematically addresses legal compliance activities. However, as the clauses of GPDL are different from FIPP, this paper cannot directly be used for compliance with FIPP clauses. Moreover, the authors have considered only four specific phases of the data lifecycle; this is a major limitation of the paper.

There is a dearth of specific research that tries to decompose privacy clauses with respect to data lifecycle phases and privacy properties. This work is an attempt to bridge this gap by identifying relationships of FIPP clauses with seven phases of the data lifecycle and privacy properties.

3 Background

3.1 Fair Information Practice Principles

The Fair Information Practice Principles [2] were first proposed in the year 1973 and subsequently different organizations like OECD, Council of Europe Convention, and European Union designed their own privacy directives based upon the core principles of FIPP. There are eight core principles of FIPP. These are:

i. Purpose Specification—This clause states that the purpose for which the personal data is collected should be specified at the data collection time itself and the subsequent usage should be for the specified purpose or other compatible purposes.
ii. Data Quality and Integrity—This states that the personal data should be relevant to the purpose identified for its use and it should maintain accuracy, completeness, and latest updates.
iii. Collection Limitation or Data Minimization—This specifies that personal data should be collected only if the data is directly relevant and necessary for the accomplishment of the specified purpose. Moreover, such data should be obtained by lawful and fair means and retained as long as is necessary for the specified purpose.
iv. Use Limitation—This describes how the usage of personal data should be limited. Personal data should not be shared, displayed, or used for purposes other than those specified except (a) with the consent of the individual or (b) by the legal authority.

v. Security—This expresses the security expectations from the data controller. It states that personal data should be protected by security safeguards against various security risks such as unauthorized access, destruction, use, modification, or disclosure of data.
vi. Accountability and Audit—Employees and contractors of data controller enterprises are accountable for complying with measures implementing the FIPPs and for auditing the actual use and storage of personal data. Ideally, strong and effective policies should be implemented.
vii. Openness or Transparency—FIPP advocates openness or transparency. It states that there should be a general policy of openness about developments, practices, and policies with respect to personal data. The information about policies and contact information for complaints/correction of personal data should be made available by the enterprise.
viii. Individual Participation—The enterprise should involve individuals in the process of using personal data and seek consent from individuals for the collection, use, dissemination, and maintenance of personal data to the extent possible.

Though different guidelines based on FIPPs present some other directives related to privacy, for the proposed analysis in this paper, these eight core principles are considered.

3.2 Data Lifecycle

Data lifecycle comprises several phases through which the data items pass, while in possession of an enterprise. The enterprise, which possesses personal data, is referred to as a data controller. A data lifecycle model helps the data controller to have a strategic understanding of the activities within a specific phase of the lifecycle. In [12], data lifecycle has been shown to be composed of four phases, namely: Collection, Storage, Recovery, and Disposal. Collection phase comprises filtering and organizing data, identifying the structure, format, and means of data collection. Storage phase comprises activities related to processing, transformation, modification, migration, and transmission of data. Recovery phase is related to reconstruction and re-visualization of data. Finally, the Disposal stage consists of identification of data that are no longer needed and removing those data appropriately.

Chisholm [13] proposed a seven-stage data lifecycle model for addressing the issue of data governance. This model also clearly defines the separation of different stages of data lifecycle. The seven stages are Capture, Maintenance, Synthesis, Usage, Publication, Archival, and Purging of data.

In Capture phase, the data enters the information infrastructure of the enterprise for the very first time. Data can either be captured directly or generated internally. In this phase, the enterprise decides which data to collect; it also specifies the purpose and usage of the data collection. In Maintenance phase, data is made ready for

analysis. New data values are derived from the captured data using deductive logic. In Synthesis phase also, new data values are derived from the captured data but here the derivation is done using inductive logic, i.e., with the help of experts' opinions, judgments, and intuitions and with the help of existing data sets of the enterprise. Techniques like data warehousing and data mining are used in these two phases. The Usage phase is defined as the application of data in the form of information to tasks that the enterprise needs to run and manage its business processes. Any special permission needed for personal data processing can be associated with this stage. Publication phase represents the point in time when data is transferred to a location outside the enterprise. Whenever data is sent outside, the enterprise or the original data controller will have less control over that data, and updating that data would be difficult. Data breaches can also be considered as a form of data publication. In Archival phase, data is removed from all active production environments and stored securely such that it can be brought back to the active environment whenever needed. It can be seen that the data is still a part of the information infrastructure of the enterprise, but maintenance, synthesis, or publication of these data are no longer permitted. Any specific data retention policy specified by privacy mandate should be associated with this phase. The final stage of data lifecycle involves the Purging of all instances of data items from the information infrastructure of the enterprise.

3.3 Privacy Properties

Privacy was first defined as the 'right to be left alone' by Samuel Warren and Louis Brandeis in the article 'The Right to Privacy' [14]. However, this definition is not suitable for technical implementation. Pfitzmann et al. [15] proposed a more technical definition of privacy. As per this definition, privacy can be expressed as a set of seven parameters namely confidentiality, integrity, availability, anonymity, unlinkability, undetectability, and unobservability. Thus, to protect privacy means protecting the privacy properties of the data item. Confidentiality, integrity, and availability are widely used properties whose definitions are rooted in information security aspects. Here, we discuss the remaining privacy-specific properties.

Anonymity of a subject means that the subject is not identifiable within a set of all possible subjects. If the anonymity of the data owner is to be protected, the dataset related to that individual should be protected in such a way that the dataset alone cannot single out the individual.

Unlinkability is the lack of ability to establish a link between two or more pieces of data items. In an enterprise, each personal data item is selected for a specific purpose, or it can be said that each purpose works with a set of personal data. All data items belonging to a particular purpose cannot be unlinkable, but the complete dataset needed for a particular purpose can be unlinkable from the dataset of some other purpose.

Undetectability of an item of interest means an attacker cannot sufficiently determine its existence. It means a data item is undetectable, if and only if no deduction

about the existence of that data item can be made from all other deductions made by the adversary.

Unobservability of a data item means: (i) the data item is "undetectable" with respect to all uninvolved subjects; and (ii) its subjects are "anonymous" even with respect to other involved subjects.

Our analyses of FIPP clauses reveal that each of them mandates the protection of one or more privacy properties during each data lifecycle phase. If these clauses can be decomposed in terms of privacy properties and data lifecycle phases, identifying appropriate technical controls to implement the same would be easier.

4 Analysis of FIPP Clauses Considering the Stages of Data Lifecycle and Privacy Properties

4.1 Relationship of FIPP Clauses with Data Lifecycle Phases

For the analysis of the relationships between FIPP clauses and data lifecycle phases, the data lifecycle model proposed by Chisholm [13] is being used in this paper. Each relationship can be one of three types, namely: highly relevant, relevant, or irrelevant. The relationships are shown in Table 1. The value 3 denotes that the relationship is highly relevant, 2 denotes it is moderately relevant and 1 denotes it is irrelevant.

Purpose specification principle has a very pronounced relationship with the Capture phase because, at this stage, the data controller specifies the purpose for which the data is collected. This is also *relevant* in the Usage and Publication phases. In Usage phase, the data is directly used by a business process of an enterprise; the

Table 1 Relationship between data lifecycle phases and FIPP clauses

	Capture	Maintenance	Synthesis	Usage	Publication	Archival
Purpose Specification	3	2	2	3	3	1
Data quality and integrity	3	3	2	3	3	2
Collection limitation and data minimization	3	2	1	1	1	1
Use limitation	1	2	3	3	3	1
Security	3	3	3	3	3	3
Accountability and Audit	1	3	3	3	3	2
Openness and transparency	3	3	3	3	3	3
Individual participation	3	3	2	3	3	2

business process should have the same purpose as that of the data. In Publication phase, data is sent outside the enterprise; ideally, the data should only be released if the data owner provides consent for the same. Therefore, it is important that the data owner should provide consent for the particular purpose. In Maintenance and Synthesis phases, new data are extracted from the personal data. As per the clause, the data should not be used for some other purposes barring for which consent has been provided by the owner. Therefore, the purpose specification is *moderately relevant* in these two phases. However, purpose specification is *almost irrelevant* in the Archival and Purging phases because archival and deletion are mostly dependent upon enterprise's policies, not on individuals' concerns.

For the data quality and integrity principle, *high relevance* is attached with data Capture, Maintenance, Usage, and Publication phases. In the Capture phase, the quality factors should be defined. As the Maintenance phase is responsible for storage of data and the next few phases are dependent on stored data, this principle is *highly relevant* here. In the Usage phase, it should be ensured that processing is done with accurate data and the integrity of data is maintained. In the Publication phase too, it should be ensured that data integrity is maintained because distorted data may harm the privacy of data owners. This principle is *moderately relevant* during Synthesis and Archival phases. During Synthesis, personal data is not directly used but insights are derived from such data. If the data is of bad quality, insights derived from the data may be different but that does not directly affect the privacy of individuals. In Archival phase too, data is not directly used for any purpose but archived in a safe location. As the data is not accessed, even if the data is of bad quality and integrity, an individual's privacy is not directly harmed.

Regarding collection limitation and data minimization, it can be said that this principle is *highly relevant* during Capture and Maintenance phases. During the Capture phase, rules, policies, and purpose of data collection are defined according to enterprise policies. While defining the policies, minimum amount of personal data, strictly necessary for fulfilling the purpose, should be identified and collected. During Maintenance phase too, minimum data storage should be adopted such that the minimum data retention criterion is met, and the storage should be consistent with purpose of data collections. This principle is not much relevant during the rest of the phases because if this principle is followed during Collection and Maintenance phases, the remaining phases will automatically deal with minimum data.

Use limitation is *highly relevant* during Maintenance, Synthesis, Usage, and Publication phases. According to this principle, the data in possession of the enterprise should be used carefully according to the consent of data owners and for specified purposes only. While deriving new insights from personal data during Synthesis, it should be ensured that the processing is lawful and done according to the specified purpose of the data. Similarly, during the Usage and Publication phases also, it should be ensured that the data is used for specified purposes only and the data owner has provided consent for the same. During Capture phase, this is not relevant because data is neither processed nor published. For Archival and Purging too, this principle is not relevant for the same reason.

Security is of utmost importance during all phases of the data lifecycle. To protect personal data from unauthorized access and other intentional or accidental actions which may lead to alteration, destruction, publication of data, or revelation of identities of individuals, leading to privacy harms, it is needed that security controls should be in place from Capture to Disposal of data.

The principle accountability and audit is *relevant* for all phases of the data lifecycle as it is mandatory to plan, incorporate and validate such controls throughout the journey of personal data in an enterprise environment such that compliance with data protection standards can be achieved. However, it is not much relevant during the Capture phase if the data collection is automated without any individual's direct involvement from the enterprise end, and the data owners are well-informed about the data collection. It is *highly relevant* during Maintenance and Synthesis phases as the new insights about personal data are obtained in these phases and data are classified or clustered which, in turn, increases the risk of privacy breaches. This clause is *highly relevant* to Usage phase too because the data is directly used by business processes to get meaningful results. This is *highly relevant* for Publication phase because this phase involves third parties and data breaches may occur. For Archival, it is moderately relevant as the data archive can be altered, if needed. Accountability and audit are *highly relevant* during Purging, as non-compliance can lead to legal issues for the enterprise. The principle openness and transparency is important for all phases of data lifecycle as this assures the data owners about defined, precise and easy access to information while their personal data is processed. Appropriate technical and administrative measures should be taken during all phases to ensure the same.

Individual participation principle is *relevant* during Capture, Maintenance, Usage, and Publication phases. During the Capture phase, the data owners should be informed about the data that is being collected, the purpose of data collection, how long the data would be maintained by the enterprise, etc. While the data is in the Maintenance phase, the enterprise should ensure that the rights of correcting, updating, and deleting data by data owners are maintained. During Usage and Publication phases, data should be used and published according to the consent provided by the data owner, and it should be ensured that the consent can be updated or revoked at any point in time. During rest of the phases, the direct participation of data owners is not needed; therefore, this principle is not much relevant for those phases.

4.2 Relationship of FIPP Clauses with Privacy Properties

In this section, the FIPP clauses are analyzed with respect to six privacy properties namely confidentiality, integrity, availability, anonymity, unlinkability, and undetectability. As unobservability property is an amalgamation of anonymity and undetectability properties, it is not considered here. The relationship can be binary: either they are related, or they are not related. If a specific privacy property needs to be

Table 2 Relationship between privacy properties and FIPP clauses

	Confidentiality	Integrity	Availability	Anonymity	Unlinkability	Undetectability
Purpose Specification	0	0	1	0	1	1
Data quality and integrity	0	1	0	0	0	0
Collection limitation and data minimization	0	1	0	1	1	1
Use limitation	1	0	1	1	1	1
Security	1	1	1	1	1	1
Accountability and audit	0	1	1	0	0	0
Openness and transparency	0	1	1	0	0	0
Individual participation	1	1	1	1	1	1

protected for implementing a FIPP clause, they are related to each other; if the property does not need protection for implementing a FIPP clause, they are not related. The relationship is shown in Table 2, where 1 indicates that FIPP clause is related to the privacy property and 0 signifies that they are not related.

Purpose specification principle says that the data should not be discoverable for purposes other than the specified ones. Datasets for different purposes should not be linked. These can be achieved by protecting Availability and Undetectability of data items and Unlinkability of datasets belonging to different purposes. Other properties like confidentiality, integrity, and anonymity are irrelevant for this clause.

Data quality and integrity principles can be achieved by ensuring that the Integrity of data items is maintained. Other properties are not important for this clause.

Collection limitation and data minimization can be achieved by protecting Integrity of data items as lesser amount of quality data are better than greater amount of irrelevant data. Anonymity of data owner is also important here as data minimization can be achieved by unlinking the data from its owner. The Undetectability of data items and Unlinkability of datasets among different purposes would help in maintaining minimum data required for various business processes of an enterprise.

For implementing the use limitation principle, access to the data should be restricted even if the data is present within the enterprise information infrastructure. Therefore, Confidentiality is important here, so is Anonymity and Undetectability. Unlinkability among different purposes will also limit the usage of data directly. Availability of data should be restricted making it relevant.

For security of data, all privacy properties of the data item should be protected. Thus, all properties are relevant here.

For accountability and audit, Integrity of data should be maintained such that the quality can be verified at any point in time. Availability is also of utmost importance because the data should be readily available for audit purposes.

For similar reasons, Integrity and Availability are important for the remaining two clauses namely: openness and transparency and individual participation.

The relationships identified in this paper can assist enterprises to plan preventive and corrective measures throughout the journey of private data while in their possession. Though it does not specify what measures are to be taken, it describes when to implement those measures as per the data lifecycle and which privacy properties need to be protected. This analysis can help enterprises in identifying the principles that need to be implemented during different lifecycle phases if they wish to comply with FIPP clauses. It is observed that privacy controls [3–6] can also be decomposed in terms of data lifecycle phases and privacy properties. Given such a decomposed set of controls, this work would help enterprises to choose appropriate controls judiciously.

5 Conclusion and Future Work

The purpose of this study is to identify the privacy properties those need to be protected to comply with all FIPP clauses and also to identify the data lifecycle phases during which the privacy controls need to be implemented such that the clauses of FIPP [2] are fulfilled.

From this study, it is observed that all data lifecycle phases are highly relevant to security clauses and therefore appropriate security controls should always exist. Another important clause is Openness and Transparency which is also important for all phases. There should be transparency to data owners about how their personal data is handled while it is in the data controller's possession. On the other hand, the clause Collection limitation and data minimization is not that relevant for phases other than Capture and Maintenance. Once the data is captured and stored, ensuring Collection limitation is not practical.

It is also observed that for protecting security, all privacy properties of data should be protected while for implementing data quality and integrity clause, only the integrity property is relevant. It is also seen that all privacy properties are important for implementing at least one FIPP clause and each clause needs protection of one or more privacy properties. Though the result of this study cannot directly be used for FIPP compliance by enterprises, it can be a supporting tool toward compliance with FIPP clauses.

As part of future work, privacy controls can be decomposed in a manner such that they can be related to FIPP clauses. Once this is done, an algorithm for selecting appropriate privacy controls for FIPP compliance can be designed. Also, a tool can be developed for verifying whether an enterprise information infrastructure is FIPP compliant.

References

1. IDPL, "The Personal Data Protection Bill, 2019." Available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf. Last Accessed May 2021
2. Fair Information Practice Principles, *Iapp.org*, 2020. (Online). Available: https://iapp.org/resources/article/fair-information-practices/. Last Accessed 04 Nov 2020
3. ISO/IEC 29134:2017: *Information technology—Security techniques—Guidelines for Privacy Impact Assessment*, 1st edn. (ISO/IEC, Switzerland, 2017)
4. ISO/IEC 29151:2017: *Information technology—Security techniques—Code of Practice for Personally Identifiable Information Protection*, 1st edn. (ISO/IEC, Switzerland, 2017)
5. ISO/IEC 27701:2019: *Information Technology—Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management*, 1st edn. (ISO/IEC, Switzerland, 2017)
6. NIST SP 800–53: *Security and Privacy Controls for Federal Information Systems and Organizations*, 4th edn. (NIST, USA, 2013)
7. A. Cavoukian, Privacy by design: The 7 foundational principles. Inf. Priv. Commissioner Ontario Can. **5**, 12 (2009)
8. K.A. Bamberger, D.K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Eurpoe* (The MIT Press, Cambridge, MA, 2015)
9. M. Alshammari, A. Simpson, Personal data management: an abstract personal data lifecycle model, in *International Conference on Business Process Management* (Springer, Cham, 2017), pp. 685–697
10. G.P. Freund, P.B. Fagundes, D.D.J. Macedo, Identification of the relationships between the stages of the data lifecycle and the principles of the Brazilian general data protection act, in ed. by DIONE 2020, LNICST 319 *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering,* pp. 1–10, (2020). https://doi.org/10.1007/978-3-030-50072-6_7
11. Brazilian General Data Protection Law (LGPD), IAPP. Available: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/. Accessed on 4 Nov 2020
12. P. Hernon, Information lifecycle: its place in the management of US government information resources. Gov. Inf. Q **11**(2), 143–170 (1994). https://doi.org/10.1016/0740-624X(94)90002-7
13. M. Chisholm, *Seven Phases of a Data Life Cycle. Information Management*. Available: https://www.informationmanagement.com/news/7-phases-of-a-datalife-cycle. Accessed on 4 Nov 2020
14. S.D. Warren, L.D. Brandeis, The right to privacy. Harvard Law Rev. 193–220 (1890)
15. A. Pfitzmann, M. Köhntopp, Anonymity, unobservability, and pseudonymity—a proposal for terminology, in *Designing privacy enhancing technologies.* (Springer, Berlin, Heidelberg, 2001), pp. 1–9

Mobile Deployed Measurement of RF Man-Made Noise Making Use of RTL-SDR



Lee McQuire, Mohamed Tariq Kahn, and Vipin Balyan

Abstract This paper will examine the feasibility of installing a cost-effective Radio Frequency Man-Made Noise (RF MMN) monitoring station onto public transport. In utilizing public transport, the RF MMN monitoring system can opportunistically collect measurements while moving through a specific area. These measurements will provide valuable data about RF spectrum use over a larger area compared to a single location-based station approach. A model of the RF MMN monitoring station is simulated to optimize the sample rate of measurements, maximize the accuracy and sensitivity of this approach. To optimize the sensitivity, an investigation is conducted on the noise floor generated by the inherent (internal) electronic noise of the system and the vehicle electronics that the system is installed in. A hardware prototype was designed to demonstrate the feasibility of the system and a pilot test run was conducted, and the measurement is plotted on a scatter plot map. The recorded measurements serve as a tool for analyzing RF MMN over the geographic area in which public transport frequently travels. The RF MMN measurement system will contribute to enhancing traditional Man-Made noise databases with the sensors moving around through public vehicles. This will assist in identifying the primary, secondary, and illegal users, confirm spectrum database accuracy, and will assist in refining current propagation models within the RF band in which the samples were measured. The RF MMN monitoring system is possibly the new "eyes and ears" of the regulatory body to actively monitor spectrum use.

Keywords Software defined radio · Interference mapping · Spectrum occupancy measurement · Radio frequency man-made noise

L. McQuire (✉) · M. T. Kahn · V. Balyan
Department of Electrical, Electronics and Computer Engineering, Cape Peninsula University of Technology, Cape Town, South Africa

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_83

1 Introduction

"Indeed, the gap between wireless supply and demands widens. It is feared that an imminent spectrum crisis, in which exploding demand from smartphones will soon overwhelm the wireless capacity, will occur. The problem is the lack of a new spectrum available to wireless data carriers. Smartphone data traffic is growing so fast that if nothing is done, they will use up the available spectrum. This just affects not only smartphones but also all wireless devices. A huge amount of spectrum is required for broadband use in the future as suggested in the National Broadband Plan (NBP) in the USA and the digital agenda in Europe" [1].

In recent years, there has been an upsurge in portable wireless devices, increasing demand for wireless data, higher transmission rates, and the ever-increasing use of electromagnetic radio frequency (RF) spectrum [2]. With the uptake of technologies such as 5G, self-driving cars, LTE-M, and NB-IoT (Internet of Things), more and more devices are connecting wirelessly to the internet. This has led to a scarcity of spectrum resources, therefore, to actively monitor RF spectrum use and optimize current usage models, this paper presents a unique cost-effective approach to conduct spectrum monitoring [3].

Spectrum monitoring has an underlying function where spectrum usage or RF MMN are measured and recorded. This RF MMN measurement data can be used to identify vacant frequencies, prompt investigation when signals are present on unassigned channels, and help with the planning for allocation of additional bands or assist with the re-assignment of existing bands. RF MMN measurements are conducted by using specialized equipment that is normally found in dedicated measuring sites which are built in a wide array of areas to create a nationwide RF monitoring system. However, commercially available RF monitoring systems are relatively expensive to build and have a very limited coverage area which leads to ineffective RF spectrum monitoring.

This paper presents a feasibility study to create a low-cost RF MMN monitoring system that is portable and has the flexibility to be installed on any vehicle (see Fig. 1). This can lead to a very cost-effective means of acquiring RF MMN data, especially when the measurement system is installed in existing public transport systems. As public transport moves, the RF MMN data can opportunistically be collected. The main advantage of the system would be that the RF MMN measurement can be measured more frequently, in areas where it was previously not feasible and at a fraction of the cost compared to existing commercial systems.

2 RF MMN Monitoring System Design

Careful consideration was taken in the selection of equipment to obtain accurate and meaningful results, to increase the capability to detect the measured signal in the frequency band of interest, and to reduce the noise floor created by the internal

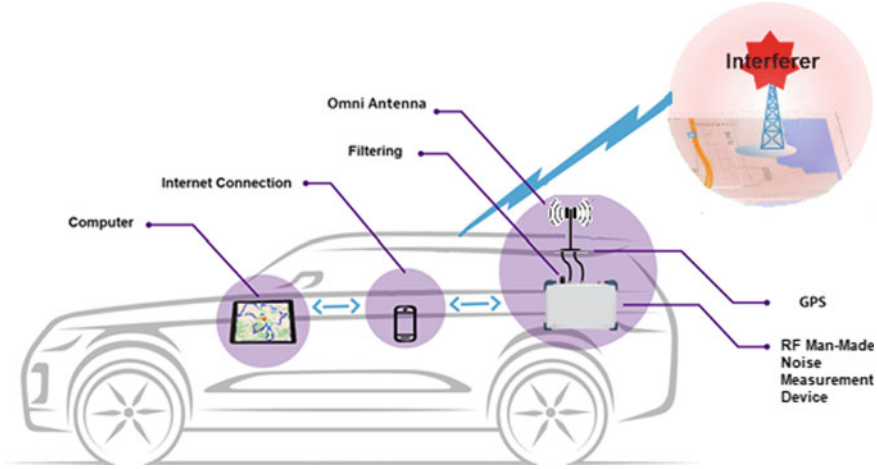


Fig. 1 Conceptual installation of the RF MMN monitoring system in a vehicle

circuit. Special considerations need to be made as the MMN monitoring system must have the capability to be installed in several public vehicles, this poses extra security, RF noise floor, and accessibility issues. Since long continuous recordings, mobility, and flexible designs are desired, a reconfigurable RTL-SDR is connected to a computer or a microcontroller. An appropriate setup for a single measurement device consists of an SDR as well as supporting components such as filters, LNA (Low Noise Amplifier), and attenuators, which are used to adapt the dynamic range of the signals, increase sensitivity, and prevent overload (see Fig. 2). To keep the cost

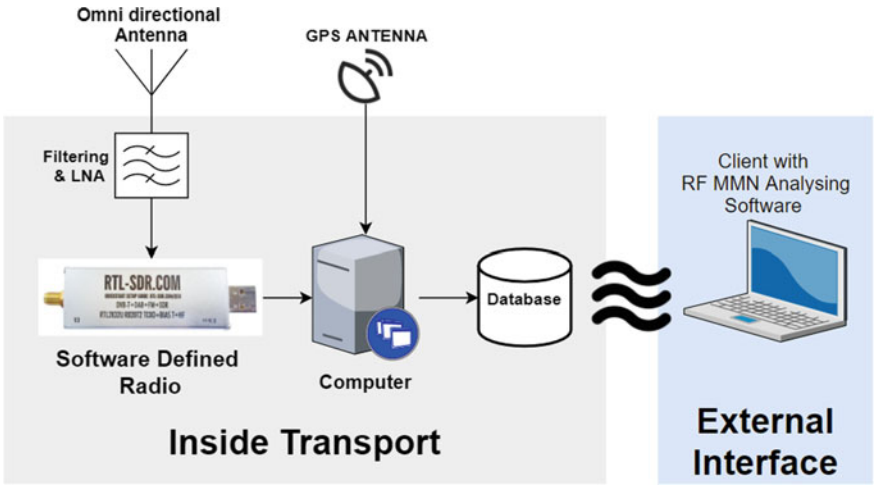


Fig. 2 Conceptual design of the RF MMN monitoring system

down existing readily available commercial consumer-based products are discussed in the build of the prototype.

The antenna is mounted on the highest point on the vehicle that receives the radio frequency from the external environment. This signal is fed via feeders to the RTL-SDR. The SDR's open RF front end can create harmonics within the equipment and this can cause ghost signals which will give faulty measurements [4]. A bandpass RF filter and LNA are fitted at the front end. This will reduce the RTL-SDR image effect, reduce radio interference, improve the signal to noise ratio, and amplifier assists in reducing the systems Noise Figure (NF). RTL-SDR is used as an inexpensive radio receiver that converts the received radio power into a digital signal called I/Q data that is needed for the RF MMN monitoring. The GPS is used to receive location data in form of longitude, latitude, altitude, standard time, date, speed, and altitude that can be used to correlate the I/Q data to a specific time and location. The output data of the RTL-SDR and GPS are processed, recorded, and manipulated by a computer. The complete system gets its power from the vehicle which is installed in. To cut down on costs, only off-the-shelf components are used, and the price of the complete system is highly dependent on frequency measured, type of SDR, filter needed, computer, storage allocation, power supply type of installation, and extras that are used.

3 Optimization of RF MMN Monitoring Results

3.1 Identifying the Effects of Inherent and Transportation RF Noise

All active electrical systems create their own internal (Inherent) noise RF noise. The intensity of inherent RF noise is dependent on the quality of the design and components used in the system [5]. RF MMN monitoring system is designed by making use of consumer-based products which quality can vary widely and thus needs to be compensated for. This internal noise can influence the noise floor of our monitoring system and lead to false readings and errors. For this reason, the noise floor parameters need to be calculated and simulated to improve overall performance, help to avoid or cancel out error as much as possible. Due to the design of the RTL-SDR dongle, there will always be spurious (unwanted) signal noise spikes at multiples of 28.8 MHz, the frequency of the internal oscillator, and strong spurs at multiples of the USB clock frequencies (48 MHz). At a bandwidth of 0.25 and 1 MHz, there are images of strong signals at every 250 kHz and 1 MHz [6]. There is unfortunately not much that can be done about this other than to know where they are and to compensate for this.

Secondly, unwanted external environmental noise can also be induced and influence the results. This external noise can come from anything, e.g., controlling computer, power supply, the transports vehicle electronics to any other source of noise or unwanted signal, etc. This will influence the noise floor and can cause undesirable

measurement results. This external unwanted interference must also be determined and needs to be minimized in the most cost-effective way for data integrity thus it's suggested that a calibration process might be implemented to mitigate these issues by pre-recording the noise generated and using this information for future analysis.

When conducting a spectrum sweep in the desired measurement frequency band of interest the internal and external noise can be established. To test the environmental noise of the RTL-SDR the dongle is placed into the transport vehicle. Emphasis must be taken that the transport vehicle must be switched on so that the vehicle noise generated by the electronics and engine can be measured. The RTL-SDR is thus directly plugged into the USB port of the laptop. The RTL-SDR is connected to an external Omni antenna inside the vehicle. Preferably the antenna connected must not have a cable run as this allows noise picked up by the cable run. With a successful run, MATLAB provides the spectrum sweep between the selected frequencies and creates a CSV file containing all the outputs of the sweep (see Fig. 3). Careful consideration is to be taken which noise floor environment the initial calibration of the noise floor is conducted as this can influence the test result.

An investigation was conducted, and it was determined that the inherent noise did create false reading and is greatly affected by the amount of internal gain that is used in the RTL-SDR. The installation vehicle also created a noise floor that changed per vehicle type and was also dependent on where in the vehicle the RF MMN monitoring system was installed. The power source that is used to power the RF MMN monitoring system also created its noise as most are based on switch mode power supplies. Much needs to be done to isolate the receiver antenna and RTL-SDR from electronics in proximity. These electronics can greatly influence measurement quality, accuracy, and reliability. These noise floor figures can be used to increase the accuracy in measurement by creating a 10dBm guard band between the measured noise floor and actual recordings [7]. This will significantly decrease the probability

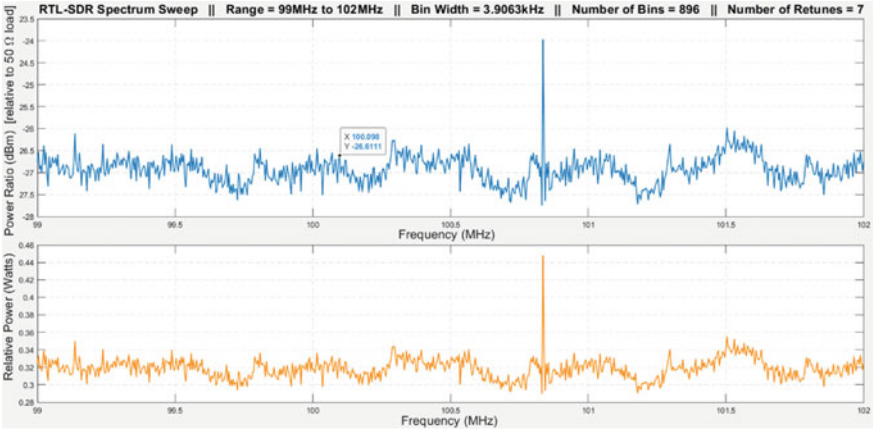


Fig. 3 RF MMN internal noise combined with RF interference created by vehicle spectrum plot for the FM band spanning from 99 to 102 MHz

of false readings. Also, this noise floor reading can be used to decrease data storage as only reading above the noise floor will be recorded.

3.2 Selective Sampling

As the RF MMN monitoring system is active, the system will be receiving frequency, signal strength, time, and GPS coordinate data. For the most accurate results, a signal strength measurement is continuously taken for each sample for all possible locations, time, and frequency but there are practical limitations to this. To be more practical, a sample is taken as a reflection of the actual data. The sampling requirement is dependent on the objective of the measurement and is limited to maintaining a manageable amount of recorded data. The sampling needs to be taken at a known distance between measurements to be able to sufficiently approximate the relationship between distance and variance. The RF MMN monitoring system is intended to be installed in public transport vehicles. This creates extra challenges when it comes to sampling. As the transport vehicle drives at varying speeds and stops frequently, this can lead to the RF MMN monitoring station collecting data heterogeneously in density. Therefore, to bypass this issue and save data storage costs, it was determined the best approach would be to use a spatial method of sampling. In spatial domain sampling measurement, the location of the transmitter and coverage is not known, this makes it perfect in monitoring MMN. By using the Spatial sampling method, a pre-determined physical distance between samples recorded can be maintained making it much easier to represent the recorded occupancy data on an RF occupancy coverage map. By using this spatial method, no unnecessary data will be recorded on a specific location, and only vital information that the operator needs are recorded. The spatial domain resolution is determined to adequately record data not to lose essential information by keeping the data amount and scanning speed to a reasonable level.

The GPS receiver will be providing the GPS coordinates. The coordinates will be used to calculate the distance traveled between points. Two of the most common methods for calculating the distance between two coordinates on the earth's surface are the Haversine formula and Euclidean distance.

Haversine [8] as a formula calculates the distance of a circle between longitude and latitude points assuming the radius of the earth R is 6367.45 km, the location of the two points in a spherical coordinate. Ignoring the structure of the earth's surface (hills and valleys) is very accurate for most calculations because the ellipsoidal effect is eliminated.

$$D = 2r \arcsin\left(\sqrt{\sin^2\left(\frac{\theta_2 - \theta_1}{2}\right) + \cos(\theta_1) \cdot \cos(\theta_1) \cdot \sin^2\left(\frac{\lambda_2 - \lambda_1}{2}\right)}\right) \quad (1)$$

where refers to D is the distance (km), radius $r = 6371$ km, $\lambda =$ longitude and $\theta =$ latitude.

Euclidean method [9] is where the distance is calculated from two points is based on the Pythagorean Theorem. The Euclidean distance is an empirical function based on the direct distance between two free space obstacles. The value of the length of the diagonal line on the triangle.

$$D = \sqrt{((\theta_1 - \theta_2)^2 + (\lambda_1 - \lambda_2)^2)} \tag{2}$$

where $D =$ Euclidean distance in degrees, $\theta =$ latitude and $\lambda =$ longitude of the locations.

The distance D in degrees is converted into kilometers by multiplying D by 111 319 km (1 degree).

Results of distance measurements between the Euclidean method and the Haversine Formula has a percentage ratio of the distance between the two methods of 99.89% [10]. Thus, based on the above information Euclidean method is fit for our purpose. By calculating the distance between coordinates samples can be taken as set distances. For our purpose, it was determined that the Euclidean method will serve our purpose and needs the least amount of processing power.

4 Measurement Data Collection Results

A pilot test drive on an FM radio station was conducted in Malmesbury, South Africa. MATLAB Simulink was the software environment used to conduct the pilot test on 10 December 2020. The MMN system was operational, collecting, and recording RF signal strength and GPS coordinates. In the noise floor test, the inherent noise and the vehicle electronics noise were recorded. In this test, the vehicle ignition was switched on, with the air conditioner, lights, and radio "ON" to make sure all RF noise that may occur within the vehicle is considered. On the frequency, 100.1 MHz a noise floor measurement of −26.6 dBm (0.33 watts) was recorded. Recordings were collected within and below this noise floor. To increase the measurement accuracy only the measurements that are 5 dBm above the equipment noise floor will be plotted, this will significantly reduce the odds of getting phantom occupancy measurements. The new measurement threshold is calculated at −21.6 dBm. By only considering measurements above this threshold noise there was a 31% reduction in data storage needs. The information that was recorded was plotted on an interference map within MATLAB see Fig. 4. In the findings, it was found that this monitored radio station transmitted much further compared to the plot on its broadcasting license. The recorded coverage was about 35% more than plotted on the license. This pilot test confirmed that spectrum use needs to be frequently tested and reinforces the need for this type of low-cost monitoring.

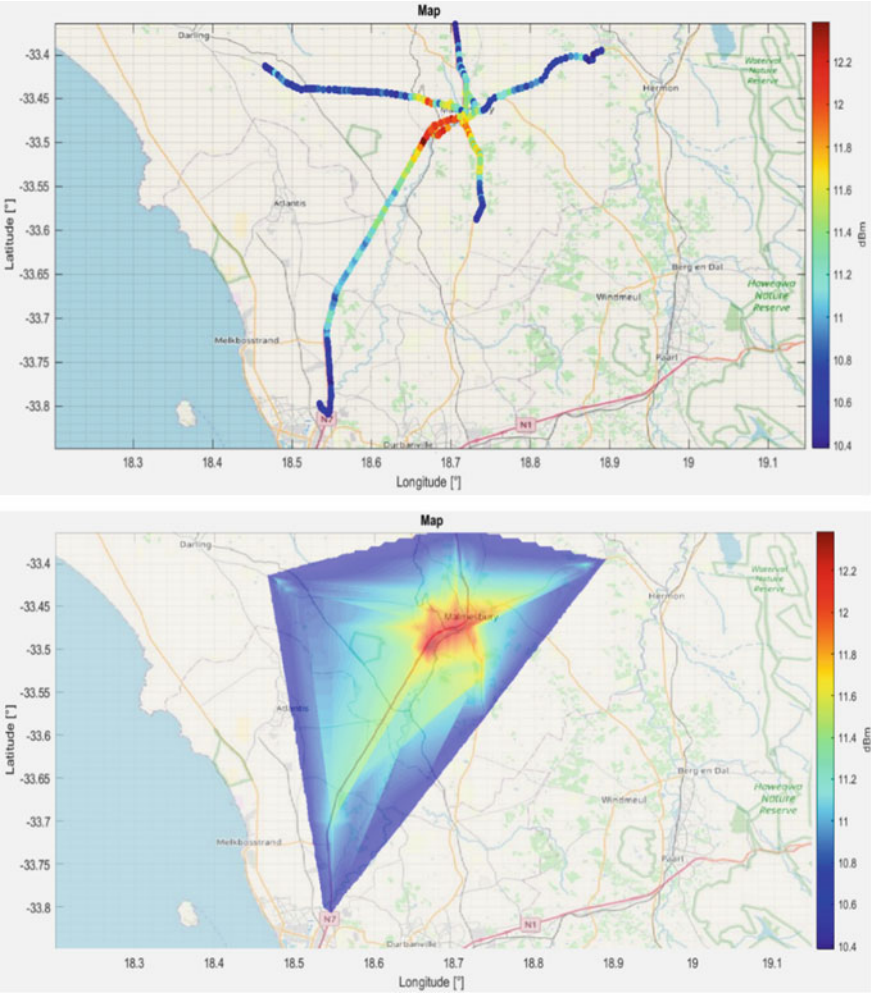


Fig. 4 (**Top**) The plot of test results scatter map and (**Below**) predicted signal strength map using natural neighbor interpolation

5 Conclusions

This paper presented an overview and challenges of creating a Mobile deployed cost-effective design for the measurement of RF MMN with emphasis on implementation in public transport.

In obtaining the four key capabilities such as being cost-effective, portable, using spatial sampling, and being able to adapt to installation noise floor levels, the RF MMN monitoring system has the potential of being a disruptive force within spectrum monitoring and management. By using the RTL-SDR for the implementation of RF

MMN monitoring provides a cost-effective solution and offers improved flexibility to overall spectrum monitoring. The RF MMN monitoring system can exploit the spectrum holes or white spaces of licensed spectrum bands provided, assist in finding non-compliant license holders, and significantly improve the efficiency of spectrum usage.

In the design, the challenges remain numerous, namely, dealing with the noise floor, receiver sensitivity, multipath fading, and shadowing. All the objectives were achieved in design- and building a mobile deployed RF MMN monitoring system that was cost-effective, is relatively small, and portable enough to be used in any vehicle. Successfully simulated and measured the RF noise generated by the RF MMN monitoring system and the installation vehicles. We mitigated data storage overhead by making use of spatial sampling and completed the pilot test and analyzed the data collected.

The RF MMN measurement system can contribute to enhancing traditional Man-Made noise databases with the sensors moving around within public vehicles. This will assist in identifying the primary, secondary, and illegal users in the band in which the samples were measured, spectrum database accuracy confirmation, and will assist in refining current propagation models.

Acknowledgments The authors gratefully acknowledge funding by Cape Peninsula University of Technology (CPUT) and the support of staff.

References

1. Y. Arjoune, N. Kaabouch, A comprehensive survey on spectrum sensing in cognitive radio networks: recent advances, new challenges, and future research directions. Sensors (Switzerland). 19(1) (2019). https://doi.org/10.3390/s19010126
2. F. Salahdine, H. El Ghazi, A real time spectrum scanning technique based on compressive sensing for cognitive radio networks, in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference UEMCON 2017*. (2018), pp. 506–511. https://doi.org/10.1109/UEMCON.2017.8249008
3. H.A. Cook, M.T.E. Kahn, V. Balyan, Radio direction-finding techniques for an unmanned aerial vehicle. Micro-Electron. Telecommun. Eng. (2020)
4. P. Collier, RTL2832 Software Defined Radio. AB9IL. https://www.ab9il.net/software-defined-radio/rtl2832-sdr.html. Published 2017. Accessed 27 Oct 2020.
5. R. Aguilar-Gonzalez, A. Prieto-Guerrero, V. Ramos, E. Santos-Luna, Lopez- M. Benitez, A comparative study of RTL-SDR dongles from the perspective of the final consumer. *Dig Tech Pap—International Conference on Consumer Electronics* 2020 (January). https://doi.org/10.1109/ICCE46568.2020.9043161
6. C. Laufer, The hobbyist's guide to RTL_SDR: really cheap software defined radio. 5 (2017)
7. M.I. Skolnik, Introduction to radar systems Second Edition-uda. *Gard City Mov Up-To-Date* (2019)
8. M. Basyir, M. Nasir, S. Suryati, W. Mellyssa, Determination of nearest emergency service office using Haversine formula based on android platform. Emit Int J Eng Technol. (2018). https://doi.org/10.24003/emitter.v5i2.220
9. R. Pramudita, F.I. Hariadi, Development of techniques to determine object shifts for PCB board assembly automatic optical inspection (AOI), in *ISESD 2018—International Symposium on*

Electronics and Smart Devices: Smart Devices for Big Data Analytic and Machine Learning (2019). https://doi.org/10.1109/ISESD.2018.8605458

10. E. Maria, E.H. Budiman, M. Taruk, Measure distance locating nearest public facilities using Haversine and euclidean methods. J. Phys. Conf. Ser. **1450**(1) (2020). https://doi.org/10.1088/1742-6596/1450/1/012080

Use of Blockchain Technology in Agriculture Domain



Nisha N. Kamble, Shankar M. Mali, and C. H. Patil

Abstract Blockchain is an emerging technology, nowadays looked at it as a solution for most of the security issues of any system. It is a breakthrough to the traditional way of developing the applications which provides robust features in security, sharing the information, and immutability. Blockchain is digital ledger, and every transaction is considered as one record. This data is stored in encrypted format, and the series of records are linked in such a way that any tampering of the data is close to impossible. This literature study is focusing on the usage of blockchain in agriculture domain in supply chain. Researchers have provided various innovative solutions to improve on traceability in supply chain of food, fruit, vegetables, and seeds. The study of literatures helps to understand the new technical concepts that make blockchain as an effective solution, for e.g., BigchainDB to avoid decentralized database issues, use of activation key for authorization, and combination of blockchain and SQL database to improve the performance and efficiency. It is also observed that the combination of IoT with blockchain will bring error-free data entry and easy to use it improving traceability in the supply chain. This paper aims to understand all these concepts from various studies.

Keywords Blockchain · Smart contract · Transparency · Seed · Agriculture · Supply chain

1 Introduction

Industry 4.0 is embracing the blockchain technology in almost all domain. This literature study is focusing on the usage of blockchain technology in agriculture domain. Agriculture is backbone of the Indian economy, and it contributes 17%

N. N. Kamble (✉) · S. M. Mali · C. H. Patil
Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

S. M. Mali
e-mail: shankar.mali@mitwpu.edu.in

C. H. Patil
e-mail: chandrashekhar.patil@mitwpu.edu.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_84

of the total gross domestic product (GDP) [1]. Farmers should be equipped with good tools for better quality crop production. This directly impacts on the health so needs to be taken with great important and highest priority. Seed is one of the basic inputs for the farming, and quality of the crop depends on it [2]. Blockchain is the revolutionary technology to provide clear tracking of the food to buyer or user like the farm production date, packaging date, who is seller, buyer. Many industries and organizations are involved in supply chain in agriculture. Following key features of blockchain technology brings improvement in terms of transparency and security in the end-to-end life cycle in supply chain.

- Immutability—it means, it cannot be altered or changed once the record is inserted in the system. Every block in blockchain is stored in hash value and has linking of the records using this hash value. Hence, there is less chances of tampering the data.
- Transparency—blockchain is digital ledger, and all records are stored with appropriate details and can be traceable for each modification.
- Smart contract—it is a set of rules or small programs which can be hosted in blockchain. It communicates or helps in small programmatical execution across the supply chain participants.
- Security—blockchain is a decentralized database; hence, there is no fear or loss of the data or availability of the data. There is no chance of adding any corrupted data due to consensus methodology that executes while adding each new block in blockchain.

In India, farmers are still facing the issues with quality of the seeds. The government of India has established law and regulation to avoid such issues. Unfortunately, despite of law and regulation, the issue retained [3].

Following are the key problems observed after study of the existing system [4].

- Deprived information sharing across the department—The supply chain of a seed is long-time process, involving various organization. The data sharing is not good across the organizations during end-to-end life cycle of the seeds. This leads to raise a question of trust in data.
- Centralized supply chain that can easily tampered—The supply chain data is a centralized system; hence, there is possibility of manipulating the data or data loss.
- No traceability of seeds life cycle—There is no single identity maintained for a seed throughout its life cycle; hence, there is no authorized traceability.

The remaining paper below is organized in various sections to reflect the various existing literature reviews of blockchain technology in agriculture domain. Section 2 explains the summary of reviewed papers to explain how blockchain can think of solution in food, fruit, and seeds supply chain. Section 3 states the observations. Section 4 shows the comparative study of these papers in terms of key features considered in their paper and proposed solutions and limitations. Section 5 is to explain the conclusions.

2 Literature Review

Blockchain technology can be implemented effectively to bring improvement in the supply chain specially for the security and transparency. Following section gives the brief review of usage of blockchain in agriculture domain.

Zhang et al. [4] aimed to build a grain supply chain information management solution based on blockchain technology for traceability, performance, and security. A cloud-based four-layered information management system architecture is proposed using five typical links in grain supply chain: production, storage, processing, logistics and transportation, and marketing. Sensors are proposed for the data collection to avoid human errors. This is a complete solution.

Salah et al. [5] have done a detailed study of the current system of supply chain soybean from farmer to port and proposing solution using blockchain technology to improve for high level of transparency and traceability by storing all transactions in the blockchain's immutable ledger with links to decentralized file and utilization of smart contracts to govern and control all interactions and transactions among all the participants. This is a complete design solution including the entity relationship diagram, sequence diagram, and implementation framework for the blockchain application.

Yadav and Singh [6] have provided blockchain-based mobile app to resolve the key issues of an Indian farmer; quality of seeds, certification of quality produce, disbursement of subsides, and minimum support price. The mobile app is further categorized into three modules, namely traceability, smart contract-based monitoring, and informative system. This paper does not give more details for the implementation approach or framework. But, the analysis of the issues is based on literature review on the similar topic and Delphi technique.

Caro et al. [7] provided details of a system, named AgriBlockIoT. This is a decentralized, blockchain-based traceability solution for food supply chain management. Proposed layered architecture along with algorithm and detailed design is a solution for a classic use case named from-farm-to-fork using two different types of blockchain implementation Ethereum and Hyperledger Sawtooth for the traceability in the food supply chain. Both are deployed and then evaluated for the performance and security aspects. The detailed reports of pros and cons of each are highlighted.

Kamble et al. [8] studies are helping the practitioners to design the strategies for blockchain technology implementation in agriculture, creating a real-time data-driven agriculture supply chain. Thirteen enablers are identified in this study to implement in agriculture blockchain-based solution in supply chain as traceability, immutability, provenance, auditability, risk management, transparency, anonymity and privacy, low transaction costs, low settlement lead time, smart contract, decentralized database, secured database, and shared database.

Tian [9] is proposing a concept named as "BigchainDB" introduced to fix the issues of decentralized database. This is more to improve the efficiency, traceability, and salability in the supply chain of food based on hazard analysis and critical control points (HACCP), blockchain, and Internet of Things. The list of hazards

with its control measures, monitoring, and corrective actions are discussed in detail. The comparison of blockchain vs distributed DB vs BigChainDB for the key features is provided in which BigchainDB has advantages, high throughput, low latency, and high capacity.

Revathy and Priya [10] are providing a blockchain-based solution to bring transparency in producer and consumer transactions. The blockchain-based producer–consumer model is to allow farmers to connect with consumer directly and avoids connection of consumer to consumer. This is effective model over the traditional model of producer to consumer. All farmers and consumers will link in the blockchain, and solution performs transaction in standard steps, i.e., creation of block, broadcasting of block, validation, consensus, and then adding the block in blockchain.

Abdulhussein et al. [11] are grabbing the attention for the design to improve the traceability in supply chain using blockchain-based solution. The solution is mainly focusing on avoiding unauthorized access and data to be added in transactions. The system worked based on the activation key, which needs to be validated by client/user, and data will be added by authorized users. The activation key plays an important role which is generated based on the Base64 encryption algorithm. It provides overview of various other techniques to bring the traceability like RFID, use of IoT, and QR code.

Yang et al. [12] come up with very unique concept of an application with blockchain and database for the traceability of fruits and vegetables. This is very efficient system to reduce the load on blockchain for storing the huge data during each transaction of supply chain. The entire transaction is stored in blockchain, and the public data is stored in database. However, avoiding human manipulation each time and the public data from database, it gets compared with blockchain public data, and if comparison is passed means, there is no tampering in this data. The public information is available in QR code so that any user can easily scan and read the details. All data stored in blockchain is in hash value using SHA256 algorithm. The proposed system is using. Net technology using MVC design pattern and MySQL, hence, will not be complex in implementation. Efficiency of the system is maintained along with traceability and security with the concept of chain-on and chain-off.

3 Observation

It is observed that all studies and research are oriented to use of blockchain technology to bring transparency and security in the existing way of working in supply chain.

Above two diagram show change from traditional way of supply chain connections, and the next is the proposed way of supply chain using blockchain. The first diagram is a traditional operating way in which all participants work in isolation and pass the information to next level. Data sharing and transparency of the data are low here. Proposed solution is system using blockchain technology that connects each participants/organization for the traceability in end-to-end life cycle of the seed in

supply chain. All the information is proposed to store in decentralized and accessible to each participant at any time. The immutability, data storing across the participants, and accessibility of authenticate data of seed throughout the life cycle are possible (Fig. 1).

Most of the literatures are concluding on the similar type of blockchain-based solution over the traditional supply chain method (Fig. 2).

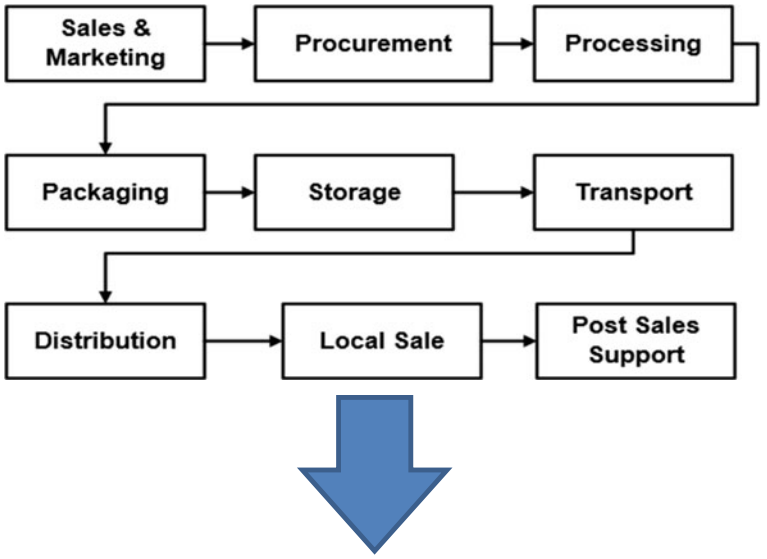


Fig. 1 Traditional supply chain participant and connections

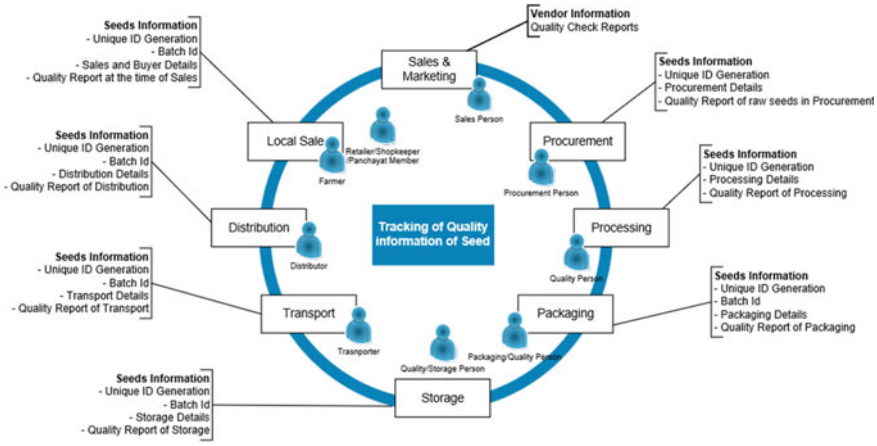


Fig. 2 Blockchain-based supply chain for seeds

4 Comparative Analysis

Table 1 shows the comparison of papers based on the key focus on the blockchain feature, solution proposed, opportunities, and limitations.

Table 1 Comparative study of reviewed papers

References	Authors	Year	Solution	Features	Limitations
1	X. Zhang et al.	2020	Four-layered cloud-based solution	Traceability, performance, and security	No use of IoT to avoid human error
2	K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar	2019	Ethereum and smart contract-based complete design solution	Smart contract, immutability, and transparency	Payment delivery is not automated
4	Vinay Surendra Yadav and A. R. Singh	2019	Mobile app-based solution	Traceability	Limited issues are in focus for the solution
5	M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda	2018	Ethereum and Hyperledger Sawtooth	Traceability	Focus on enhanced performance analysis
6	Sachin S. Kamble, Angappa Gunasekaran, and Rohit Sharma	2019	Blockchain-based system solution	Thirteen enablers, traceability, decentralized database, etc.	Analysis is only from India and needs wider analysis approach
7	Feng Tian	2021	Blockchain-based solution using IoT and BigchainDB	Decentralized database	Traceability can be improved using IoT
8	S.Revathy, S.Sathya Priya	2020	Blockchain-based producer–consumer model	Transparency	Performance and efficiency are not in focus
9	A. B. Abdulhussein, A. K. Hadi, and M. Ilyas	2020	A blockchain solution using activation key, Base64 encryption algorithm	Transparency	Performance improvements
10	X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun	2021	MVC framework-based. Net solution with dual-storage blockchain and database	Traceability, efficiency, and decentralized database	Cross-chain technology and enhanced consensus mechanism

5 Conclusion

Various studies and proposed designs in their research indicate that blockchain is the future for supply chain to improve on traceability, security, and availability aspects of the transactional data. Blockchain concept can be more effective by using Internet of Things like RFID, QR, and sensors for reading the data. The tampering of the data can be avoided by using decentralized database of blockchain and storing data in encrypted format which cannot be modified so that the once the record is inserted, then it is immutable. Various validation techniques also proposed to authorize the data while inserting, i.e., using activation keys, consensus. Complexity in implementation of blockchain-based application can be reduced since this concept is flexible to implement in any known technology, i.e., Microsoft.Net, Ethereum, and Java.

Agriculture domain is one of the key areas since it deals with food. And, food is directly linked with health. There are various open concerns in food supply chain for the traceability of origin to end user. Blockchain is bringing a positive hope to reduce current issues in supply chain, especially in agriculture domain.

References

1. G.S. Nagaraja, A.B. Soppimath, T. Soumya, A. Abhinith, IoT based smart agriculture management system. 2019 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS), (2019), pp. 1–5. https://doi.org/10.1109/CSITSS47250.2019.9031025
2. https://vikaspedia.in/agriculture/agri-inputs/seeds/seed-quality
3. https://seednet.gov.in/PDFFILES/National%20Seed%20Plan.pdf
4. X. Zhang et al., Blockchain-based safety management system for the grain supply chain. IEEE Access **8**, 36398–36410 (2020). https://doi.org/10.1109/ACCESS.2020.2975415
5. K. Salah, N. Nizamuddin, R. Jayaraman, M. Omar, Blockchain-based soy-bean traceability in agricultural supply chain. IEEE Access **7**, 73295–73305 (2019). https://doi.org/10.1109/ACCESS.2019.2918000
6. V.S. Yadav, A.R. Singh , Use of blockchain to solve select issues of Indian farmers, in Proceedings of the AIP Conference, vol. 2148 (2019), p. 030050. https://doi.org/10.1063/1.5123972
7. M.P. Caro, M.S. Ali, M. Vecchio, R. Giaffreda, Blockchain-based traceability in agri-food supply chain management: a practical implementation. IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany) **2018**, 1–4 (2018). https://doi.org/10.1109/IOT-TUSCANY.2018.8373021
8. S.S. Kamble, A. Gunasekaran, R. Sharma, Modeling the block-chain enabled traceability in agriculture supply chain. Int. J. In-form. Manag. **52**, 101967 (2020). ISSN 0268-4012. https://doi.org/10.1016/j.ijinfomgt.2019.05.023
9. F. Tian, A supply chain traceability system for food safety based on HACCP, blockchain and Internet of things. Int. Conf. Serv Syst. Serv Manag **2017**, 1–6 (2017). https://doi.org/10.1109/ICSSSM.2017.7996119
10. S. Revathy, S.S. Priya, Blockchain based Producer-Consumer Model for Farmers. 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), (2020), pp. 1–5. https://doi.org/10.1109/ICCCSP49186.2020.9315214
11. A.B. Abdulhussein, A.K. Hadi and M. Ilyas, Design a tracing system for a seed supply chain based on blockchain, 2020 3rd International Conference on Engineering Technology and its

Applications (IICETA), (2020), pp. 209–214. https://doi.org/10.1109/IICETA50496.2020.9318792

12. X. Yang, M. Li, H. Yu, M. Wang, D. Xu, C. Sun, A trusted blockchain-based traceability system for fruit and vegetable agricultural products. IEEE Access **9**, 36282–36293 (2021). https://doi.org/10.1109/ACCESS.2021.3062845

Analysis of Impedance Matching Technique on Broadband Powerline Communication Network Topologies



D. Smitha Gayathri and K. R. Usha Rani

Abstract The paper presents a new design of creating a household powerline model with parameters provided in random. The actual parameters on the powerline communication are approximately calculated with required accuracy. The previous and present studies in modelling of powerline communication are explained briefly in this paper. The transmission line variables are measured and verified with powerline modelling. Powerlines are basically varied from telephone lines in terms of topology and impedance of the loading. In this, ABCD parameters of the separate modules are used to study the powerline channel which consists of 10 bridge taps with overall distance of 600 m length. Among the noise profiles, periodic impulse noise is included as it is the primary among the noises present in powerline communication aside of AWGN. The **impulsive noise** is described as a high **PSD** that reaches more than 50 dB than the background **noise**. Discrete multi-tone transmission (DMT) is applied in VDSL2 with bandwidth of over 30 MHz in order to get the profiles of tone loading. This leads to the fact in order to achieve rates of conventional VDSL2, lower transmit PSD is sufficient with open bridge taps. But, due to the inductive loads in the residential areas, we need to (1) use the existing VDSL2 setup with adjustable impedances in the front-end so that the load impedance can be matched conjugate and (2) ability to increase transmit PSD and to further increase the sub-bands in order to achieve the required rates smoothly like VDSL2.

Keywords Discrete wavelet transform (DWT) channel modelling · SVD · Discrete multi-tone · AWGN · Powerline communications (PLC)

D. S. Gayathri (✉)
ECE Department, DonBosco Institute of Technology, Bengaluru 560074, India

K. R. U. Rani
ECE Department, RVCE, Bengaluru 560059, India
e-mail: usharani@rvce.edu.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_85

1 Introduction

In the previous works, the capacity of channel is determined using adaptive bit loading using SNR profile of various powerline communication topologies including impulse and AWGN noises which is maximum in the powerlines. The generation of the impulse noise signals was studied. In this, the phenomenon of connecting the bridge taps with loads is studied in detail. The combination of the inductive loads and the impulsive noise presence is studied, and consequences of it on the SNR are also determined. A conclusion that enhances the SNR sufficiently is recommended and illustrated in this work. The electric apparatus that works on the same network produces noises which are impulsive cyclo-stationary or stationary. Out of all of the above-mentioned types, impulse noise is the root cause of interference which leads to the distortions in the communication signals and causes errors during transmission of data packages. This is caused by the transients generated due to switching of electric appliances and power supplies. In equipment, for example cooling and heating apparatus, the transients is caused by switching as well as internal control of thermostatics. The transfer function of powerline network is modified due to the sudden switching of the loads which leads to more losses and reduces the transmission rates. In this, impedance mismatch is studied with connecting the conjugate impedances and thereby studying the developments in capacity of the transmission line and SNR capacity (Fig. 1).

The effect of adding the impulse noise and mismatched impedance on the powerline communication channel is studied. The capacity of the communication channel is reduced by the mismatched impedance, and impulse noise for single inductive-loaded BT and the SNR reduces with increasing BTs. A limit is set on the rate of data transmission less than that of the capacity of the power transmission line. Also, the inclusion of matching impedances is also analysed along with increase in signal PSD. The consequences of the inductive loads in powerline transmission are studied in this paper, the point of reduction in SNR with inclusion of the inductive load is inscribed with impedances matched, and the consequences of impulse noise and inductive load in the power transmission line for the test case scenarios are provided with results and a study with a strategy to reduce the consequences of reduction in SNR.

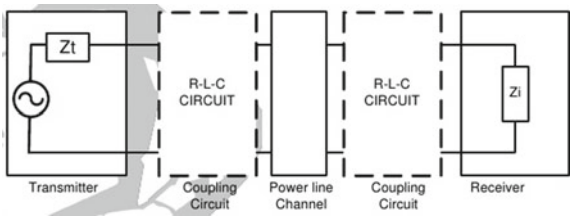


Fig. 1 PLC architecture

1.1 Discrete Multi-tone Modulation

The discrete multi-tone (DMT) modulation is a scheme of multi-carrier modulation techniques with active bit loading for powerline transmission sub-channels and yields a sturdy transmission strategy against reflections due to multiple paths, interference due to radio frequency and impulse noise because of domestic equipment in a power line transmission network. DMT basically splits a powerline communication channel into a various bands of frequencies with equal space [1]. In every band, a part of the information signal is transmitted in a subcarrier. This is done by assigning various number of information signal bits to various sub-channels according to the individual SNR rates for better data transmission. A tone having more SNR carries more number of bits than that of tones having lesser SNR. It is used in digital subscriber line (DSL), which is a sturdy, flexible, and not difficult to use multiple vendor access for high speed, low-cost data transmission networks. DSL simultaneously directs to a bunch of technologies which uses the unconsumed bandwidth in the existing network in order to provide services on high-speed data transmission from the distribution centre to user with bandwidth of 30 MHz, and rate of a data with maximum of 100 Mbps is done with this higher bandwidth on the transmission wire line. There are various variants of available technologies of DSL, which are influenced by location and bandwidth requirements [2, 3]. There are two types of DSL technologies available, whose standards have improved.

1. ADSL/ADSL2 + : It provides two different operating speeds of data transmission [4] with downstream (distribution centre to user) speed higher than that of upstream (user to distribution centre) speed. It can provide 1–8 Mbps in downstream data transmission where ADSL2 + provides maximum data transmission in downstream of 20 Mbps.
2. VDSL2 provides higher data transmission speeds than that of ADSL in shorter range of distances. It can able to run with both asymmetric and symmetric rates. The maximum rate provided for VDSL is of 50 Mbps. The frequency band allotment for both downstream and upstream for different services for DSL is mentioned in the band plan provided by standards of International Telecommunication Union (ITU). ADSL provides the range of operating frequency of 1.1 MHz, and VDSL2 provides the range of operating frequency of 30 MHz.

1.2 Loop Topology Estimation

The assessment of performance of the DSL is vital in order to satisfy the service quality (QoS) needs to the user. The dispatch of the user line depends on the power transmission line setup. It involves the powerline transfer function which depends on the power transmission line topology and the noise power spectral density (PSD). Transmission line setup requires to be independently evaluated as trading apparatus, and cable plants are customarily possessed by various companies. The ability of a

service provider to predict precisely of the power transmission line conditions is vital to predict the dispatch. Single-ended loop testing (SELT) permits the power transmission lines to be equipped in bulk with no manual intervention [5, 6] and thereby vital to accomplish placement of DSL at low cost. It operates on the concept of reflection and provides of three important states [7, 8] (i) measurement stage—this is performed in the modem's material layer. An inquiry signal is dispatched, and the signals which are reflected (echoes) are controlled in this stage. (ii) Analysis stage—the reflected signals which are received are handled and converted to occur at the loop topology. (iii) Performance estimation stage—the maximum power-carrying limit of the power transmission line is calculated for the evaluated conditions for the loop by pertained guide lines of PSD according to the ITU.

1.3 Powerline Modelling

The power transmission line network has been developed for electrical energy distribution and delivery to consumers but not designed for communication purposes. Thus, it faces a challenge in modelling the communication channel which is mentioned in scarce in the literature [1, 5, 6, 9–22]. Aside of a wide gauge (14 AWG), the power transmission lines are basically shorter than that of telephone lines but have more shunt bridge taps with mainly inductive loads that are switched often ON and OFF. The power transmission lines have endless length, and hence, the impedance can be matched accordingly with the transmitter and receiving end. Various techniques are developed for modelling the of the power transmission line's characteristic impedance. There are two modelling aspects, namely modelling algorithms and parameters of the model. These aspects determine the accuracy and efficiency of the model.

1.4 Powerline Noise

The power transmission lines are of pair of wires in which there is no near-end crosstalk (NEXT) and far-end crosstalk (FEXT). Compared to other channels of communication, the power transmission line network consists of noise which cannot be reported only by additive white Gaussian noise (AWGN) model. Therefore, a complete interference analysis is much needed for modelling the noise factors. It can be categorised into three parts, viz periodic impulse noise which is synchronised with fundamental frequency, asynchronous variable impulse noise, and background noise [18–28]. The noise in power transmission line is considered as sum of collective impulse noises and AWGN. Asynchronous impulse noise is the critical one among all the noises present in the system which is the result of transients in turning ON and OFF of the loads [23]. It produces burst or bit errors in high-speed transmission of data packages [10, 12], which can be reduced by forward error correction and interleaving

techniques. The maximum power transmission limit of the power transmission lines can be calculated from noise and the SNR profiles.

1.5 Tone Loading Algorithms and Channel Capacity

The effectiveness of DMT system relies on the performance of the proposed technique of tone loading. The algorithms for tone loading provide the bit allocation for the sub-carriers so that the bit error rate (BER) can be reduced, and hence, the bit rate (BR) is increased [9]. The evaluation of the capacity of the transmission line is done using modified Shannon's theorem [17]. The transmitted bit number in the tone is determined by the SNR. It is decided with the channel and related to the tones in a symbolic representation of DMT. The taps of the bridges associated with the inductive loads cause reduction in data rates as the impedances of transmission line receiver side are mismatched. It can be increased by tuneable impedance conjugates so that the receiving end and transmission line impedances are matched. Hence, it is adapted to get required bit rates and to increase the normal transmit PSD.

2 Proposed Methods

2.1 The Channel Model

The matrices for distribution and main transmission lines can be found with ABCD parameters for individual segments of the complete network using the products of ABCD parameters for the individual segments along with the loop which is provided in Fig. 3.5 and Eq. (3.13). The entire loop transfer function can be acquired using Eq. (3.26), which is shown below:

$$V_1 = AV_2 + BI_2 = B\left(\frac{V_2}{Z_R}\right) \tag{1}$$

$$V_1 = AV_2 + BI_2 = AV_2 + B\left(\frac{V_2}{Z_R}\right)$$

$$H(f) = \frac{V_2}{V_1} = \frac{Z_R}{AZ_R + B}$$

$$H(f) = 20\log_{10}|H(f)|dB$$

2.2 Loop Topology Estimation

Various electric appliances will be connected to the customer end node of the various branches of distribution powerline network. In order to get the knowledge about the customer side network topology, two strategies [3] are followed, named as:

- Single-ended loop testing (SELT) and
- Double-ended loop testing (DELT)

DELT is done with equipment at both sides of the network, customer end, and the transformer of that particular area. DELT needs a service personal with equipment needed in the customer end. It cannot be utilised when there is no physical contact between customer end and the corresponding transformer. SELT is done without sending any personal to the customer end as it can be dealt from the area transformer itself. It is economical and quick to deal with initial construction and troubleshooting the faults if any occurred [24].

2.3 Multi-point CTDR Method

Power-line communication network consists of a higher number (greater than 5) of bridge taps by default. The echo which is received impacts highly in first few taps, and it will be less impactful for the remaining ones. At each taps, the strength of the sending end signal is reduced by 30%. Hence, if we move along on the successive taps, the signal strength will be poor. Hence, in CTDR SELT, measuring signals at single point leads to inability in estimating the entire topology. To avoid this, multi-point measurement points are utilised. Figure 3.8 provides a home PLC network example with the measurement points. The accuracy of the predicted line segments is increased by a strategy, named as Nelder-Mead optimisation algorithm (NOA) by comparison of the simulated echo of the predicted loop and the received echo in any instant of time or for a period of time (Fig. 2).

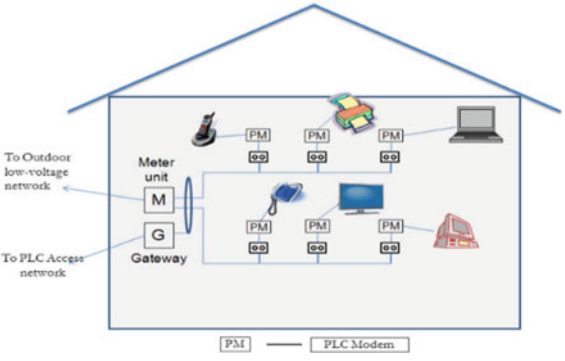


Fig. 2 Outdoor PLC network

As the number of variables is high, iterative method cannot be used for entire network topology.

Number of variables = 2 × No. of taps + 1.

Hence, tuning of the length of the transmission line is performed at the segments, not for entire topology level.

2.4 FDR Verification

FDR technique is used at multiple nodes in order to validate the predicted loop topology. It is used for generating the data for FDR. The means square value of the error from the measured data is shown in the following equation:

$$\text{MSE} = \left(\sum_{n=1}^{N} \left| R(\Phi, f_n) - \hat{R}(f_n) \right|^2 \right)$$

Figure 3 provides the flowchart for the combined FDR and multi-point CTDR technique.

3 Simulation Analysis

In this, the transfer function for the residential powerline nodes is derived. There was no conventional topologies listed. Hence, we have provided with a set of test cases in powerline network. In this, distribution lines exist with open circuit and closed circuit with loads connected which are inductive in nature. The transfer function of various test cases is provided in Fig. 3.10 transmission line with changing lengths with one to ten bridge taps in unloaded and loaded conditions. An inductance of 600 mH with 140 dbm/Hz AWGN noise signals and the losses increases with increase in distance of the line, increase with loads, and number of taps.

3.1 Simulation Conditions

The ratings of AWG12 and AWG14 are applied in simulation. But, due to higher number of bridge taps, attenuation depending on frequency is developed. The circuit topologies of customer end considered for study are provided in Fig. 3. The transfer function which depends on frequency is derived using the above-mentioned technique. The frequency response of the power transmission line lengths 600, 1200, and 3000 mts is provided in Loop 1 figure. In this, we can note that the losses increase by 20 dB as the length of the powerline increases twice (Fig. 4).

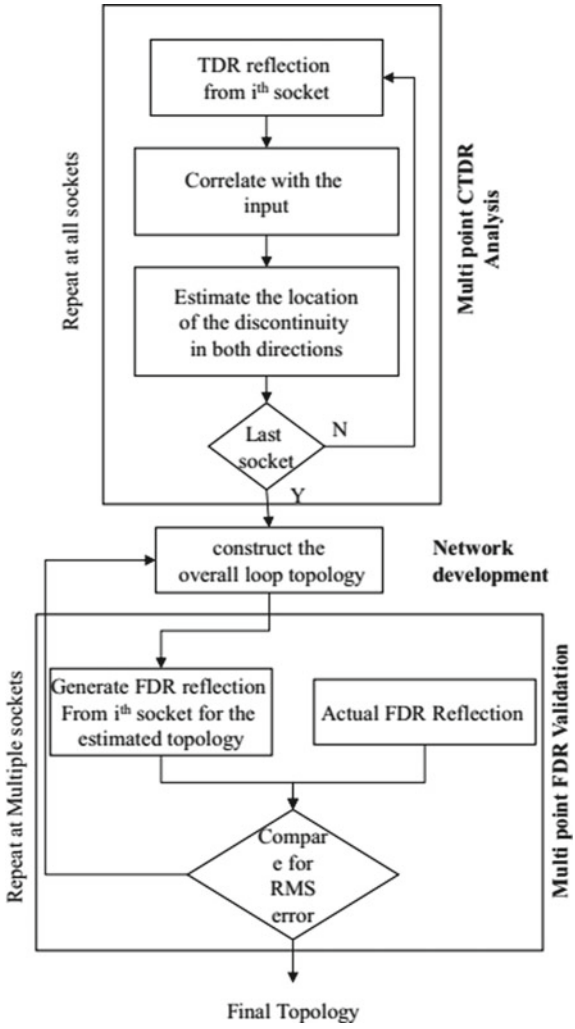


Fig. 3 FDR topology flowchart

3.2 Result of Topology Estimation

The simulation results for the test loops are shown below in Fig. 5. The powerline with one and two bridge taps is considered for the analysis, and more practical constraints are provided for the user-end powerline network with five and ten bridge taps for open BT and with AWGN of 140dBm/Hz, and also, inclusion of the inductive loads is considered.

Test loops considered are:

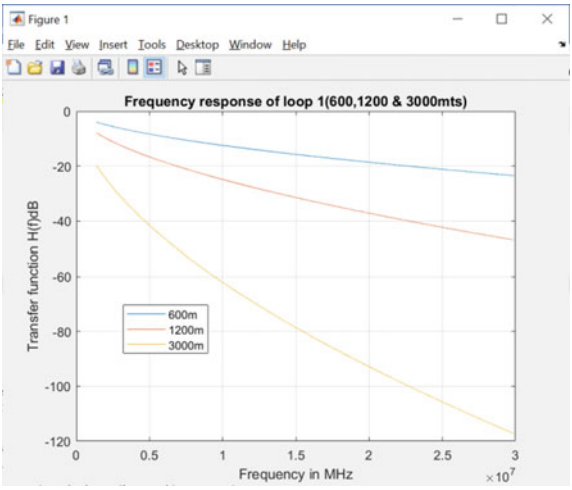


Fig. 4 Channel transfer function without BT

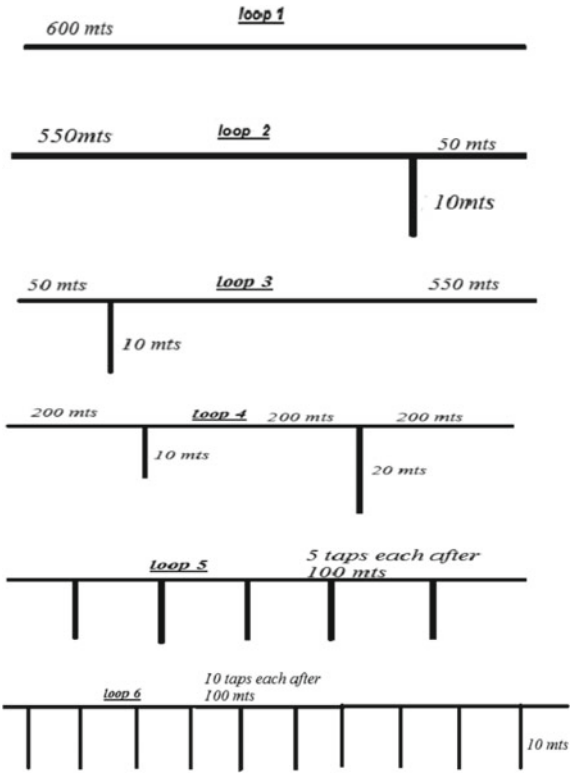


Fig. 5 a–e: Indoor powerline network topologies

1. Undisturbed transmission line as provided in Fig. 5a, the transfer characteristics are noted for various lengths such as 600, 1200, and 3000 mts which represent short, medium, and long-distance transmission lines.
2. To analyse the impact of a tap, line with single branch of 10 mts length at the receiving end is provided in Fig. 5b, and similarly, a single branch of the same length at the sending end as provided in Fig. 5c is regarded.
3. To analyse the impact of increasing taps, a line with double taps with varying length as provided in Fig. 5c is regarded.
4. As to the condition near to practical way of the indoor power distribution line, five and ten taps as provided in Figs. 5e and 4f have been regarded for study.

The normalised transfer functions which are dependent on line frequency 20log $H(f)$ are provided in following figures:

3.3 Effect of Inductive Loads and Input Impedance on the Channel Characteristics

In power transmission lines, residential loads such as refrigerator, fan, and mixer are connected to the BTs which are inductive loads. When these loads are connected to the system, the look-in impedance of the powerline network is modified. Therefore, there will be mismatch in impedance, which results in change in the network transfer function. Appropriate impedance matching is done by switching in the input side impedance in order to increase the power transfer or to reduce the reflections from the load.

3.4 Bridge Taps with Inductive Load

In this, Z_R is the load impedance provided in Eq. 3.30, in which the loads are coupled to the bridge taps are inductive in nature. It is given by

$$Z_R = r + j\omega L,$$

where conventional actual impedance of the fan is $r = 0.1\Omega$ and $L = 600\text{mH}$. The results from the simulation work for the previously mentioned test cases in Fig. 5 have been provided for both cases, open circuit BT and BTs connected with the inductive loads.

It is noted from the simulation results as provided in Fig. 5 that there are more losses and deeper notches due to the inductive loads connected to the bridge taps. This is because of the frequency-tuned loads proposed by the addition of inductance. In such scenarios, if the impulse noise is provided to AWGN, then the SNR reduces and the capacity of the powerline network channel is zero.

3.5 *Adaptive Impedance Matching*

Generally, in a power transmission line coupling, the load and source together should have same impedance: Z load $= Z^*$line, in which Z line is the transmission line characteristic impedance. In such states, there will be zero mismatch and, hence, no degradation of the signal. But, due to varying input impedance as various inductive loads are being switched ON and OFF of power line network, there will be mismatch in the line and load impedances. Maximum power gets transferred from generator to the load happens only when the load is matched to the generator. Complex conjugate matching is utilised when the maximum power transfer is needed as provided in Fig. 6

This maximum power transfer can be done by connecting a set of matching conjugate impedance with the modem using a hybrid circuit which is nothing but an electrical bridge. Generally, modems are connected to line with a bridge, and a simplified equivalent circuit for electrical or hybrid bridge is provided in Fig. 7.

A set of impedances which is almost complex conjugate of Z_{in} input impedance is connected with Z_b which will be chosen for balancing the bridge. A condition for balancing this hybrid bridge is reached when equation shown below is satisfied,

$$\frac{Z_i}{R_1 Z_i} = \frac{Z_b}{R_2 + Z_b}$$

The input impedance of the test cases provided in Fig. 5 is derived from the equations, and the calculated values are tabulated. Complex conjugate of the input side

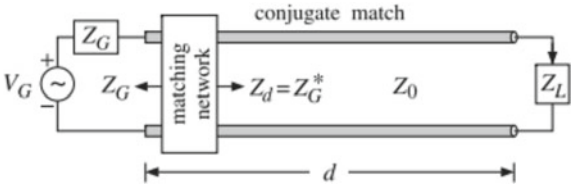


Fig. 6 Impedance matching of a transmission line

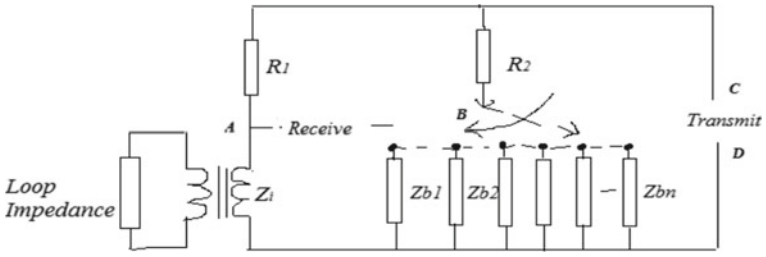


Fig. 7 Hybrid or electrical bridge

impedance provides the matching of impedance, and the capacity of the transmission powerline channel is improved. From the two-port network model of transmission powerline as provided in Fig. 3, the input side impedance will be a function of load side impedance. The look-in impedance is acquired using ABCD parameters of the transmission matrix. The input impedance is provided in the following equation

$$Z_{in} = \frac{V_1}{I_1} = \frac{AZ_R + B}{CZ_R + D}$$

For open tap, $I_2 = 0$ and $Z_R = 0$; hence,

$$Z_{in} = \frac{B}{D}$$

3.6 Proposed Impedance Matching with T *and* π *Filters*

In either 'T' or 'π' topology, a high-pass, low-pass, band-stop, or band-pass filter characteristic is feasible. The circuit components used can be symmetric or not, relied on the desired characteristics of line frequency. The high-pass T-filter in the given example possesses a very low impedance with higher frequencies and a very high impedance at lower frequencies. It results in the high frequencies being allowed to pass, while low frequencies are being reflected. Similarly, for the low-pass π-filter, the circuit can be coupled with a transmission line, permitting lower frequencies and reflecting higher frequencies. The m-derived filters with accurate impedances and the input side impedance can be almost constant in the pass band (Fig. 8).

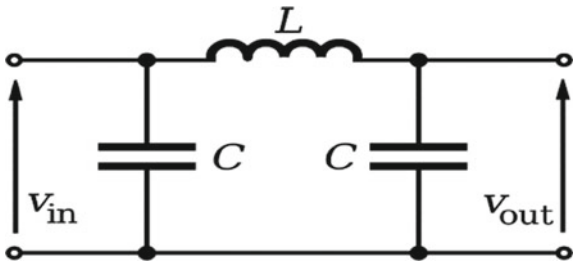


Fig. 8 T and Pi filter circuit

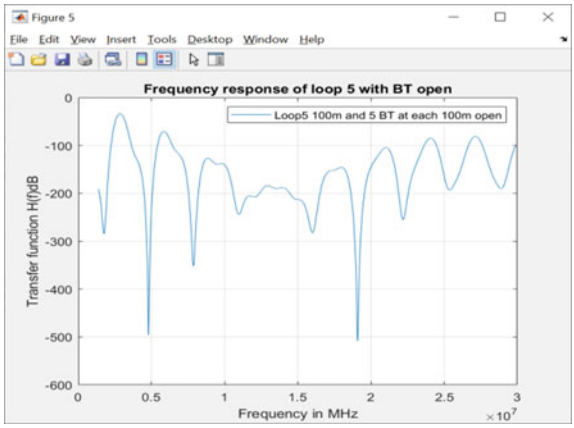


Fig. 9 US transfer function $H(f)$ Loop 5 BT with open

3.7 Channel Capacity in the Presence of Periodic Impulsive Noise and Inductive Load

The more number of the taps in the powerline network causes additional losses in the power cables. In this, there are no ideal or reference test cases for indoor power transmission lines. Test loops similar to the practical networks are provided in Fig. 5.

4 Simulation Results and Analysis

The load profile with bit and SNR for both downstream and upstream inclusion of inductive loads and impulse noise is provided for the test case loops provided in the figure. Results from simulation are provided by maximising the transmitting signal PSD and by coupling the conjugate impedance as corrective measures for reducing SNR with noise and inductive load. The maximum limit of the powerline transmission channel for the test cases under noise and inductive loading conditions is analysed with constant rate bit loading. Test Loop 5: line with five BTs with impulse noise and inductive load. The test loops with ten and five taps are regarded for simulation work. The SNR can be increased using impedance matching by adding a pair of conjugate impedances, which is also provided in figure. Figures 9, 10, 11, 12, 13, 14, 15, and 16.

5 Channel Capacity Estimation

As of first, observe the BT in second loop to be connected with an inductive load. SNR without and with impulse noise, with inductive load, for second loop is provided

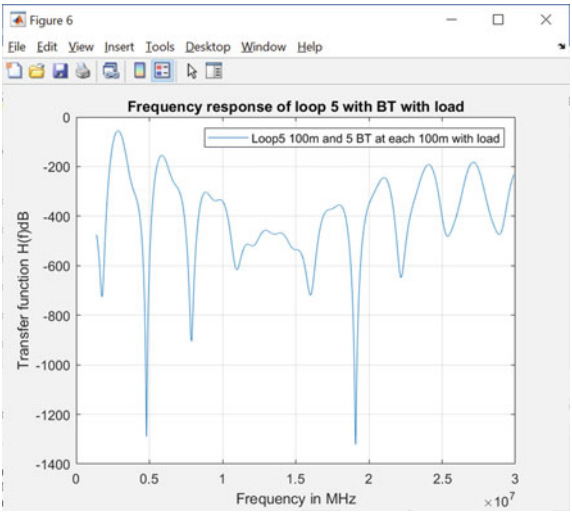


Fig. 10 US transfer function $H(f)$ Loop 5 BT with load

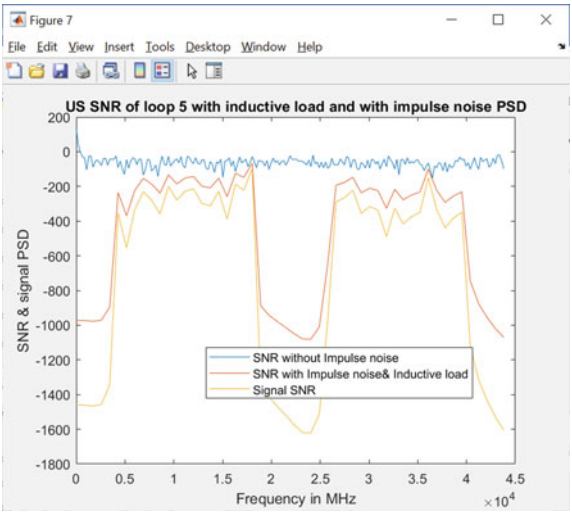


Fig. 11 US Loop 5 frequency versus SNR with load

in the figure for US and DS, respectively. When the SNRs are already high, a nominal development in transmission side PSD would be enough as is looked upon for second loop with BT ended within an inductive load which can be provided in figure for US and DS. The estimation of maximum limit for second loop with increase in transmission side signal PSD and inductive load is tabulated in Tables 1 and 2.

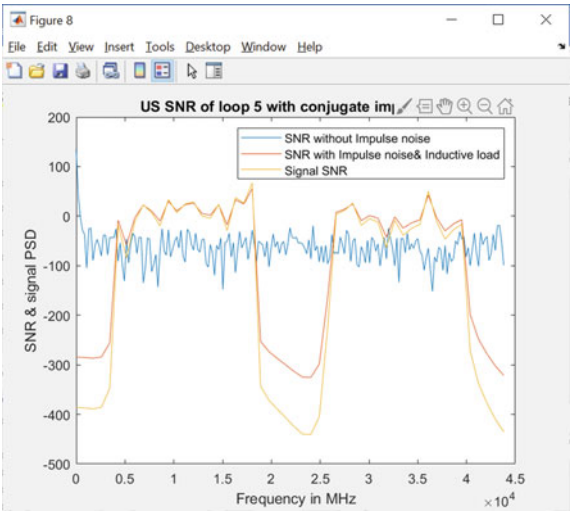


Fig. 12 US Loop 5 frequency versus SNR with and imp. noise load and impedance matching

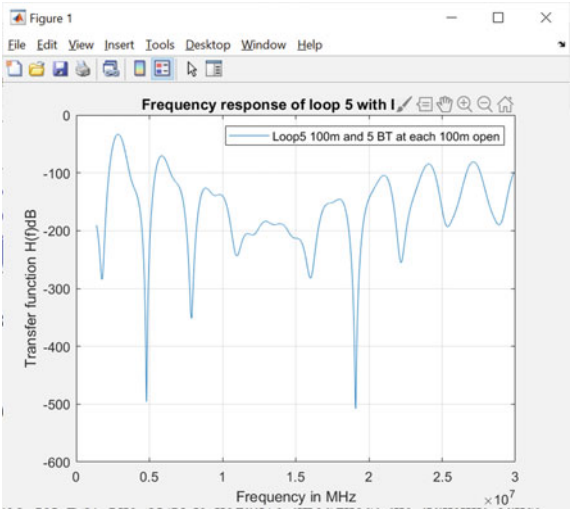


Fig. 13 DS transfer function $H(f)$ Loop 5 BT with open

6 Conclusion

In this paper, we studied about the conduction of an indoor power line (AWG14) with ten BTs, using ABCD matrix channel model depending on two-port network theory. The profiles of loading and SNR have been designed using VDSL2 masks that exercise DMT line code along with impulse noise aside from AWGN. The current transmission side PSD is enough for open-ended BTs. But, BTs with inductive load causes severe losses in data rates due to mismatch of line and characteristic impedance. Data rates are improved by adopting adjustable values of conjugate

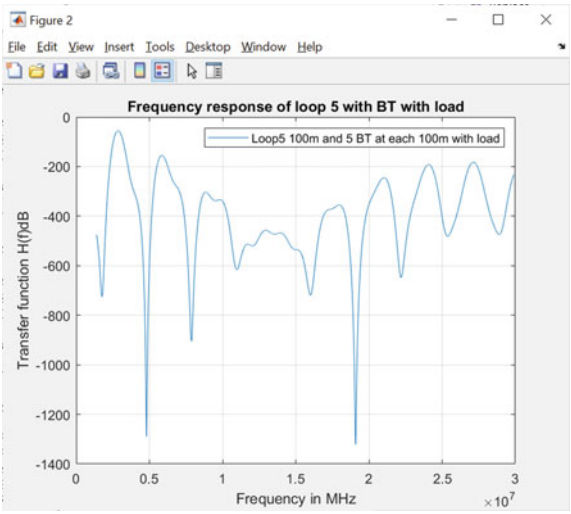


Fig. 14 DS transfer function $H(f)$ Loop 5 BT with open

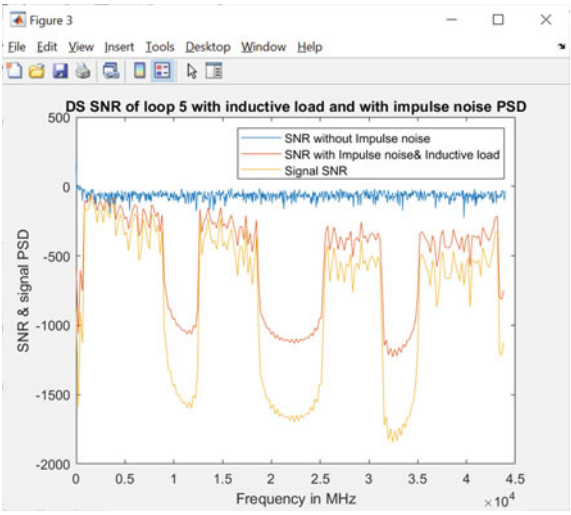


Fig. 15 DS Loop 5 frequency versus SNR with load and imp. noise

impedances in the modem that match with the look-in impedance. Hence a combination of adjustable hybrid impedances matching system, nominally increase PSD in order to get required data rates. This technique has a distinct advantage in that it reuses the complete digital part of conventional ADSL and VDSL2 modems .

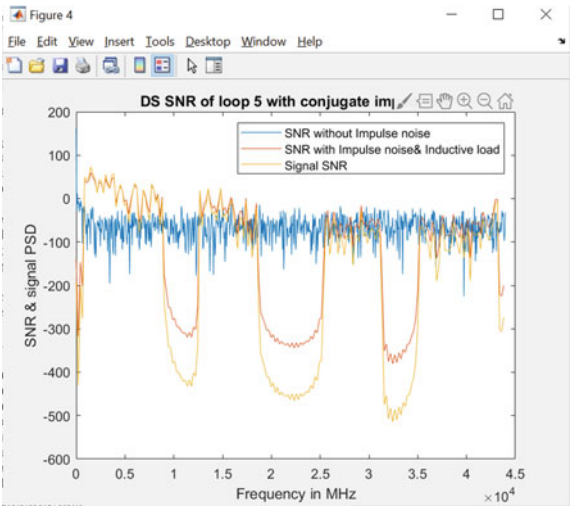


Fig. 16 US Loop 5 frequency versus SNR with load and impedance matching

Table 1 Capacity estimation

Line topology	US rates with inductive load (Mbps)	DS capacity with inductive load (Mbps)
Loop 2	40.7	14.38
Loop 3	35.6	13.38
Loop 4	30.2	9.14
Loop 5	25.7	7.9
Loop 6	20.2	3.2

Table 2 Capacity estimation with impedance matching system

Line topology	US rates with inductive load (Mbps)	DS capacity with inductive load (Mbps)
Loop 2	100.34	90.26
Loop 2	110	89.3
Loop 3	97	85.4
Loop 4	90	80
Loop 5	85	75

References

1. X. Carcelle, *Power Line Communication in Practice* (2009)
2. V. Oksman, S. Galli, G.Hn: The new ITU-T home networking standard. IEEE Commun. Mag. (2009)
3. S. Galli, O. Logvinov, Recent developments in the standardization of power line communications within the IEEE. IEEE Commun. Mag. (2008)

4. R. Sathya, Use of ubiquitous powerline infrastructure for providing broad-band access to bridge the ICT divide, Brussels, 22 March 2006. Online www.ist-powernet.org
5. S.Galli, A. Scagllone, K. Dostert, Broadband is power: internet access through the power line network. IEEE Communications Magazine, Guest editorial, pp. 82–83, May 2003
6. Y. Lin, H.A. Latchman, M. Lee, A power line communication network infrastructure for smart home. IEEE Wireless Commun., 1070-9916/02,Dec. 2002
7. A. Matov, Measurements and Modeling of Power Line Channel at High Frequencies. *Integrated Systems Lab.Swiss Federal Institute of Tech* (Lausanne, Switzerland, 2021)
8. M. Zimmermann, K. Dostert, A multi path model for the power line channel. IEEE Trans. Commun. **50**(4), (April 2002)
9. Mains Network, http://en.wikipedia.org/wiki/Mains_network
10. IEEE P1901, Draft Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications, PUA and UPA contribution to IEEE 1901 call for submission on BPL access requirements Functional and Technical Requirements, pp. 1–41, February 2006. Online www.upaplc.org
11. H. Hrasnica, A. Haidine, R. Lehnert, *Broadband Powerline Communica-tions: Network Design*, (Wiley, 2004)
12. P. Donal, General Overview of the UPA and Its Activities, January 2009. Online www.upaplc.org
13. http://en.wikipedia.org/wiki/Power_line_communication
14. http://en.wikipedia.org/wiki/Automatic_meter_reading
15. P. Borle, A. Saswadkar, Automatic meter reading for electricity using power line communication (2013)
16. M. Zimmermann, K. Dostert, A multipath model for the powerline channel. IEEE Trans. Commun. **50**(4), 553–559 (2002)
17. W. Liu, H. Widner, P. Raffin, Broadband PLC access systems and field deployment in European power line networks. IEEE Commun. Mag., (May 2003)
18. Query ID="Q12" Text="QueryCE:[CROSSREF]Score: 0.40crsid: hTQYHStype: bibarticleAuthors: Hualyu Dai, H.V. PoorYear: 2003JournalTitle: IEEE Communications Magazine-JournalAbbTitle: IEEE Commun. Mag.ArticleTitle: Advanced signal processing for power line communicationsVolumeID: 41IssueID: 5FirstPage: 100LastPage: 107BibArticleDOI: 10.1109/MCOM.2003.1200108" H. Dai, H. Vincent poor, Advanced Signal Processing for Power Line Communications. IEEE Commun. Mag. 0163-6804/03, pp.107, (May 2003)
19. M. Gotz, M. Rapp, K. Dostert, Power line channel characteristics and their effect on communication system design in IEEE Communication Magazine, (April 2004)
20. M. Gebhardt,F. Weinmann, K. Dosert, Physical and regulatory constraints for communication over the power supply grid. IEEE Commun. Mag., (May2003)
21. P.S.Henry, Interference characteristics of broadband power line communication systems using aerial medium voltage wires. IEEE Commun. Mag., (May2003)
22. H.C. Ferreira, H.M Grove, O. Hooijen, A.J.H. Vinck, Power Line Communications: An Overview. 0-7803-3019-6/96, in *Proceedings of the 4th IEEE AFRICON*, vol. 2, (1996), pp. 558–563
23. S. Galli, The inter inter-co-PHY protocol (IPP): A simple co existence protocol. IEEE International Symposium on Power Line Communications, Dresden, Germany, 31 March 2009
24. S. Goldfisher, S. Tanabe, IEEE 1901 Access system: an overview of its uniqueness and motivation. IEEE Commun. Mag., (October 2010)
25. S. Galli, L. Oleg, Recent developments in the standardization of power line communications in the IEEE. IEEE Commun. Mag., 64–71, (July 2008)
26. MainsNetwork, http://en.wikipedia.org/wiki/Mains_network
27. R. Sathya, Broadband over powerlines: a rapid way to join the knowledge society. Africa/Middle East Next Generation Network Summit, Johannesburg, South Africa, 17–19 February 2008. Online www.ist-powernet.org
28. OPERA, Open PLC European research alliance for new generation PLC integrated network phase 2. Online www.ist-world.org/ProjectDetails.aspx

29. P.K. Ray, A. Hazra, Broadband Powerline Communication an Indian Experience IEEE international Symposium on Powerline Communication and its Applications, (2011)

Automated People Monitoring System Using OpenCV and Raspberry Pi



Dipankan Bandopadhyay, Vinod Jha, Atri Bandyopadhyay, Pratik Roy, Rupesh Halder, and Swagatam Majhi

Abstract Over the last decade, there has been a quantum leap in terms of the evolution of new methodologies to better our quest to understand artificial intelligence and machine learning. One such field, where there has been an unparalleled advancement, is computer vision. The paper aims to design and structure an automated monitoring system that automates the monitoring of the number of people in this COVID-19 scenario in a designated enclosure. We have deployed the system on Raspberry Pi module and integrated a HOG detector which transcends ordinary Haar cascades in terms of performance. This model can then subsequently be connected and integrated with other modules to further enhance its applicability and spectrum of usage.

Keywords Raspberry Pi · OpenCV · SVM · HOG · COVID-19

1 Introduction

The applicability of embedded systems, such as Raspberry Pi and Arduino Uno, has skyrocketed over the years. The present work uses Raspberry Pi for implementation of automated people monitoring system using image processing and machine learning. The motivation for this project came from the need of this pandemic situation where

D. Bandopadhyay (✉) · V. Jha · A. Bandyopadhyay · P. Roy · R. Halder · S. Majhi
School of Electronics Engineering, KIIT Deemed to be University, Bhubaneswar 751024, India
e-mail: 1804093@kiit.ac.in

V. Jha
e-mail: vjhafet@kiit.ac.in

A. Bandyopadhyay
e-mail: 1804088@kiit.ac.in

P. Roy
e-mail: 1804111@kiit.ac.in

R. Halder
e-mail: 1804123@kiit.ac.in

S. Majhi
e-mail: 1804066@kiit.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_86

offices, public places and transport vehicles are allowing limited presence of people. The presented device can be used to minimize human involvement to observe the people count in public places. The project shall be deployed using the OpenCV platform and will actively identify the count of people within a space covered by the visual input feed (a connected camera in most instances) [1]. For the purposes of demonstration, a pre-recorded video has been passed into the model. However, this can be replaced by a Raspberry Pi camera module or other similar camera receptors that can be attached with the Pi board.

2 Integrating Raspberry Pi with OpenCV

Digital image processing has come a long way in the modern world. The multi-faceted potentialities of the subject give rise to a smorgasbord of possibilities as far as application-oriented thinking is concerned. The utility of such powerful and modern image processing tools has not gone unnoticed and is in fact being actively used today by all agencies and even governments across the world [2]. Computer vision (CV) is defined as "*… an interdisciplinary scientific field that deals with how computers can gain high-level understanding from digital images or videos*" [3]. Computer vision enables the machine to decode and understand what actions, or information, are present in the image or the motion graphic presented to it. In this project, we harness computer vision's power by utilizing the OpenCV library.

2.1 OpenCV Fundamentals

OpenCV, as its name suggests, is an open source, publicly accessible package library that provides for a host of features related to computer vision. It has cross-platform support, thus enabling programmers specializing in multiple languages to work on its offerings and develop novel computer vision solutions. Although OpenCV was originally built for C/C++ , its developers provided a Python binding for it soon after its release. We connect to the Raspberry Pi through the VNC Viewer software, which acts as a bridge between the Windows PC and the Raspberry through a CAT-5 Ethernet cable[4]. The advantage of ensuring an SSH connection is that it offers both security (by ensuring data encryption between transfers) and hassle-free root-level access on the remote machine. We also install a few dependencies for the Python binding of OpenCV. These dependencies have to be installed prior to the actual installation and are required for the smooth functioning of the library[5].

3 The Viola–Jones Detector

One of the more primitive, but universally recognized algorithms that exists for face detection is the Viola–Jones detector. First proposed in 2001 by Paul Viola and Michael Jones, it is essentially a framework that captures and detects image features in real time. The algorithm works best for faces oriented towards the camera; that is, detection rates directly depend on if the image has a frontal face [4]. Before applying its mask to detect features, the Viola–Jones detectors convert the 3-channel RGB spectrum into a grayscale image by the following formula: $Y_{\text{Grayscale}} = 0.3 * R + 0.59 * G + 0.11 * B$.

This conversion helps to compress the image and speed up processing times. Later, it identifies the locational coordinates on the RGB image from the values obtained in the grayscale image, so there is no major difference with respect to identification performance. The algorithm works by defining a stride (a box) that scans the image pixels for Haar-like features. More specifically, it hunts for three Haar features: edge features, line features and four-sided features. It is with the help of these features that the machine deciphers what an image contains. An edge would mean a variance of shadow and lighting effects, which consequently impact pixel values around an edge. The horizontal and the vertical features are what the key facial features, such as the nose and the eye, look like to the detector; while the Haar cascade classifiers are fast, they are not reasonably accurate. The Viola–Jones algorithm often misses out faces, even when clear, because of slight variations in pixel values. In the task of building a people counter, the last thing to do would be to feature an algorithm that not only reports inaccurate results, but is also fifteen years old [5]. Thus, in the quest to better detect results and ensure fast processing, another technique is employed: the histogram of oriented gradients (HOG) coupled with a linear support vector machine (LSVM) (Fig. 1).



Fig. 1 Viola–Jones detector in action

4 Understanding Histogram of Oriented Gradients (HOG)

The HOG technique is an incredibly fascinating way to extract features out of an image. To better understand the process, we shall take the help of some examples. Let us zoom into the image of a car (grayscale) as shown in Fig. 2 and try to compute the gradient and the magnitude for that cell. In the below example, the gradient in the X-direction $= 120 - 70 = 50$.

The gradient in the Y-direction $= 100–50 = 50$.

Thus, the overall gradient magnitude $= \sqrt{50^2 + 50^2} = 70.1$.

Also, the gradient angle can be computed as $= \tan^{-1}(\frac{50}{50}) = 45°$.

Hence, in a similar manner, we can compute the magnitude and the angle pair values for each pixel block within an image. Let us take another example to now understand HOG feature extraction from an image [6]. Consider the image of a red truck as the input image, as shown in Fig. 3.

Right away, as a preliminary step, using a 8×8 pixel cell, we compute the gradient magnitude and gradient direction. This is similar to a Sobel operation in the X- and the Y-directions. Once the computation is done, the results look like (Fig. 4).

From the below processed images in Fig. 5, we know that for each pixel, we have a magnitude value and an angle value. The beauty of this process lies in the fact that it can take the oriented gradients and make a histogram that represents the same. For purposes of the distribution plot, we segregate the pixels into 9 bins of 20 degrees

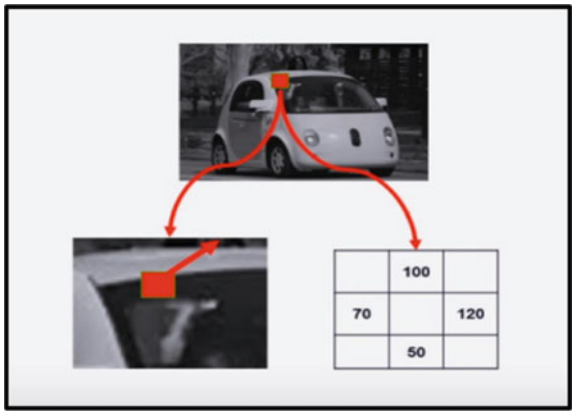


Fig. 2 Demonstration of magnitude and gradient calculation



Fig. 3 An input image of a red truck



Fig. 4 Gradient in *X*-direction



Fig. 5 Gradient in Y-direction

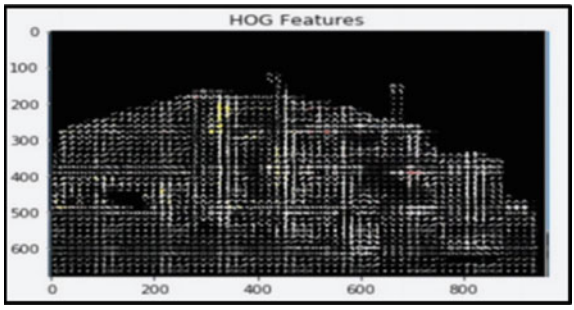


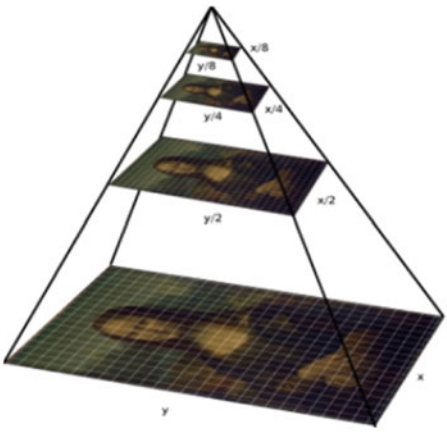
Fig. 6 HOG feature vector's image representation

each (0–180 degrees in all). This reduces 64 vectors into only 9 values. In practical applications, the HOG will compute feature vectors by the sliding window method, going on concatenating values until the end of the block [7]. For the truck image, the image representation of the feature vectors is as shown in Fig. 6.

4.1 SVM Detector and HOG Descriptor Parameter Tuning

Figure obtained immediately above is the feature vector representation. It is this feature vector that we pass onto the linear SVM detector, which OpenCV provides for as part of its default package library. After initiating the HOG descriptor and setting the SVM detector with the default people detector, we define the detector function that returns the count of the total number of people detected within the frame and displays

Fig. 7 Image pyramid



the count by embedding it into the output frame. The HOGCV.detectMultiScale() function requires an elaborate understanding as it is crucial to the performance of the program. By fine-tuning this function in itself, the output accuracy can be improved significantly [8]. Some of the parameters that are of particular interest are listed below.

1. *winStride*: The winStride parameter, shorthand for Window Stride, is a tuple parameter that defines the size of the sliding window that assesses the image. At each stop of the sliding window, the program extracts the HOG features.
2. *Padding***:** The padding property is also a tuple like the winStride parameter. Its value sets the number of pixels in both X- and Y-directions that the sliding window should pad the border pixels prior to HOG feature extraction. Adding padding before the process of feature extraction actually helps better the performance of the model in itself.
3. *Scale:* The scale parameter in the HOG descriptor is used to determine the number of layers that the model will work with. At each succeeding layer of the image pyramid [9, 10], the image is downsized and optionally Gaussian blur is added to minimize potential noise problems (Fig. 7).

5 Results

A Raspberry Pi has been used as a computer motherboard to successfully calculate and demonstrate people count via digital image processing with the help of OpenCV which is actually a cross-platform computer vision tool alongside two machine learning detection algorithms—support vector machine (SVM) and histogram of oriented gradients (HOG). As it can be observed below (from Figs. 5 and 6), it is clear that the output result that can be seen via this image processing mechanism is almost always true regarding the data at the given place and time. Hence, this

project is expected to work properly and accordingly and come into a lot of good use. However, this being more of an experimental initiative rather than a capitalized end product, there might be some flaws and errors and there is always a room for improvement. The results hence obtained are given in Figs. 8 and 9.

As it can be observed below (from Fig. 8 and Fig. 9), it is clear that the output result that can be seen via this image processing mechanism is almost always true regarding the data at the given place and time. Hence, this project is expected to work properly and accordingly and come into a lot of good use. However, this being solely an open-source project due to lack of proper resources and the reason of doing it being more of an experimental initiative rather than a capitalized end product, there

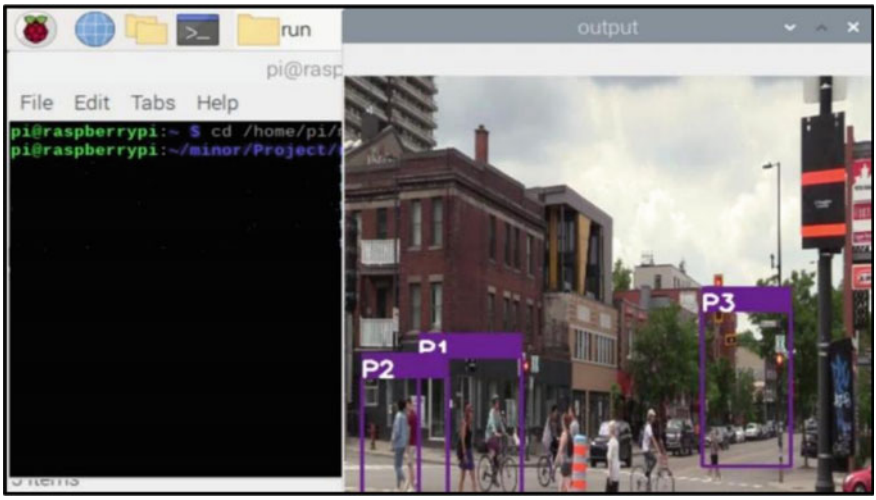


Fig. 8 Total person count in actual video is 3



Fig. 9 Total person count in actual video is 6

might be some flaws and errors and there is always a room for improvement. The results hence obtained are given in Figs. 8 and 9.

6 Conclusion

It is common knowledge that no model can be cent per cent perfect in its area of deployment. Hence, we cannot claim that a singular solution exists to a certain problem sphere. In this domain of work, we have tried to take a holistic approach towards development, keeping in mind and knowing fully well the design and implementation constraints.

(a) The Raspberry Pi is inherently a resource-limited device. The trade-off that it makes to ensure portability and ease of use is by shedding a significant chunk of processing power [11]. The Pi board comes loaded with 1 gigabytes (GB) of RAM memory, which is comparatively small by modern standards. Hence, running resource intensive projects, particularly image processing applications that devour GPU power as well as demand effective RAM swaps and CPU threading, are slowed down. Yet, we still can effectively minimize the drawbacks as we already know the constraints beforehand.

(b) Generally, detection rates can be further improved by utilizing advanced image processing utilities like YOLOv3. It applies neural networks to the entire image at once to predict probabilities. However, these results perform well only on powerful GPUs. On a resource-constrained device as the Raspberry Pi, the performance gains are minimal to none. However, overheating is observed when using the YOLOv3. Most users begin by implementing the OpenCV–Haar cascade model. However, to improve performance and detection rates and to avoid overheating, the work has used the HOG model and then compared it in an SVM detector to get the classification results.

References

1. E. Khoumeri et al., People counter with area occupancy control for Covid-19. in *International Conference in Artificial Intelligence in Renewable Energetic Systems.* (Springer, Cham, 2020)
2. M. Shubham et al., Human detector and counter using raspberry Pi microcontroller. in *2017 Innovations in Power and Advanced Computing Technologies (i-PACT).* (IEEE, 2017)
3. N. Gagandeep Singh et al., Facial detection and recognition using OPENCV on Raspberry Pi zero. in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN).* (IEEE, 2018)
4. P. Wilson, J. Fernandez, Establishing a face recognition research environment using open source software. in *ASEE Gulf-Southwest Annual Conference* (2005)
5. Y.-Q. Wang, An analysis of the Viola-Jones face detection algorithm. Image Processing On Line **4**, 128–148 (2014)

6. K. Mateusz, M. Kluczewski, M. Gorgon, Floating point HOG implementation for real-time multiple object detection. in *22nd International Conference on Field Programmable Logic and Applications (FPL).* (IEEE, 2012)
7. M. Kachouane et al.,HOG based fast human detection. in *2012 24th International Conference on Microelectronics (ICM).* (IEEE, 2012)
8. S. Yahia, M. Atri, R. Tourki, Human detection based on integral Histograms of Oriented Gradients and SVM. in *2011 International Conference on Communications, Computing and Control Applications (CCCA).* (IEEE, 2011)
9. Z.R. Tan, S. Tian, C.L. Tan, Using pyramid of histogram of oriented gradients on natural scene text recognition. in *2014 IEEE International Conference on Image Processing (ICIP)* (2014), pp. 2629–2633
10. Wahyono, V. Hoang, L. Kurnianggoro, K. Jo, Scalable histogram of oriented gradients for multi-size car detection. in*10th MECATRONICS2014- Tokyo* (2014), pp. 228–231
11. G. Ishita et al., Face detection and recognition using Raspberry Pi. in *2016 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE).* (IEEE, 2016)

Sign Language Recognition Using Convolutional Neural Network



Ayush Kumar, Sumeet Kumar, Shivam Singh, and Vinod Jha

Abstract Sign language is learned by deaf and dumb, and usually, it is not known to normal people, so it becomes a challenge for communication between a normal and hearing-impaired person. Thus, we decided to bridge the gap between hearing impaired and normal people and make the conversation easier. Sign language is one of the oldest and most natural forms of language for communication, but since most people do not know sign language and interpreters are very difficult to come by we have come up with a real-time method using neural networks for finger-spelling-based American sign language. In this research, a hand image is first passed through a filter and after the filter has applied the image is passed through a classifier that predicts the class of the hand gesture. Our method provides above 98% accuracy for the 26 letters of the alphabet. The paper implements that a functional real-time vision-based American sign language recognition for D&M people has been developed for ASL alphabets.

Keywords Sign language · ASL · Hearing disability · Convolutional neural network · Optimizer · Loss function

1 Introduction

ASL [1] is a predominant sign language. Since the only disability D&M people have is communication-related and they cannot use spoken languages, the only way for them to communicate is through sign language. As well stipulated by Nelson

A. Kumar (✉) · S. Kumar · S. Singh · V. Jha
School of Electronics Engineering, KIIT Deemed to be University, Bhubaneswar 751024, India
e-mail: 1804015@kiit.ac.in

S. Kumar
e-mail: 1804063@kiit.ac.in

S. Singh
e-mail: 1804058@kiit.ac.in

V. Jha
e-mail: vjhafet@kiit.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_87

Mandela [2], "Talk to a man in a language that he understands, that goes to his head. Talk to him in his language, that goes to his heart, language is undoubtedly essential to human interaction and has existed since human civilization began." It is a medium humans use to communicate to express themselves and understand notions of the real world. Without it, no books, no cell phones, and not any word would have any meaning. This model is a visual–gestural language [3] used by deaf and dumb people for the communication process [4]. By using this, they can easily communicate with themselves or with other peoples through sign language and hence the communication gap between them and other people becomes lower. For expressing their ideas with other people, they would use their hand expressions [5] for better communication. This paper implements its own data set, and after training the data set, the result shows very high accuracy which can become better if more and more research and development are done on this paper.

Sign language is a visual language that consists of three major components that are as follows [6] (Table 1).

In this paper, the paper focuses on producing a model which can recognize finger-spelling-based hand gestures [7] to form a complete word by combining each gesture, which gives us the result helping those affected people understand easily. The gestures which the paper aims to train are as given in the image below (Fig. 1).

Table 1 Major components of sign language

Finger spelling	World-level sign vocabulary	Non-manual features
Used to spell words letter by letter	Used for majority of communication	Facial expressions and tongue, mouth and body position

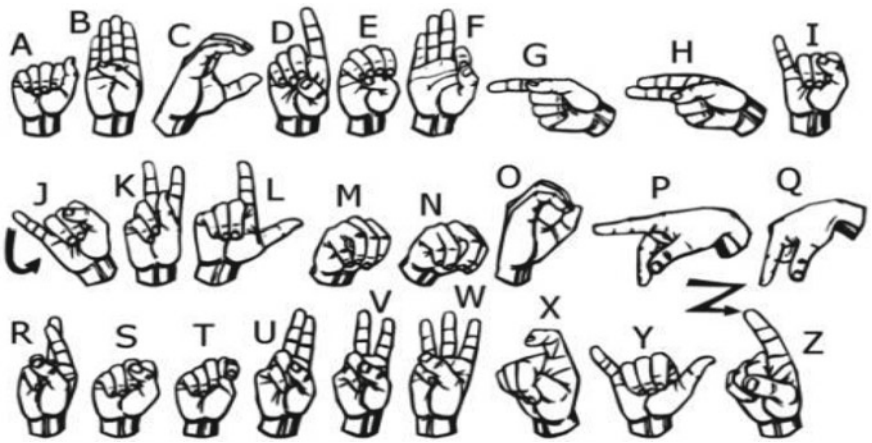


Fig. 1 American sign language alphabet

2 Methodology

Data collection is the most important part to start our project, but due to lack of data set over the Internet there was a need of creating a data set of 26 alphabet signs, from A to Z in ASL having 6500 images. At first, creating a data folder was important and in that data folder there were two more folder names as test and train and each folder contains 26 folder names on alphabet a to z. Therefore while capturing an image, it should be placed in the right folder. There are 6500 images in which 5000 images are for training and 1500 for testing. Now through the webcam, the images were captured for different hand gesture symbols from A to Z. For capturing an image, at first, the image is defined where it should be stored like in the test or train folder.

Then, the image is chosen for a particular alphabet and the quantity or number of images which has to be saved for that particular alphabet. After that, the camera input captures our hand gesture and saves what that gesture indicates by pressing a key from a to z in the respective folders. By this, the images were stored in the desired folders and our data set has been created. And then we applied a threshold filter to form the grayscale image. Here, the color of images is in black and white, whereas black color for hand gesture and white for the background.

The method which we use in this project is CNN.

Convolutional Neural Network:

CNN is a type of deep neural network which takes an image as input with various filters like convolutional filter which performs the convolution between image and the kernel to get the desired result; the filter can be of any type like edge detection, a color filter, or anything. The sign language model is model-based.

Desired output is in the form of a particular character from A to Z what the paper wants. So, the basic architecture of this model is based on CNN.

Since the network core is CNN, so dealing with the image is a main part and the reason behind choosing CNN was a simple as CNN is more accurate and is also more of an image-based processing neural network.

CNN involves many layers; one of them is convolution which is used for feature extraction. In CNN the input data or input image passes through many stages. In the last stage artificial neural network provides the desired output.

Layering:

At first, the paper takes the input image of a sign from A to Z in ASL. The size of the input image is 128 $\times$ 128 pixels which is then applied to the first convolution, comprising of 32 filters, which then applied on the input image and provided the resultant size of 126 $\times$ 126. Next was the application of max pooling resulting in 63 $\times$ 63 pixel-sized image. Again, the second convolution, the same 32 filters on the image resulted in the size of 61 $\times$ 61 pixels and then we again applied max pooling on it. Then, afterward flattening is applied which converts our image into 1 D array, and after applying a fully connected layer a.k.a artificial neural network, the desired output in the form of text from A to Z is displayed (Fig. 2).

Convolution:

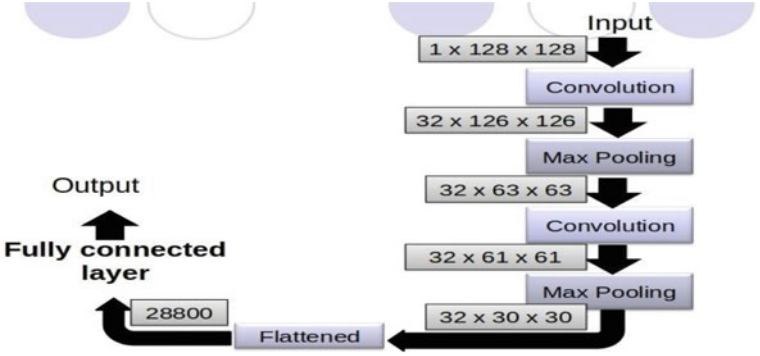


Fig. 2 Process of convolutional neural network

It is the simplest application that works on a filter applied to an input that results in inactivation. Application of the same filter to an input results in a map of activations called a feature map. Convolution is the simplest application of a filter to an input that results in an activation feature.

$$
\begin{aligned}
(f * g_N)[n] &= \sum_{m=0}^{N-1} f[m] g_N[n-m] \\
&= \sum_{m=0}^{n} f[m] g[n-m] + \sum_{m=n+1}^{N-1} f[m] g[N+n-m] \\
&= \sum_{m=0}^{N-1} f[m] g[(n-m)_{mod N}] \triangleq (f *_N g)[n]
\end{aligned}
$$

3 Deep Learning Classification Models

In the term "deep learning," the word "deep" quantifies the hidden layers in a particular neural network architecture. Classification of hand gestures is built on deep learning technique which involves one method:

convolutional neural network (CNN).

3.1 Convolutional Neural Network (CNN)

For the classification of the hand gesture, a convolutional neural network with a structure consisting of seven layers, a single input layer, followed by five hidden

layers, and finally an output layer, is ideal. The input layer contains an image of (128 × 128) pixels which indicates that the input layer consists of 784 neurons, which is equal to the number of input features. The pixels of the input image are in a grayscale mode which means that zero value is appended for a white pixel and a unity value to represent a black pixel. The design model comprises five hidden layers.

The first hidden layer plays the role of the first convolutional layer of the design, which accounts for the feature extraction from the input data. It is also responsible for performing the convolutional operation between a filter (or kernel) and the immediate previous layer. Formation of multiple feature maps along with adaptable kernels as well as rectified linear units (or ReLU), acting as activation functions, is contained in this layer. The size of the filter (or kernel) fixes the filter localization. An activation function (ReLU) [8] is casted-off at the termination of each convolutional layer and the fully connected layers to inflate the model performance [9]. The first pooling layer [10] acts as the second hidden layer in the system, which decreases the output data arriving from the convolutional layer, thus decreasing the number of parameters and eventually increasing the computational efficiency. The "max pooling" scheme has been used to subsample the feature map dimensions. Next, other set of convolutional and pooling layers are designed having the same functionalities as that of the first set of convolutional and pooling layers except for their variations in kernel size and feature maps. The output dimension of the feature map is given by

$$n_o = \left[\frac{n_i - k + 2p}{s} + 1\right]$$

where "n_o" accounts for the dimensions of the input image, "k" represents the size of the kernel or filter, and "p" and "s" account for padding and stride, respectively.

Then, a flatten layer [11] is used to map the two-dimensional feature map matrix into a single-dimensional vector. Now, the first fully connected layer is designed, which is nearly equivalent to the hidden layer of the artificial neural networks except for bridging every neuron from the immediate previous layer to the layer that follows the next. To prevent model from over-fitting, the method of dropout regularization is generally adopted at the first fully connected layer, which cancels out few neurons at random during the training process to enhance the model performance. The second fully connected layer is the last hidden layer of the model, which plays the role of the output layer [12]. This layer contains 26 neurons because there are twenty-six classes in the output, that is, alphabets from A to Z. The output layer uses the "SoftMax" activation function [13], which is used to provide the probability distribution of the output classes (Fig. 3).

A loss function, also regarded as an error function or cost function, determines the degree to which the designed algorithm models the data set. Moreover, the loss functions come up with a static blueprint of how the model is performing. Optimizers bind together the loss function and the parameters of the model and refurbish the model depending upon the output of the loss function. Both the loss functions and the optimizers play an important role in determining the accuracy of any model.

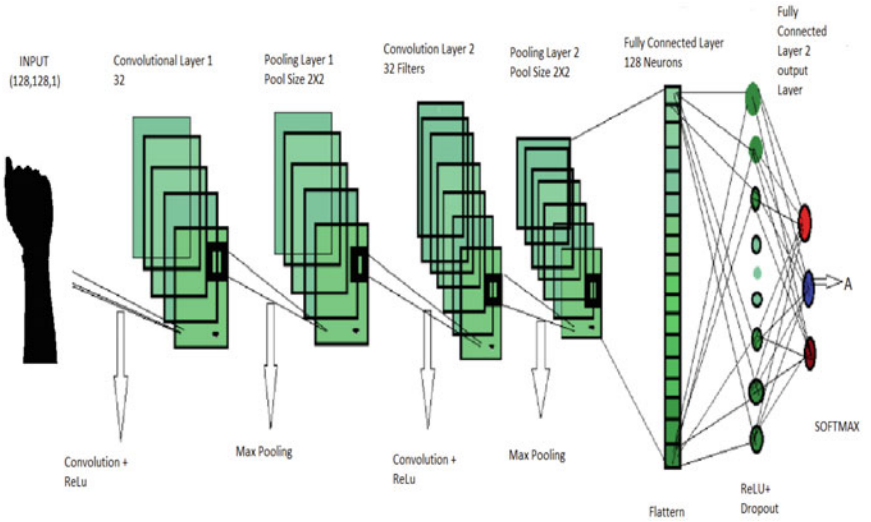


Fig. 3 Process flow of convolutional neural network

Table 2 Comparison of CNN models based on optimizer and accuracy

Sl. no.	Model	Epochs	Loss function	Optimizer	Accuracy (%)
1	CNN	26	Categorical cross-entropy	SGD	93
2	CNN	26	Categorical cross-entropy	Adam	98

In this paper, a performance comparison is depicted by using loss functions with two different sets of optimizers over the designed CNN model used for the recognition of hand gesture sign recognition. In the first case, stochastic gradient descent (SGD) [14] is used as the optimizer along with categorical cross-entropy loss as the loss function and has attained a test set accuracy of approximately 93% while computing for twenty-six epochs. In the second case, the optimizer used was Adam [9] along with the categorical cross entropy Loss function [9] to achieve a test set accuracy of approximately 98% while computing for the same number of epochs (Table 2; Fig. 4).

4 Future Scope

The world is a place of never-ending problem, and one of the problems deaf and dumb people face is lack of knowledge in communicating with other people which makes it difficult for them to communicate. Considering this problem on a small scale, this project is created, but given the chance of growth it can even live translate the sign language with the inbuilt voice which gives output and makes the conversation easier

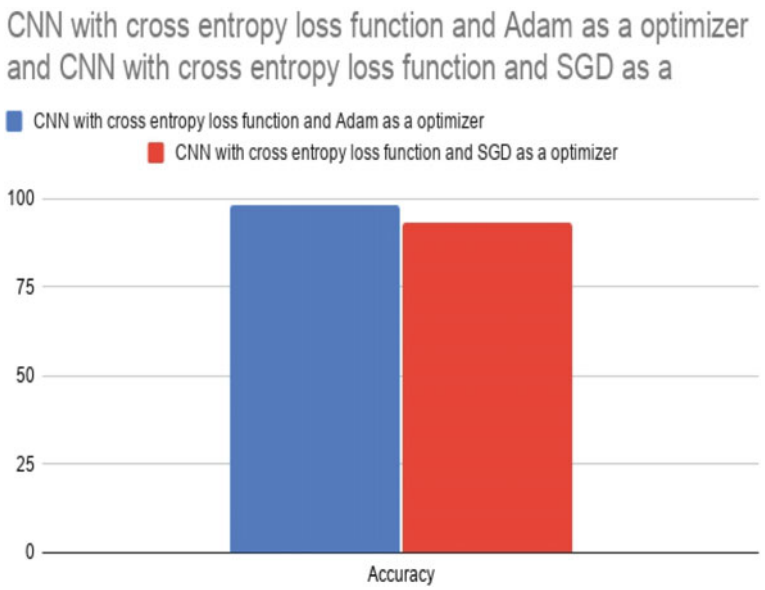


Fig. 4 Accuracy comparison of sign language recognition model

with other people. If we consider this, it can solve a whole big problem in our society in the upcoming future with ease. In the present work, there is a possibility of improvement of accuracy of sign recognition by utilizing other loss functions, optimizers, and classifiers.

5 Conclusion

Other researchers are using heavy gadget which is costly and cannot be afforded by poor people, whereas in this research model normal hand has been used without any gadget. So, there is no need to buy any accessories, which makes our model cheaper as compared to others. In deep neural network techniques, this paper used CNN to classify the 26 alphabets from A to Z in ASL for the recognition of sign language over the data set. In this research, the input is an image of 128 pixels and then application of convolutional and other layers to extract its feature. Here, the paper takes two different types of optimizer which are used to compare the accuracy of the model, in which the Adam optimizer with categorical cross-entropy loss as a loss function gave the better accuracy of 98% as compared to the other optimizer, that is, SGD, with same loss function which gave the accuracy of 93%.

References

1. V. Subedha et al., Sign language recognition to aid physically challenged using opencv and CNN. IRJMETS **3**(4), (2021)
2. https://peda.net/id/08f8c4a8511
3. M. Nguyen et al., Sign language recognition from digital videos using deep learning methods. Geometry Vision **1386**, 108–118 (2021)
4. S.G.M. Chavaan, Implementation of hand gesture recognition system to aid deaf-dumb people. Adv. Signal Data Process. LNEE **703**, 12 (2021)
5. J.W. Smith, S. Thiagarajan, R. Willis, Y. Makris, M. Torlak, Improved static hand gesture classification on deep convolutional neural networks using novel sterile training technique (2021). https://doi.org/10.1109/ACCESS.2021.3051454
6. http://www-i6.informatik.rwth-aachen.de/~dreuw/database.php
7. B. Shi et al., Finger spelling detection in American sign language. *Computer Vision and Pattern Recognition, Computer Science*, Cornell University, Submitted on 3rd April 2021
8. V.S.M.S. KartikKonjeti et al., Sign language to text conversion using deep learning. in *Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems*, vol 145. (Springer, Singapore, 2021)
9. Y. Le Cun, B. Boser et al, Handwritten digit recognition with a back-propagation network. (AT&T Bell Laboratories, Holmdel, N. J. 07733,1989)
10. T. Goswami et al., CNN model for american sign language recognition. ICCCE, LNEE **698**, 12 (2020)
11. C.K.M. Lee et al., American sign language recognition and training method with recurrent neural network. Expert Syst. Appl. **167**(1) (2021)
12. K. Jemimah,Recognition of handwritten characters based on deep learning with tensorflow. Int. Res. J. Eng. Technol. (IRJET) **06**(09), (2019)
13. V. Kasinathan et al., Sign language translation system using convolutional neural networks approach. in *Advances in Mechatronics, Manufacturing and Mechanical Engineering*, 06 August (2020), pp. 161–171
14. D. Bhavna et al., Hand sign recognition using CNN. IJPAS **17**(3), 314–321 (2021)

Covid Waste Management Using IoT: A Smart Framework



Mitra Tithi Dey and Punyasha Chatterjee

Abstract The influence of Covid-19 is reshaping our daily life. Along with protecting lives, management of contaminated covid wastes is very essential to reduce environmental and human health risks. Inappropriate management of covid wastes can cause serious possibilities of disease transmission to health workers, waste pickers, patients, and the community in general through spreading of Corona virus. Poor management of these infected wastes has created huge problems in healthcare waste handling as the amount of waste generated due to pandemic is excessively large. In this paper, we have presented an Internet of Things(IoT)-based smart framework for covid waste management. We have proposed two types of smart covid waste bins here, one for collecting covid wastes for home isolated patients and other for covid medical wastes, generated from hospitals/nursing homes, etc. These intelligent bins can capture waste information automatically by attached sensors, and the collected data is sent wirelessly to remote municipality server for further analysis. Municipality officials can take decisions such as number of bins to be deployed, at which time intervals wastes are to be cleared, etc., based on those information. The proposed framework minimizes the human interaction with the covid waste and restricts the spreading of virus.

Keywords IoT · Covid-19 pandemic · Covid waste management · Smart Covid Waste Bin · Sensors · Patient Tracking App · Household Covid Waste · Medical Covid waste · Automatic waste segregation

1 Introduction

Trash management is the steps and acts required to manage garbage starting from its formation to dumping [1]. It consists of collection, transfer, treatment, and dumping of wastes. It also requires monitoring the steps of total trash management. The essential reasons for waste management includes recycling materials, maintaining health

M. T. Dey (✉)
Netaji Nagar Day College, Kolkata, India

P. Chatterjee
School of Mobile Computing and Communication, Jadavpur University, Kolkata, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_88

of local citizens, controlling pollution, etc. In some cases, improperly managed trash can effect human health severely. With an unprecedented surge of Covid-19 contamination rate and lockdown situation, a lot of unsafe wastes are generated daily from each infected person and are increasing day by day [2]. Conventional ways like incineration have been outdated, and there is an immense pressure for handling Covid wastes that the waste management offcials are currently facing. Alongside, one time-use plastic items and personal protective equipment (PPEs) also bring a new hazardous PPE pollution [3] in the environment.

In most of the existing waste management systems, a city collection service travels a predefined route on a regular basis and empties trash bins and recycles receptacles. The fixed nature of this system is highly resource-intensive and involves excessive human intervention. This includes serious risks of virus transmission to the waste collectors, patients, health workers, and the community in case of handling Covid wastes. With the help of Internet of Things(IoT), smart waste management solutions [4, 5] have been evolving in smart cities. The main component of this system is smart garbage bin (SGB) [6, 7]. Generally, SGBs are battery-powered, and a SGB contains sensing, communication, and processing units. The sensing unit consists of different sensors to measure waste status. These data are sent to remote municipality server wirelessly for further processing. A microcontroller is required to run all these operations.

As per the literature survey, unfortunately there is no specific smart solution for managing Covid wastes till now. In this paper, we have proposed a novel covid waste management framework using IoT. Also, we propose architectures of two specific SGBs for deploying in covid medical centres and residences of home isolation patients. The paper is organized as follows: Sect. 2 explores the existing works carried out in this field, Sect. 3 describes the proposed smart covid waste management framework, and Sect. 4 represents the conclusion and future scopes.

2 Related Work

Authors in [8] discuss the different healthcare solid waste management strategies practiced in different countries, the challenges faced, and the possible solutions during the Covid-19 pandemic. In [9], a prospective scenario of the current waste generation, possible management options, and future implications of various types of wastes throughout the pandemic period have been presented. They also propose some approaches towards a better waste management service with viable consideration for the waste workers during this pandemic. Authors in [10] discussed the handling of solid and liquid biomedical covid wastes generated from hospitals, laboratories, and quarantine centres. Authors of [11] critically evaluate the implications of the preventative and protective measures adopted against Covid-19 for the generation of the hospitality sector's food and plastic wastes. The paper proposes potential strategies to aid in the management of these wastes in a post-pandemic world. All these works propose some manual waste handling approaches which is undesirable in the

management of Covid wastes, as human contact with the waste may spread the virus even more. Author in [12] discusses about the smart trash management approaches for post Covid-19 scenario in Japan. A multi-benefit self-driving mobility system is proposed here. Use of robotic arms in waste treatment along with remote controlled waste incineration services will take on more importance for achieving automated contactless service. They are focussing on mainly post-pandemic scenario, but not discussed about any smart infrastructure for the present situation.

In this paper, we are proposing an IoT-based smart framework for Covid waste management which can mitigate the challenges of present situation. We also propose two different SGBs for deploying in covid medical centres and residences of home isolation patients.

3 Proposed Smart Covid Waste Management Framework

According to the Association of Cities and Regions for sustainable Resource management [13], this ongoing global pandemic caused by corona virus produces challenges for municipal trash management actions. Healthcare centers, hospitals, nursing and elderly homes, and similar facilities are the most impacted zones by covid. Also, when recycling the covid affected garbage, it needs to be dumped separately so that there are safe 'waiting periods' for materials. So, a smart waste management will help to handle the covid waste more efficiently than the traditional waste management system.

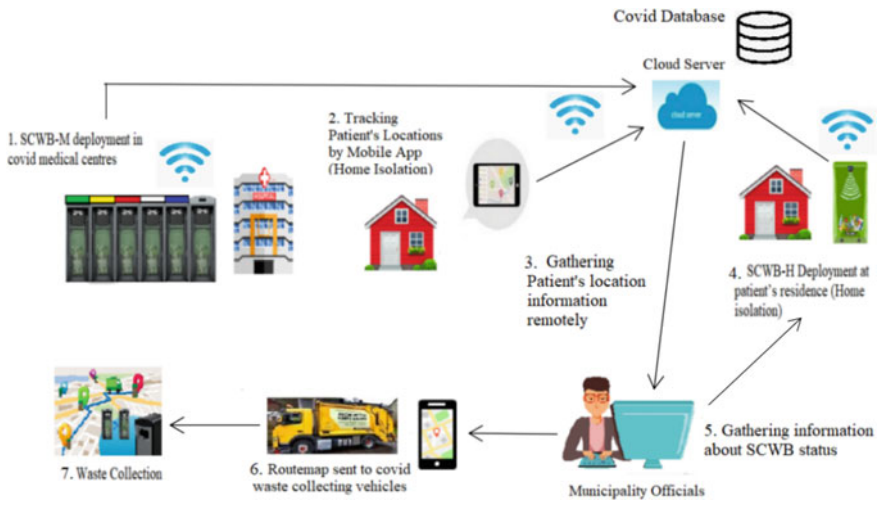


Fig. 1 Smart Covid Waste Management Framework

Figure 1 shows the framework of our proposed smart Covid waste management system. In this framework, we have proposed two kinds of SGBs: *Smart Covid Waste Bin-Medical or SCWB-M* for deploying at covid medical centres (like hospitals/nursing homes/safe homes/diagnostic units/isolation centres etc.) to collect covid medical wastes and *SCWB-Household or SCWB-H* for deploying at the residences of covid patient's for home isolation cases. In the next subsection, we will illustrate the detailed architecture of two types of *SCWB*s and the description of the individual events, presented in this framework.

*3.1 Smart Covid Waste Bin (*SCWB*) Structure*

Here, we are introducing two types of *SCWB*s because the types of wastes are different in case of Covid household wastes and Covid medical wastes. Generally, household Covid wastes contain regular municipal solid wastes like food scarp, clothing, masks, sanitizer, oxygen cans, bottles, product packaging etc., but medical wastes contain needles, cotton swabs, PPE kit, gloves, face-shields, urine bags, syringes, tubing, intravenous tubes and sets, catheters, broken or rejected and contaminated glass like medicine vials, ampoules, etc. It is vital to segregate all medical scrap materials at the point of generation, properly treated and safely disposed because medical wastes contain potentially dangerous micro organisms that can infect patients, healthcare staffs and citizens.

3.1.1 Structure of *SCWB-H* :

- Sensors: Load sensor (to detect waste weight) [7], Infrared sensor (to detect waste level) [7], gas sensor [4] (to detect poisonous gas emission inside bin), flame sensor [14](to detect fire inside bins. For example, if there is a fire inside the bin, then disposed oxygen cans or disposed sanitizer bottles can catch it easily.)
- Communication unit: LoRaWan [15]; LoRaWan is a wide-range, low-powered communication module, which provides energy-efficient communication for battery powered *SCWB*s.
- Microcontrollers: Arduino [16]

Figure 2 shows the structure of *SCWB-H*.

3.1.2 Structure of *SCWB-M*

SCWB-M allows waste segregation. It contains six containers for different types of medical wastes. We have used general standard for medical waste segregation, while determining the colour of these different containers [17].

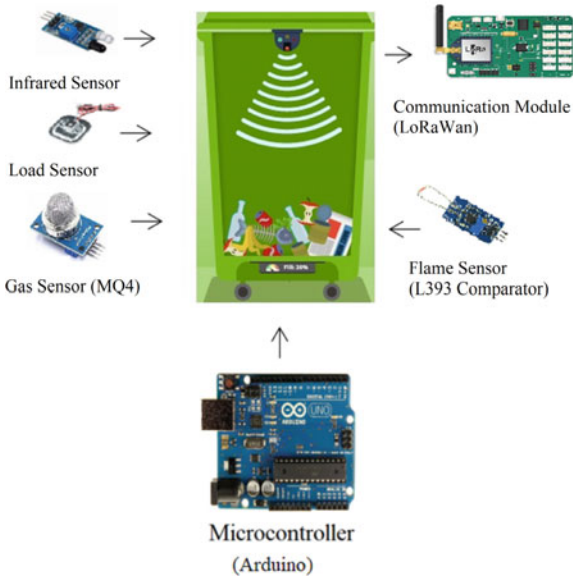


Fig. 2 Proposed structure of *SCWB-H*

- Green container: For bio-degradable wastes (covid food scraps, paper tissues, paper packaging, etc.)
- Yellow container: For mostly contaminated wastes (plaster casts, dressings, cotton swabs, blood components of patients, bags containing residual or discarded blood, body parts, human tissues, testing kits, discarded medicines, etc.)
- Red container: For recyclable wastes (tubing, intravenous tubes and sets, PPE kits, etc.)
- White container: For metal objects (sharp wastes like needles, scalpels, blades, scissors, etc.)
- Blue container: For glassware materials (broken/discarded glass objects like medicine vials/ampoules, syringes, tubes, etc.)
- Grey container: Non-categorized wastes (users unaware of the waste type).

The *SCWB-M* can be operated by a mobile app [18], through which authorized users can select specific waste types. Depending upon the chosen option, lid of the appropriate container is opened, so that users can put the medical wastes in designated bins. If no suitable container is found to put a specific type of waste or user is unable to categorize the waste, he opts for grey container. It makes the system totally contactless. Grey container allows automatic waste segregation [4, 19]. Inside the grey container, a conveyor belt is embedded, near to which some specific sensors (plastic sensor [19], metal sensor [20] and glass sensors [19]) are attached in series to identify diferent types of wastes. All the containers are attached with weight, level, gas and flame sensors. Proposed structure of *SCWB-M* is shown in Fig. 3.

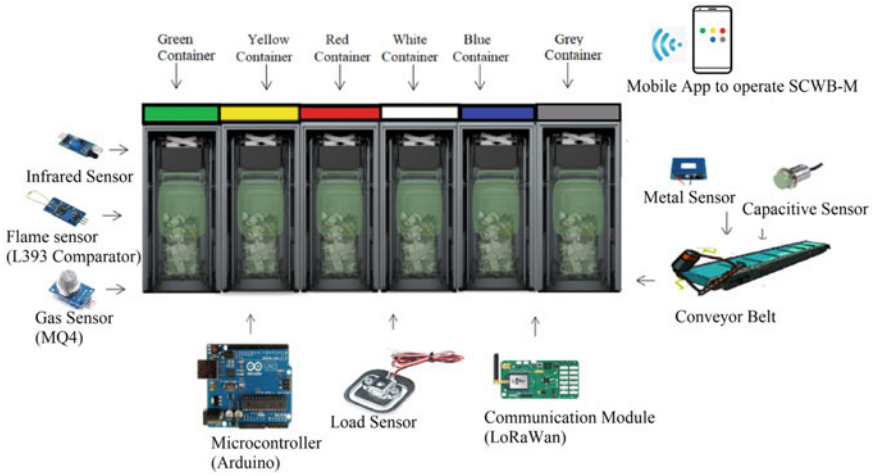


Fig. 3 Proposed structure of *SCWB-M*

3.2 Sequence of Activities in the Framework:

1. *SCWB-M* deployment in Covid medical centres: Initially, *SCWB-M*s are deployed in Covid medical centres such as Covid speciality hospitals, nursing homes, safe homes, isolation centres, health clinics, diagnostic centres, etc., so that all wastes related to Covid patients can be separately treated. This minimizes the chance of contamination from Covid wastes.

2. Tracking patients' locations by mobile app: With the help of Covid patient tracking apps like Arogya Setu[21], Unmaze app[22], etc., affected person can send useful information to the Goverment. All these huge data are stored in a Covid database in a cloud server.

3. Gathering Patients' location information from Covid database: Local municipality fetches required data from these Covid database and can identify the location of individual Covid patient. The density of Covid affected persons in a specific area, the contaminated zones, and Covid clusters can also be determined.

4. *SCWB-H* Deployment at patient's residence (Home isolation): For home quarantined persons, depending upon the patient density in a particular area, the required number of bins need to be deployed can be estimated. Then the physical deployment of the *SCWB-H*s are carried out as per requirement.

5. Gathering information about *SCWB* status: *SCWB*s send their Covid waste status to the cloud server of the remote municipality. After data analysis, different statistical information can be fetched like *SCWB* filling rate, in which areas and at what time of the day generally the *SCWB*s are filling fast, percentage of different types of wastes in various locations, number of emergency alerts(fire, gas) sent by

*SCWB*s per day, etc. Based on these infomartion, some strategic planning can be made for future decision making like in which areas more/less number of *SCWB*s are to be deployed, in which areas, cleaning is more frequently needed etc.

6. Routemap sent to Covid waste collecting vehicles: Once the *SCWB*s location and status information is known, then by executing shortest path algorithms, an optimal route can be calculated, which can traverse all the *SCWB*s with minimum delay and least fuel consumption. Also depending upon the waste volume in different *SCWB*s, the minimum number of vehicles can be engaged in this purpose. The routemap is sent to the vehicles through the mobile app of the drivers. In case of autonomous waste collecting vehicles, routemap is directly sent to the smart vehicles, avoiding human driver's engagement.

7. Waste Collection: With the use of GPS technology, drivers or the autonomous vehicles can easily locate *SCWB*'s position. Wastes are collected in a contactless way using robotic arms of the vehicles and are dumped in a separate area in dump-yard so that covid wastes do not mix with other wastes.

3.3 Advantages of the Proposed Framework

Our proposed system has several advantages over the manual covid waste management system:

- Automatic: Proposed system is automated, so less human involvement is required, which is very much essential in case of covid waste management to prevent spreading the virus.
- Real-time operation: Adverse situations (like waste overflow, presence of gas or flame within garbage bin etc.) are immidiately detected through sensors and reported to the municipality in real time, so that urgent actions can be taken.
- Seperate Bins: *SCWB-H* for households and *SCWB-M* for medical centres are proposed, considering the specific type of wastes.
- Resourse utilization: Less fuel consumption, minimum number of vehicles engaged for waste collection, least human intervention.
- Scalability: Bins can be added/removed as per requirement without hampering the operation of the whole system.
- Integrity: The proposed system can be easily integrated with the existing manual system.

4 Conclusion and Future Scope

In this paper, we present a novel IoT-based smart framework for Covid waste management. Two different types of smart Covid waste bins are featured here, one for home isolation patients and another for Covid medical centres. The system is auto-

mated, provides real-time action, and requires least human inervention, which are indispensible in Covid waste management scenario. However, it has some initial establisment cost for deploying the SCWBs. In future, we have a plan to develop prototypes of the proposed *SCWB*s and implement and test the whole framework in laboratory environment.

References

1. L. Melece, J. Brizga, R. Ernteins, Municipal waste management issues, in *17th International Scientific Conference Engineering for Rural Development* (2018), pp. 1245–1252
2. R.R. Kalantary, A. Jamshidi, M.M.G. Mofrad, A.J. Jafari, N. Heidari, S. Fallahizadeh, M.H. Arani, J. Torkashvand, Effect of covid-19 pandemic on medical waste management: a case study. J. Environ. Health Sci. Eng. (2021), pp. 1–6 (Springer)
3. R. Dean, Ppe: polluting planet earth. Br. Dental J. **229**(5), 267 (2020) (Nature Publishing Group)
4. S. Dubey, P. Singh, P. Yadav, K.K. Singh, Household waste management system using iot and machine learning, in *Procedia Computer Science*, vol. 167 (2020), pp. 1950–1959 (Elsevier)
5. M.T. Dey P. Chatterjee, Challenges and opportunities of smart solid waste management: a review, in *Horizons in Computer Science Research*, vol. 20, February 2021, pp. 61–109 (Nova Science Publishers)
6. M.T. Dey, P. Chatterjee, A. Chakrabarti, Smart waste monitoring using internet of things," in *Data Management, Analytics and Innovation*. Springer, Berlin (2021), pp. 419–433
7. A. Noiki, S.A. Afolalu, A.A. Abioye, C.A. Bolu, M.E. Emetere, Smart waste bin system: a review, in *IOP Conference Series: Earth and Environmental Science*, vol. 655, no. 1 (2021), p. 012036 (IOP Publishing)
8. A.K. Das, N. Islam, M. Billah, A. Sarker, Covid-19 pandemic and healthcare solid waste management strategy—a mini-review, in *Science of the Total Environment*. Elsevier (2021), p. 146220
9. M.S. Haque, S. Uddin, S.M. Sayem, K.M. Mohib, Coronavirus disease, (covid-19) induced waste scenario: a short overview. J. Environ. Chem. Eng. **2020**, 104660 (2019
10. S. Chand, C. Shastry, S. Hiremath, J.J. Joel, C. Krishnabhat, U.V. Mateti, Updates on biomedical waste management during covid-19: The indian scenario, in *Clinical Epidemiology and Global Health*. Elsevier (2021), p. 100715
11. V. Filimonau, The prospects of waste management in the hospitality sector post covid-19, in *Resources, Conservation and Recycling*, vol. 168. Elsevier (2021), p. 105272
12. H. Onoda, Smart approaches to waste management for post-covid-19 smart cities in japan, in *IET Smart Cities*, vol. 2, no. 2, IET (2020), pp. 89–94
13. https://www.acrplus.org/en/municipal-waste-management-covid-19
14. K.L. Raju, M.A. Hussain, U. Chandra, V.N. Phanendhra, D. Narendra, "Iot based dust bin monitoring system using node mcu, in *Innovations in Power and Advanced Computing Technologies (i-PACT)*, vol. 1. IEEE (2019), pp. 1–5
15. M. Cerchecci, F. Luti, A. Mecocci, S. Parrino, G. Peruzzi, A. Pozzebon, A low power iot sensor node architecture for waste management within smart cities context. Sensors **18**, 1282 (2018)
16. A.S. Wijaya, Z. Zainuddin, M. Niswar, Design a smart waste bin for smart waste management, in *2017 5th International Conference on Instrumentation, Control, and Automation (ICA)*, IEEE (2017), pp. 62–66
17. R.B.V. Gopinath, K. Subramanian, G. Thangarasu, V. Gopalkrishnan, K. Gopinath, New classification and colour code development for an efficient medical waste segregation, in *LIFE: International Journal of Health and Life-Sciences*, vol. 3, no. 2 (2017)

18. O. Taiwo, A.E. Ezugwu, N. Rana, M.A. Shafii, Smart home automation system using zigbee, bluetooth and arduino technologies, in *International Conference on Computational Science and Its Applications*. Springer, Berlin (2020), pp. 587–597
19. M. Rafeeq, Ateequrahman, S. Alam, Mikdad, Automation of plastic, metal and glass waste materials segregation using arduino in scrap industry, in *International Conference on Communication and Electronics Systems (ICCES)*. IEEE (2016), pp. 1–5
20. K. Devi, D. Dharini, L. Vandhana, Design of iot based garbage segregation for automatic smart trash bin using ni labview. Int. J. Innov. Technol. Exploring Eng. **8**(11), 725–729 (2019)
21. https://www.aarogyasetu.gov.in/
22. https://theprint.in/tech/india-is-using-at-least-19-apps-to-track-and-trace-covid-19-including-aarogya-setu/401459/

Phishing URL Detection and Vulnerability Assessment of Web Applications Using IVS Attributes with XAI



Vivek John Sudhakar, Srimathi Mahalingam, Vaman Venkatesh, and V. Vetriselvi

Abstract The number of cyber attacks which are carried out are increasing day by day and pose a serious threat worldwide. The most common methods of launching these attacks include delivering phishing URLs and exploiting built in vulnerabilities present in web applications due to faulty and error prone code. Most of these vulnerabilities occur due to the absence of input user data validation before processing. This paper presents solutions to identify phishing URLs and input validation and sanitization based vulnerabilities, i.e., SQL injection, Cross Site Scripting, and File Inclusion in PHP code using machine learning models, after the extraction of certain IVS attributes.

Keywords Machine learning · Prediction models · Sql injection · Cross site scripting · File inclusion · Phishing

1 Introduction

A cyber attack can maliciously disable computers, steal data or use a breached computer as a launch point for further attacks. Given a URL, the types of attacks that can be carried out on systems or users are by phishing and through the exploitation of vulnerabilities present in the source code of the web application. These vulnerabilities are mostly present in the data processing part of the source code.

Phishing is carried out by fooling or forcing a user to click on a malicious phishing URL that can steal information or redirect the user to a malicious page. Thus, detecting if a given site is phishing or not given just the URL is very important. A vulnerability is a backdoor for attackers. Most vulnerabilities present in web applications are due to user data being trusted and absence of Input Validation and Sensitization (IVS) of data before processing by the developer. This lets malicious users input data of their choice which can then be used to break or misuse the system. According to OWASP's Top Ten Project [1], the most common and serious web vulnerabilities that

V. J. Sudhakar (✉) · S. Mahalingam · V. Venkatesh · V. Vetriselvi
College of Engineering Guindy, Anna University, Chennai, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_89

occur due to the absence of input data validation are SQL Injection (SQLI), Cross Site Scripting (XSS), and File Inclusion (FI). Thus, IVS based attributes should be able to act as indicators for detection of all these vulnerabilities. Early detection methods against these vulnerabilities are critical in securing web applications, users and preventing losses.

Machine learning algorithms have become increasingly better in pattern recognition and classification tasks. Thus, researching the use of ML in automating the detection of these kinds of threats is crucial for improving security. Most data processing and input data validation in a web application occur in server side code. Since PHP is the most common server side programming language used, our paper focuses on PHP source code. Thus the 3 objectives for this paper are:

- Efficient detection of phishing sites using only the URL and dealing with tiny URLs.
- Detecting presence of certain vulnerabilities present in web application PHP source code using IVS attributes, instead of only taint analysis.
- Explaining the predictions and model learned.

The remainder of this paper is organized as follows: We introduce the related work in Sect. 2. In Sect. 3, the proposed system is explained with a detailed design of each module. Our implementation details and results are analyzed in Sect. 4. Finally, we conclude this paper in Sect. 5.

2 Related Work

Several approaches have focused on detecting phishing URLs and web application vulnerabilities in a given source code. However, it is still an active research area in web application security and researchers are trying to incorporate Machine Learning to help in these tasks. The advances of machine learning in pattern detection make it worthwhile in researching its use in vulnerability detection. A detailed literature survey has been carried out to explore the existing work and identify the research gap, its limitations, and future work.

Traditionally blacklists have been used to try and filter malicious URLs. But this process is time consuming as a database lookup has to be carried out every time and is only effective if the URL has already been added to the blacklist. To increase the effectiveness and the efficiency of this process, Apoorva Joshi et al. [2] propose using Machine Learning in detecting malicious URLs. This approach extracts various lexical features from the URL such as the number of digits, etc., and uses them as input to a Machine learning model. Yang et al. [3] combine URL statistical features, web-page code features, and web-page text features along with character sequence features to classify URLs. However as the use of machine learning has increased in defensive security, there is a threat that malicious attackers could also make use of AI to improve their attacks. This was supported in [4] by Torroledo et al. where the authors developed an AI algorithm called 'DeepPhish' to enhance the threat actor's

human-generated URLs and produce AI-generated phishing URLs. To counter this new futuristic threat, Sameeni et al. [5] proposed a new system called 'PhishHaven 'which can detect AI-generated phishing URLs as well as deal with tiny- URLs. Alejandro Correa Bahnsen et al. [6] developed a Deep Learning model, in particular an RNN model with LSTM units to detect phishing URLs and obtained state of the art performance of around 98% and was the first paper to leverage the power of neural networks and in particular LSTM for such a task.

Among the vulnerabilities that hackers try to compromise in a web application, the most common are based on input validation and sanitization. Miguel Correia et al. [7] proposes a system to correct vulnerabilities in PHP code as well as return feedback to the programmer. It combines the use of taint analysis as well as data mining to reduce false positives. A limitation of it derives from the lack of formal specification of PHP. Miao et al. [8] conducted a survey and summarized the various exploitation and detection methods for XSS. They however only cover static analysis, dynamic analysis, and hybrid methods. Vignesh et al. [9] presented a paper where they use a combination of static and dynamic analysis to obtain certain input validation and sanitization (IVS) attributes, from which vulnerability predictors are built. The IVS attributes are passed through an ML model for vulnerability prediction. These IVS attributes are obtained after performing hybrid analysis and slicing on the program code. The program analysis is done based on the control flow graph, control dependence graph, and system dependence graph of a web program. In [10] by Kevin Zhang, an ML classifier is built to identify SQL injection vulnerabilities present in PHP code. In this approach, however, the classifier models were trained and evaluated using input validation and sanitization features extracted directly from source code files. The IVS attributes used in this paper identified if in-built input validation or sanitization functions present in PHP were called by the developer.

Explainable AI (XAI) refers to methods and techniques in the application of artificial intelligence technology (AI) such that the results of the solution can be understood by humans. Marino et al. [11] are concerned with designing interfaces that help users to understand the decisions made by a trained machine learning model. It presents an approach to generate explanations for incorrect classifications made by data-driven Intrusion Detection Systems. An adversarial approach is used to find the minimum modifications required to correctly classify a given set of misclassified samples. In [12], Paul Rad et al. explored why XAI is important, several facets of XAI, and categorized them in respect of their scope, methodology, usage, and nature towards explaining deep neural network algorithms. Their findings showed that considerable research in XAI is focused on model-agnostic post-hoc explainability algorithms due to their easier integration and wider reach. Amina Adadi et al. [13] took inspiration from how we assimilate and familiarize ourselves with new topics. They focused on the Five W's and How (What, Who, When, Why, Where, and How) to cover all aspects related to XAI. Findings showed that XAI is not just a labcoat research field ad that its impact is spanning a large range of application domains. It has then been concluded that considerable effort will be required in the future to tackle the challenges and open issues with XAI.

Most research in this area uses taint analysis combined with dynamic analyses for vulnerability detection. This paper researches the use of ML on IVS attributes extracted from source code for prediction. This is the first attempt in using xgboost models for vulnerability identification. It also focuses on 3 injection based vulnerabilities, i.e., SQLI, XSS, and FI, and tries to find IVS attributes that will help in their identification. Further, phishing URL classification using only the given URL is combined to help solve all possible attack vectors which can be associated with a given URL.

3 Proposed System

The working of our system, which counters the threats which can be exploited from a given URL is explained. The proposed system consists of two main components, a phishing URL detector, and a source code vulnerability detector as shown in Fig. 1.

An URL is given as input to the phishing URL detector. The system first checks to see if the URL is currently live by sending it a GET request. The response is analyzed and if it is an active URL a check is done to test if it is a shortened URL. This helps in dealing with tiny URLs. The expanded URL is obtained if it is shortened and the relevant whois information is displayed to the user. The URL is then passed through a Support Vector Machine (SVM) classifier to detect if it is a phishing URL or not. If it is not a phishing URL, a sitemap of the URL is generated. The user can choose the URL of any PHP website for vulnerability assessment or enter another URL. The PHP source code is read and displayed along with its AST (Abstract Syntax Tree). The AST is analyzed and the tainted symbols present in the code are displayed to the user. The source code is then read and a set of attributes are extracted to check for

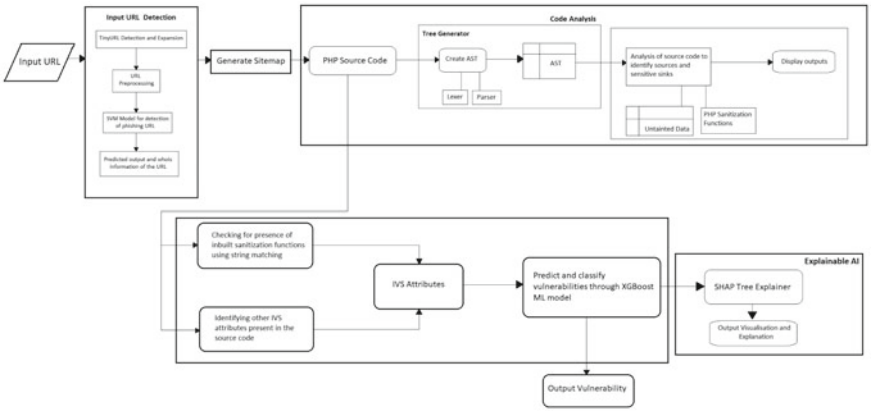


Fig. 1 Overall architecture

the presence of Input validation and sanitization (IVS) based vulnerabilities (XSS, SQLI, FI) in the code.

These IVS attributes are a combination of detecting the presence of certain PHP built-in functions, which validate or sanitize data and other general attributes. They are then sent through three separate XGBoost models each trained to detect the presence of XSS, SQLI, and FI. Due to the imbalance of the dataset used to train the models, over sampling was employed for the SQLI model. Explainable AI is then used with the help of the SHAP package to provide feature weights and importance of the models to the user as well as visualize the prediction explanation's with a force plot.

URL Analysis In this module, the system takes a URL as an input. Since many phishing URLs are short lived, the system checks if the URL still exists or not. If the URL still exists, a request is sent to the URL. Based on the response, the system determines if it is a shortened URL and if it is, the expanded URL is displayed along with the related information about the site such as the created date and whois information. The expanded URL is then preprocessed and vectorized before passing through an SVM Machine Learning model which predicts if it is a phishing URL or not. The detection is done by only using the URL and the code of the URL's web page is not accessed at all.

Code Analysis The PHP file containing source code is given as input. An abstract syntax tree of the program is constructed using Node JS and is displayed to the user. Static analysis is performed on the AST and the possible entry points of user data in the program, i.e., tainted variables present in the code are identified and displayed to the user along with its line number. This allows the user to know all possible sources present in the code.

Obtaining IVS Attributes The source code file is used as input for this module. String matching is done on the code to identify the presence of certain attributes which are to be checked in the code. These attributes are termed IVS attributes and are extracted as binary values of either 1 or 0 indicating presence or absence respectively. An array of these values corresponding to each attribute are then sent as input to the machine learning models.

Predicting vulnerabilities and applying xAI The array of attributes from the previous module are sent to the three XGBoost models to predict the presence of vulnerabilities. Three XGBoost models are trained on the training data, each to detect the presence of a particular vulnerability (SQLI, XSS, and FI). The predictions are displayed as probabilities to the user and are also sent to the explainable AI interface to make the results more interpretable.

The user is given the option to visualize the feature weights which have been learned by each model. This gives the user a rough idea of what attributes can lead to the model predicting the presence of vulnerabilities. The prediction outputs can also be visualized to gain insights using a force plot in the SHAP package. SHAP Values (SHapley Additive exPlanations) break down a prediction to show the impact each feature has on the output.

4 Results Analysis

The URL analysis consisting of tiny URL detection and phishing detection is implemented in python. The URL is tokenized, stemmed, and converted into count vectors after preprocessing. The phishing detection model is an SVM implemented using sklearn and was trained on a dataset consisting of 549346 URLs.

In the second module, once the source code of the PHP file is read, it's AST is constructed using the php-parser tool available in Node JS. The tainted symbols are identified by parsing the AST using PHP and displayed. The extraction of the IVS attributes are also implemented in PHP by parsing through the code and performing string matching. The attributes used are a combination of general and vulnerability specific attributes which are shown in Table 1. Three XGBoost models are then built and trained on these attributes to detect the vulnerabilities.

The SARD PHP vulnerability test suite [14] was used to compile our dataset of vulnerable and safe PHP code samples with SQLI, XSS, and FI. Due to the class imbalance present in the SQLI class, oversampling is used. Finally, a PHP script was written to extract the IVS attributes from these code samples and compile them into a CSV file to be used for training and testing the ML models.

The machine learning models built for URL phishing detection as well as vulnerability detection on source code are evaluated using metrics like confusion matrix, precision, recall, accuracy, ROC curves, and log loss curves.

A confusion matrix is used to help visualize the results. Precision and recall are used together along with accuracy to give an overall view of the performance of our system. Log-loss is an appropriate performance measure when your model output is the probability of a binary outcome (Fig. 3).

Phishing URL Detection Model:

In the Phishing URL Detection Model we obtained a precision of **99.6%**, recall of **99.4%** and accuracy of **99.4%**.

As it can be observed from Fig. 2, the number of true positives and true negatives are very close to the total number of samples. Thus the accuracy, precision, and recall

Table 1 IVS attributes used

S.No	IVS Attribute	S.No	IVS Attribute
1	is_cookie_file_accessed	9	Is_filter_var
2	is_db_accessed	10	Is_filter_input
3	is_session_accessed	11	Is_preg_replace
4	String_to_num_conv	12	Is_preg_match
5	accessing_file_path	13	Is_addslashes
6	Limit_str_len_func	14	Is_trim
7	Is_htmlspecialchars	15	Is_bind_param
8	Is_htmlentities	16	Is_mysql_escape_string
		17	Is_user_inp_accessed

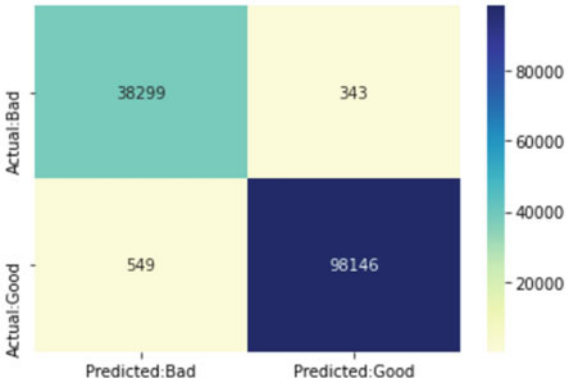


Fig. 2 Phishing URL detection model confusion matrix

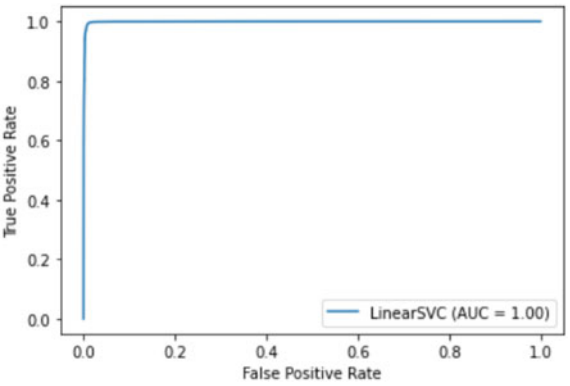


Fig. 3 ROC curve

are all greater than 0.99, i.e., more than 99% which indicates that the model performs very well.

Source code vulnerability detection models (XGBoost): **Cross Site Scripting (XSS)**:

In the detection of XSS in source code, our model only gives an accuracy of 0.67. This can be explained by the fact that the attributes are chosen turn out to give very sparse values, which can be seen in Fig. 4 are used to train the model. This can be made better by adding more attributes specific to XSS.

In this model, a precision of **61%**, recall of **62%** and an accuracy of **67%** was obtained respectively.

The log loss on the test dataset, as seen in Fig. 5, is higher than in the train set. This may indicate the presence of overfitting. However, the values plateau early on. It also shows that after approximately 20 epochs no improvement is made and the model can be stopped earlier.

SQL Injection (SQLi): As it can be seen from Fig. 6, the precision and recall of the model trained to detect SQLI in source code is low because the number of false positives (FP) and false negatives (FN) is much greater than the true positives (TP).

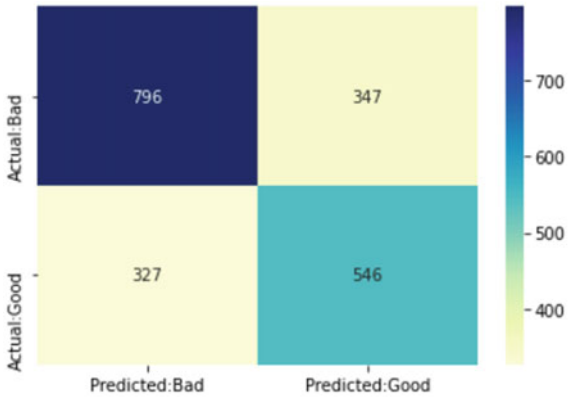


Fig. 4 XSS confusion matrix

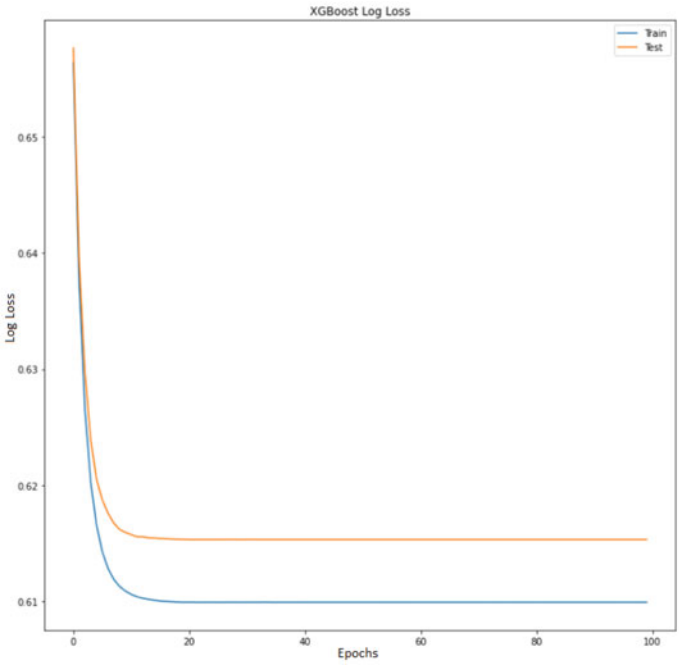


Fig. 5 XSS log loss

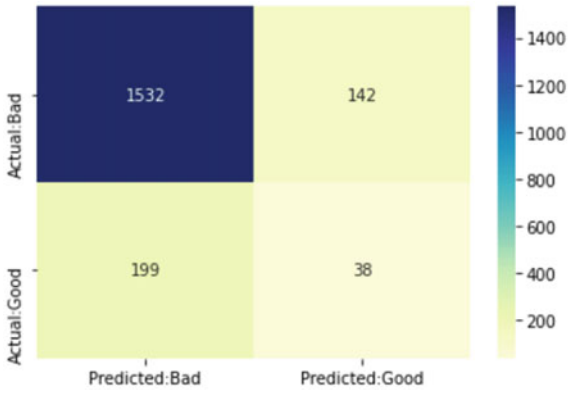


Fig. 6 SQLI confusion matrix

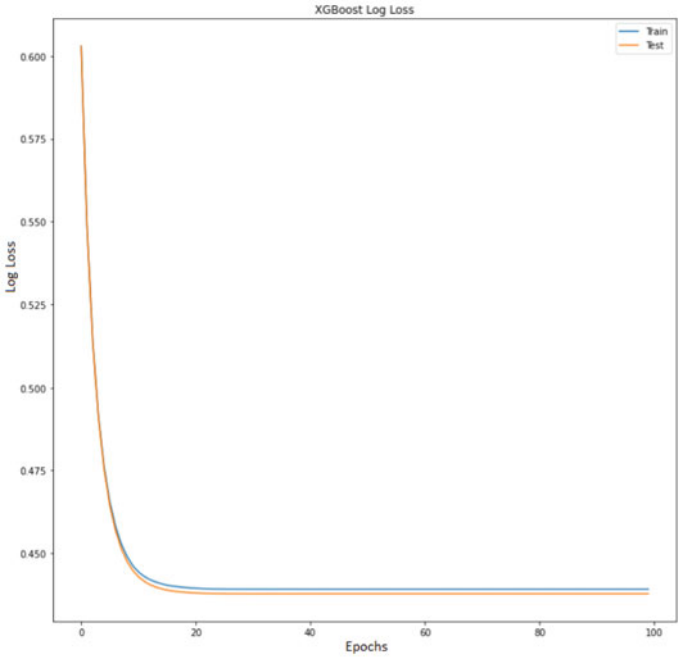


Fig. 7 SQLI log loss

This is due to the large class imbalance in the dataset. However the accuracy is comparatively higher with 82% (Fig. 7).

The SQL injection model gave a precision of **21%**, recall of **16%** and an accuracy of **82%**.

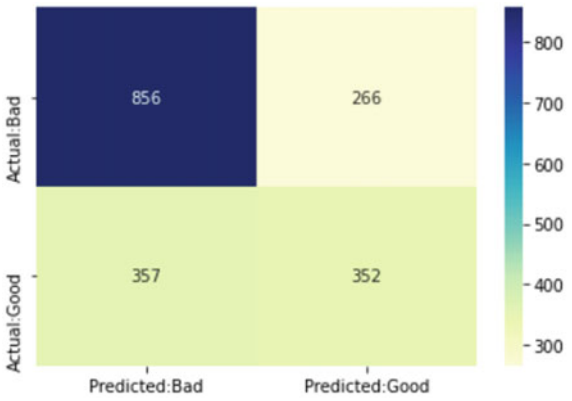


Fig. 8 FI confusion matrix

For SQLI, both the values are extremely close to each other and lower than the other two models. The values fall and then plateau for the majority of the epochs. No overfitting seems to occur. However, no new training occurs after a few epochs. This could be due to the use of a sparse dataset.

File Inclusion (FI): The recall is around 0.5 because the number of false negatives is almost equal to the true positives as shown in Fig. 8. This implies that only half the actual vulnerabilities are identified correctly. To improve this, more FI specific attributes could be included.

Here, we observed a precision of **57%**, recall of **50%** and accuracy of **66%** respectively (Fig. 9).

For FI, the log loss values on the test dataset are lower than on the train dataset. This implies that although the model generalizes better, there is not enough information in the training set. There is an absence of overfitting. The values plateau here too, but are higher than for the SQLI model.

5 Conclusion and Future Work

We have evaluated our system based on metrics such as precision, accuracy, and recall; as well as monitored XGBoost's performance using a log loss curve. Although the accuracy of SQLI is 82

In terms of how the system may be improved in the future, the accuracy of the model can be increased by optimizing XGBoost or using better models. The datasets we used were created from the SARD dataset and were not optimal. On using a better dataset, better results should be seen. More IVS attributes can be added after dataset inspection as there are other functions that may sanitize the code that we might have overlooked, such as type casting operations.

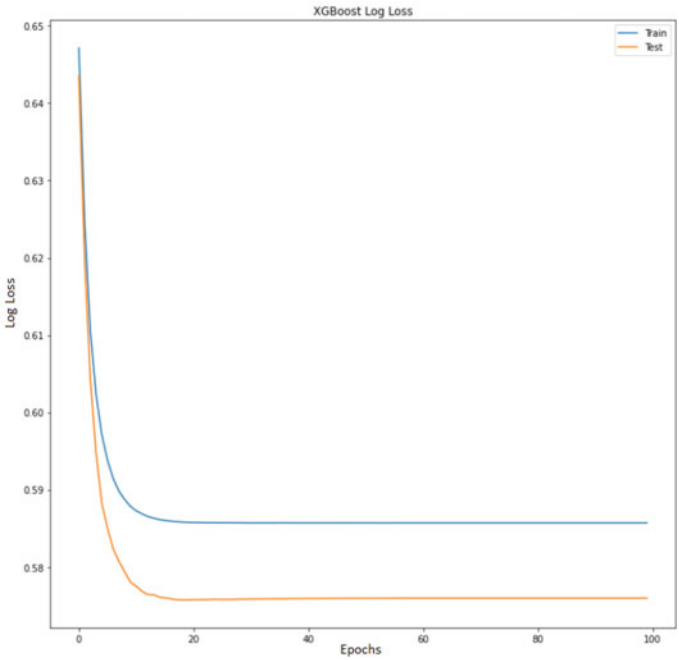


Fig. 9 FI log loss

References

1. OWASP, The open web application security project http://www.owasp.org
2. A. Joshi, L. Lloyd, P. Westin, S. Seethapathy, Using lexical features for malicious URL detection—a machine learning approach, 2019 [Online]. Available: http://arxiv.org/abs/1910.06277
3. P. Yang, G. Zhao, P. Zeng, Phishing website detection based on multidimensional features driven by deep learning. IEEE Access 1–1 (2019)
4. A.C. Bahnsen, I. Torroledo, D. Camacho, S. Villegas, DeepPhish: simulating malicious AI (2018)
5. M. Sameen, K. Han, S.O. Hwang, PhishHaven" an efficient real-time AI phishing URLs detection system. IEEE Access **8**, 83425–83443 (2020)
6. A.C. Bahnsen, E.C. Bohorquez, S. Villegas, J. Vargas, F.A. González, Classifying phishing URLs using recurrent neural networks, in *2017 APWG Symposium on Electronic Crime Research (eCrime)* (2017), pp. 1–8
7. I. Medeiros, N. Neves, M. Correia, Detecting and removing web application vulnerabilities with static analysis and data mining. IEEE Trans. Reliab. **65**(1), 54–69 (2016)
8. M. Liu, B. Zhang, W. Chen, X. Zhang, A survey of exploitation and detection methods of XSS vulnerabilities. IEEE Access 1–1 (2019)
9. M. Vignesh, K. Kumar, Web application vulnerability prediction using machine learning. Int. J. Sci. Eng. Rese. **8**
10. K. Zhang, A machine learning based approach to identify SQL injection vulnerabilities, in *2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE)* (2019), pp. 1286–1288

11. D.L. Marino, C.S. Wickramasinghe, M. Manic, An adversarial approach for explainable AI in intrusion detection systems, in *IECON 2018—44th Annual Conference of the IEEE Industrial Electronics Society*, pp 3237–3243
12. A. Das, P. Rad, Opportunities and challenges in explainable artificial intelligence (XAI): a survey (2020)
13. A. Adadi, M. Berrada, Peeking inside the black-box: a survey on explainable artificial intelligence (XAI). IEEE Access, 1–1 (2018)
14. N.I. of Standards and Technology, Software assurance dataset project. [Online]. Available: https://samate.nist.gov/SARD/index.php

A Smart Device for Power Theft Detection



A. Jagadeesh, S. Praneeth Varma, A. Sreeja, and I. Mamatha

Abstract Increasing efficiency in the power sector does not occur only by improving the technical losses. Although many thoughtful improvisations like power line communication, advanced metering infrastructure have been done to decrease non-technical losses, but not at large scale. The idea of this work is to attain accurate detection of power theft without installing expensive meters. Proposed system combines and improvises conventional consumer meter and smart meter features to design and construct a small-scaled advanced metering infrastructure and enhancing it to detect and mitigate different methods of power theft with reliable communication using a cloud platform rather than GSM network. Proposed system is capable of locating the theft area and controls the illegal load usage, by placing a separate energy meter. The observer meter energy reading is compared with the value at the main energy meter situated at the individual subscriber's premises. If any difference occurs between both meter readings, an error signal is sent to concerned authority stating power theft at particular location. ThingSpeak is handed down as a platform for cloud services and data transfer and IFTTT (if this then that), and an interface for sending an alert message without a GSM module is used. The proposed system is simulated on a Proteus platform for apartment models and household models and tested successfully.

Keywords Smart meter · Power theft · ThingSpeak · Advanced metering infrastructure · Observer meter

1 Introduction

In India, there is a huge amount of power loss due to ineffective usage of appliances such as appliances being ON indefinitely. Effective and smart way of managing the loads at home utilities through IoT-enabled energy management system has been

A. Jagadeesh (✉) · S. P. Varma · A. Sreeja · I. Mamatha
Department of Electrical and Electronics Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Bengaluru, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_90

proposed in, and, where, the consumer is controlled not to exceed power consumption beyond a preset value[1, 2]. Electricity is a key input for accelerating economic growth. Due to power theft, there is a huge revenue loss [3, 4]. This revenue loss outcome shortens and fails to adopt newer technologies or solutions that are economical [5, 6]. Power theft is a major issue even in the most advanced and efficient power systems. AMR and AMI are two such advancements, AMR stands for Automatic Meter Reading where the billing person is eliminated and energy is always compared with the main meter [7]. Advanced Metering Infrastructure which works full-fledged in smart grids. But upgrading existing digital meters to AMR or AMI might not be that easy and economical at present [8].

One possible way of reducing power theft is through prepaid metering, where users will be given a fixed amount of units at first and when consumption is done the power is cut off [9]. In this way, revenue losses and power theft are at check, and there is a constant look on consumption [10]. These meters are basically built using the GSM networks, where it incorporates the facility of prepaid metering system and remote load control [11]. This system can be further enhanced to detect the different methods of power theft such as shorting the phase line, disconnecting the neutral line, whole meter bypassing and tampering [11–13]. One of the most common methods of theft is damaging the meter by opening it and tampering which results in the meter showing wrong/less consumption [14, 15]. To avert it, two lever switches are kept on either side of the meter which normally reads high signals [16, 17]. If any disturbance occurs or any bypassing occurs, there will be zero voltage detection, and the concerned person is notified of theft.

1.1 Control of Power Theft Using Observer Meter

Generally, these sorts of theft cannot be detected completely by a single meter at home. To detect such recorded theft, an observer meter is used in the system. The observer meter keeps the record of energy consumption of all meters (summation of all households) at regular time periods [18, 19].

This work focuses on complete power theft detection by installing prepaid meters or advanced metering infrastructure (AMI). These various methods of theft can be alleviated by using an observer meter or secondary meter. It is done by comparing consumer meter and observer meter using a cloud platform which will be again a substitute for GSM which makes work less complex and more reliable. This idea has been simulated using Proteus software. Organization of the paper has been done in four subsections. Section 2 discusses the proposed system and system specifications. Section 3 focuses on the methodology/flowchart and results. Section 4 concludes the present work.

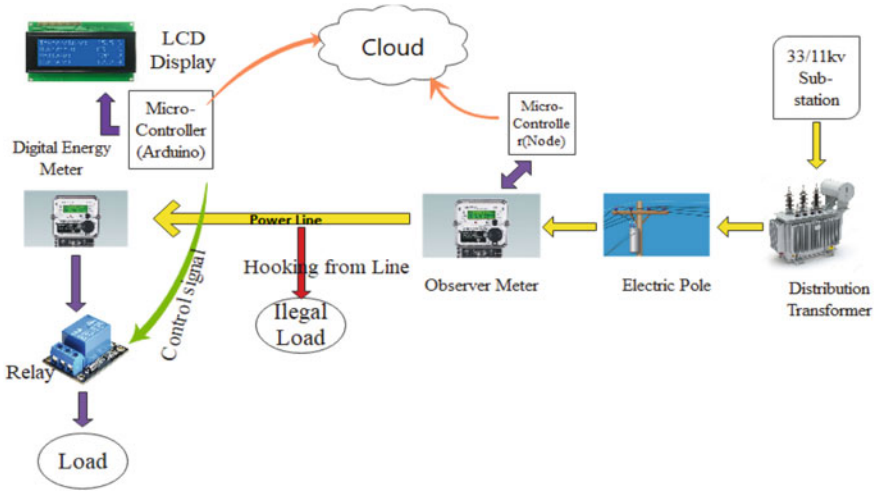


Fig. 1 Block diagram

2 Block Diagram and System Specification

2.1 Block Diagram

The work proposes the plan and development of a microcontroller-based anti-theft electric energy metering system. This system enables control of electricity theft using observer meter and remote power disconnection in case of energy theft. The block diagram of the proposed system is shown in Fig. 1. Proteus simulation software was used to model the system. The system provides high performance in power monitoring by placing another meter (observer meter) near the electric pole which monitors the units consumed from the electric pole/transformer. The observer meter and house-side meter are synchronized in a way during a mismatch in between these two meters an alert message will be sent.

2.2 System Specifications

Electric energy meter shown in Fig. 2 computes the consumption of energy by individual customers as it gauges the electrical energy devoured by a home. Here, voltage and current sensors are used to sense the voltage and current, and the power and energy consumption is calculated using PIC microcontroller. Energy meter readings are communicated wirelessly which are done using ThingSpeak platform. ThingSpeak is an Internet of Things (IoT) application and API to store and retrieve data from things using the HTTP protocol over the Internet or via a local area network

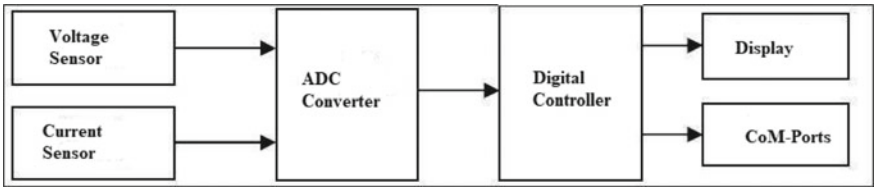


Fig. 2 Energy meter with voltage and current sensors



Fig. 3 ThingSpeak channels and fields

(LAN). ThingSpeak provides instant views of data sent to fields from the devices as shown in Fig. 3.

3 Methodology and Results

The entire development of the system is broken down into two sections. First section contains design of digital energy meter using Arduino, and current sensor for a lamp and resistive load for computing energy consumption. The algorithm for designing the Arduino as the digital meter is explained in the flowchart and simulation. The second section is the identification of power theft. The observer meter technique used in this paper is illustrated. This section deals with ThingSpeak cloud platform for unit data monitoring between the two meters. Discrepancy observed in the fields of ThingSpeak platform activates the IFTTT interface for sending the alert message to the lineman.

The Arduino/Node MCU is used as digital energy meter. It starts with defining the analog read pins to configure as ADC modules. ADC of Arduino is a 10-bit module. The resolution of the module is formulated in (1).

$$\text{Resolution} = \frac{1}{2^{10}} = \frac{1}{1024} \tag{1}$$

For sensing the load current, the current sensor is connected to the ADC of Arduino. Vout is calculated from ADC reading using (2).

$$V_{\text{out}} = \frac{\text{adc values} \times 5000\,\text{mV}}{\text{resolution}} \tag{2}$$

Further, the current measured is obtained using (3) where a scaling factor for the sensor from the data sheet is 66 mv/A.

$$\text{Current} = \frac{V_{\text{out}}}{\text{scaling factor}} \tag{3}$$

The input is fed into the controller on each instance up to 200 values. This helps in recording the maximum current of alternating current at every cycle of 50 Hz. Then follows with the calculation of the root mean square) value of the alternating current. RMS current is calculated using (4) of the current sensor.

$$\text{RMS Current} = \frac{\text{current(Im)}}{\sqrt{2}} = I_{\text{rms}} = \text{Im} \times 0.707 \tag{4}$$

Units consumed for the load (3 lamps and 1 Motor) as shown in Fig. 4a is calculated as below:

Current Recorded = 1.79 A, RMS Power = $V \times I = 230 \times 1.79 = 411.7$ W

1Unit = 1 kWH

$\therefore$ Units consumed for 0.4117 kW load turned for 3 min is 0.02units.

3.1 Simulation Results

Simulation diagram of the single-phase energy meter using Arduino is shown in Fig. 4. Units are calculated as below:

$$\text{Units Consumed} = \text{Power(kW)} * \text{Time}$$

LCD screen displays the RMS current passing through the load and number of units consumed and the maximum load (power) switched in the house. Virtual terminal displays the RMS current and the consumption of units for a particular load at regular intervals of time.

Radial distribution is used for simulating the Transmission network. Individual house and apartment model as in Fig. 4b displays the radial distribution network of 11 kV and 55 MW from Generation station is stepped up to 132 kV for long

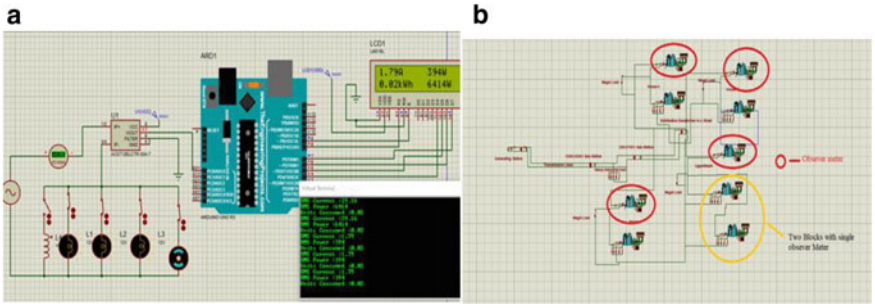


Fig. 4 **a** Simulation of single-phase energy meter using Arduino. **b** Radial distribution network with apartment and individual houses model

transmission and then stepped down to 33 kV and given as input to 33/11 kV substation for stepping down to 11 kV.

The 11 kV feeders from sub-station are connected to the poles at the road side which is connected to the primary side of the distribuion transformer (11 kV/230 V single phase). Observer meter is placed at the incoming supply line of house and apartment. Individual house model with illegal load by directly tapping from the line is recorded by the observer meter as shown in Fig. 5. The readings of the meters for apartment model are shown in virtual terminals as in Fig. 6.

The observer meter reading which is cumulative reading of all meters and household meter is recorded using the Arduino, and the difference in readings of both the meters is highlighted. Whenever there is a power theft, there will be a difference in observer meter reading when compared to sum of the individual household meter readings which are indicated in the LCD screen and also in the virtual terminals which trigger the alert. The three terminals in Fig. 7 represent the apartment model. Left most terminal is for block 1, middle one is for block 2, and third one is observer meter. Any variation in the readings is analyzed in the ThingSpeak cloud and reverted back for the immediate action. The units in both household meter and observer meter of individual house model are displayed in virtual terminal as shown in Fig. 8.

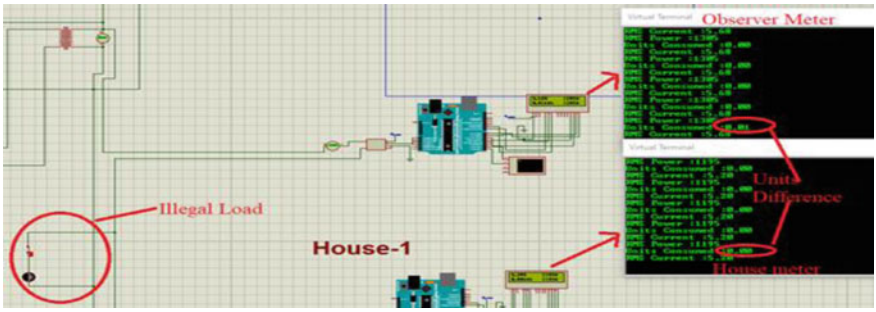


Fig. 5 Individual house with illegal load

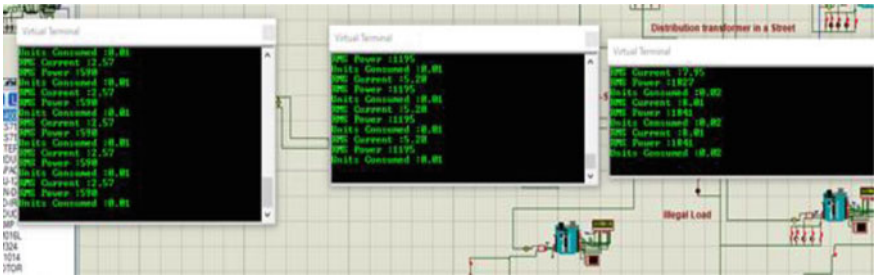


Fig. 6 Virtual terminals of observer meter and household meter for apartment model

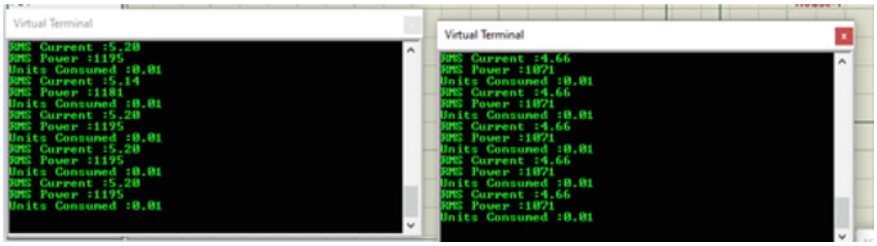


Fig. 7 Virtual terminals of observer meter and household meter for individual house model



Fig. 8 Household meter sending units' data to the cloud

3.2 Communication and Alert Notification

The units and the current data are being recorded by the controllers present at the household and the observer meter in a radial distribution network. This data have to be cross verified for any difference in the readings. The data in two controllers are to be accumulated in a platform for further analysis.

ThingSpeak platform (wireless) serves the purpose of a cloud platform and enables communication securely using the Hypertext Transfer Protocol (HTTP). Using this, the current/units at the particular instant of time is being calculated by the Arduino

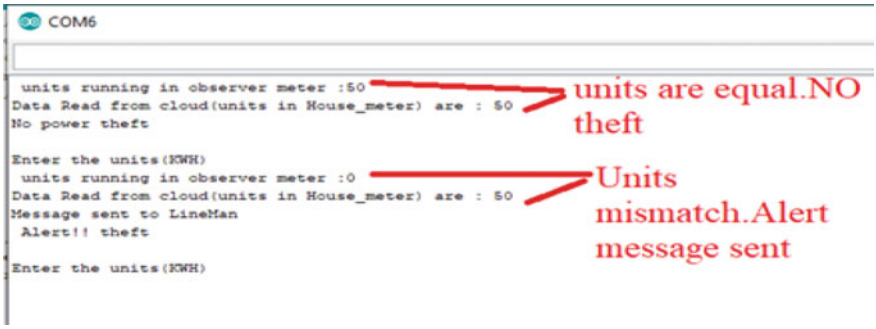


Fig. 9 Observer meter receiving (reading) the unit's data sent by the house meter

which is configured as the digital energy meter. The communication part for identifying the theft is executed using the physical node module (resembles energy meter) connected to laptop which is accompanied by all the sensors which behave as household meter. Units of household meter and observer meter are entered using the serial monitor as seen in Fig. 8, and running units are sent to cloud. The node microcontroller is configured to connect with the Wifi router, and then, the household algorithm is uploaded. Using the serial monitor, the units can be entered into the controller with the help of API keys. The data are successfully sent to the respective channels fields as indicated in Fig. 8. The controller present at the observer meter fetches the data sent by the house meter and compares the units running in the meter at the current instant of time with the units read from the field (house meter) in Fig. 9. The controller sends an alert message if there is any deviation in the meter units using the if this then that (IFTTT) interface as shown in Fig. 10.

If this then that (IFTTT) is an interface which helps to create own applets. The applet can be monitored from the mobile application. The basic block of the applet is the if statement that is, if the statement is true, then the block is executed. This IFTTT interface helps to connect to the applet via the HTTP request method and eliminates the need of the GSM module for sending the alert message. Using the IFTTT applets, the message block of the phone is triggered.

4 Conclusion

In this work, design and simulation of a system for power theft detection and alerting mechanism has been carried out. The theft is detected by using an observer meter and comparing the readings with that of the house hold meter. Consumer side energy is calculated and will be matched continuously in regular intervals with the units supplied by the transformer. The units in observer side meter on transformer are noted and matched with consumer side energy meter as this can alert us if theft happens. Apartment model and individual house model have been designed in Proteus and

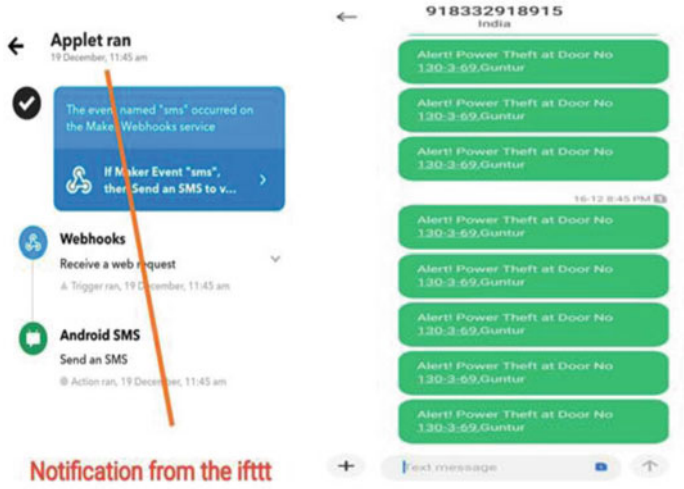


Fig. 10 Observer meter receiving (reading) the unit's data sent by the house meter

are simulated and tested successfully. An illegal load at the poles of the distribution transformer is connected, and the observer meter present at the pole captures the reading of the pole hooking by reading extra units to that of the house meter. The unit data are being wirelessly sent to the observer meter for further analysis, and an alert message is sent to the concerned person. In this way, all the power theft methods are at check. This can be done in various ways such as by integrating GSM with microcontroller, but this all requires additional circuit and code. In the proposed work, ThingSpeak platform using IFTTT interface for alert notification is used in an optimal way. The concept of prepaid metering to overcome power theft problem is planned for future work.

References

1. N.S. Shibu, A. Hanumanthiah, S.S. Rohith, C.H. Yaswanth, P.H. Krishna, J.V.S. Pavan, Development of IoT enabled smart energy meter with remote load management, in *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)* (IEEE, 2018), pp. 1–4
2. R.D. Arya Devi, T.S. Subeesh, M.V. Ramesh, Design and implementation of user interactive wireless smart home energy management system, in *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (IEEE, 2013), pp.626–631
3. Z. Tir, Y. Xue, Y. Shu, H. Yang, S. Liu, and Y. Xu, Electric theft behavior detection method based on power customer data analysis, in *2020 International Wireless Communications and Mobile Computing (IWCMC)* (IEEE, 2020), pp. 99–102

4. M.B. Shahid, M.O. Shahid, H. Tariq, S. Saleem, Design and development of an efficient power theft detection and prevention system through consumer load profiling, in *2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)* (IEEE, 2019), pp. 1–6
5. A.S. Metering, S. Visalatchi, K.K. Sandeep, Smart energy metering and power theft control using arduino & GSM, in *2017 2nd International Conference for Convergence in Technology (I2CT)* (IEEE, 2017), pp. 858–961
6. W.N. Mohammad, A. Barua, M.A. Arafat, A smart prepaid energy metering system to control electricity theft, in *2013 International Conference on Power, Energy and Control (ICPEC)* (IEEE, 2013), pp. 562–565
7. M. Saad, M.F. Tariq, A. Nawaz, M.Y. Jamal, Theft detection based GSM prepaid electricity system, in *2017 3rd IEEE International Conference on Control Science and Systems Engineering (ICCSSE)* (IEEE, 2017), pp. 435–438
8. S. Yip, C. Tan, W. Tan, M. Gan, A.A. Bakar, Energy theft and defective meters detection in AMI using linear regression, in *2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)* (IEEE, 2017), pp. 1–6
9. A. Annaswamy, IEEE vision for smart grid control: 2030 and beyond roadmap, in *IEEE Vision for Smart Grid Control: 2030 and Beyond Roadmap* (2013), pp. 1–12
10. X. Jin, Y. Zhang, X. Wang, Strategy and coordinated development of strong and smart grid, in *IEEE PES Innovative Smart Grid Technologies* (IEEE, 2012), pp. 1–4
11. R.B. Colak, S. Sagiroglu, The effects of the smart grid system on the national grids, in *2020 8th International Conference on Smart Grid (icSmartGrid)* (IEEE, 2020), pp. 122–126
12. J. Navani, N. Sharma, S. Sonal, Technical and non-technical losses in power system and its economic consequence in Indian economy. Int. J. Electr. Comput. Sci. Eng. **1**(2), 757–761 (2012)
13. P. Chandel, T. Thakur, B.A. Sawle, R. Sharma, Power theft: major cause of non-technical losses in Indian distribution sector, in *2016 IEEE 7th Power India International Conference (PIICON)* (IEEE, 2016), pp. 1–6
14. V. Paruchuri, S. Dubey, An approach to determine non-technical energy losses in India, in *2012 14th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South)* (IEEE, 2012), pp. 111–115
15. R.D. Arya Devi, M.V. Ramesh, Power theft detection in microgrids, in *4th International Conference on Smart Cities and Green ICT Systems* (IEEE, 2015), pp. 1–8
16. U.H. Priya, P. Jyothi, V.V.S.S. Phanipavan, K. Deepa, A. Jain, Energy conservation strategy for dc motor load applications. in *Recent trends and advances in artificial intelligence and Internet of Things*. ed. by V.E. Balas, R. Kumar, R. Srivastava, (Springer, Cham, 2020), pp. 177–186
17. P.N. Seema, V. Deepa, M.G. Nair, Consumer level intelligence in a smart micro-grid, in *2016 International Conference on Energy Efficient Technologies for Sustainability (ICEETS)* (IEEE, 2016), pp.320–324
18. T. Ranjith, P. Sivraj, Futuristic smart energy meter-design based on embedded perspective, in *2nd International Conference on Intelligent Computing and Control Systems, ICICCS 2018* (IEEE, 2019), pp. 1379–1384
19. A.R. Baskaran, S. Aravindh, S.A.M. Varman, E. Prabhu, Smart energy meter for power grid using fuzzy logic, in *2017 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2017* (IEEE, 2017), pp.1–5

Correction to: The 3D Facemask Recognition: Minimization for Spreading COVID-19 and Enhance Security



Ashish Sharma, Ara Miran, and Zanyar Rzgar Ahmed

Correction to:
Chapter "The 3D Facemask Recognition: Minimization for Spreading COVID-19 and Enhance Security" in:
S. Fong et al. (eds.), ICT Analysis and Applications,
Lecture Notes in Networks and Systems 314,
https://doi.org/10.1007/978-981-16-5655-2_60

In the original version of the book, the affiliations of authors "Ashish Sharma, Ara Miran, Zanyar Rzgar Ahmed" have been updated in the Chapter "The 3D Facemask Recognition: Minimization for Spreading COVID-19 and Enhance Security". The chapter and book have been updated with the changes.

The updated version of this chapter can be found at
https://doi.org/10.1007/978-981-16-5655-2_60

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes
in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2_91

Author Index

A
Aalam, Zunaid
Agarwal, Parul
Aggarwal, Palvi
Ahmed, Zanyar Rzgar
Aital, Padmanabha
Akshara, M.
Alam, M. Afshar
Alam, Tanvir
Ali, Hala S.
Aman, Muhammad Naveed
Ambat, Shaneth
Aradhya, Sumalatha
Arora, Pallavi
Atmaja, Eduardus Hardika Sandy
Avhad, Om

B
Bajpai, Gaurav
Bajpai, Rishabh
Balyan, Vipin
Bandopadhyay, Dipankan
Bandyopadhyay, Atri
Bartakke, Isha
Bedse, Gayatri
Bhat, Aishwarya
Bhatia, Gresha
Bhavsar, Kaushal
Biswas, Partho Sharothi
Bokhari, Hasnain
Bylaiah, Sushma

C
Chakravarthi, Veena S.
Chandak, Yug
Chandrachud, S.
Chatterjee, Punyasha
Chaudhry, Shehzad Ashraf
Chettri, Sarat Kr.
Chingmuankim
Choudhari, Kshitija

D
Dakshayani, R.
Dani, Rakesh
Debnath, Dipankar
Deshpande, Shilpa Shrikant
Devi, M. Nirmala
Dey, Mitra Tithi
Dhananjaya, M. K.
Divya, I.
Divya, S.
D'souza, Jordan
Dutta, Ajoy Krishna
Dutt, Himanshu
Dutt, Varun
Dwivedi, Rajendra Kumar

F
Fatima, Nida
Fernandes, Salil

G
Gangurde, Tejashri
Gawai, Mayuresh
Gayathri, D. Smitha
Geetha, P.

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

S. Fong et al. (eds.), *ICT Analysis and Applications*, Lecture Notes in Networks and Systems 314, https://doi.org/10.1007/978-981-16-5655-2

Gehlot, Neha
Ghorpade, Divya
Gireesh Kumar, T.
Goel, Lavika
Goel, Mridula
Goel, Supriya
Golhar, Yogesh
Gomes, Elroy
Gour, Tryambak
Govekar, Prasad
Gowda, Leena
Gupta, Aman
Guzman, Daryl G.

H
Hajare, Aparna
Halder, Rupesh
Hitimana, Eric
Hong, Dung Luu

I
Iftekhar, Bisma
Indrabalan, Uma Bharathi

J
Jadhav, Bharat T.
Jadhav, Dipti
Jagadeesh, A.
Jagdale, Akshta
Jain, Prakhyath
Jain, Sapna
Jangirala, Srinivas
Jante, Shubham
Jha, Pratyush
Jha, Vinod
Jindal, Rajni
John, Ansamma
Jose, Fredin

K
Kahn, Mohamed Tariq
Kalamdani, Sudharm
Kamble, Nisha N.
Kamble, Satish
Kandpal, Meetu
Kapoor, Jitaksh
Karthika, S.
Katakwar, Harsh
Kattikaren, Anthony
Kaur, Amritpal
Kaur, Baljeet
Kaur, Satnam
Kayalvizhi, Jayavel
Kesavan, Sridharan
Khairnar, Hitendra
Khandekar, Shreya
Khedekar, Ankita
Khedkar, Vijayshri
Kolhe, Kishor
Koli, Rahul
Korade, Shraddha
Kowshik Hurshan, S.
Kshirsagar, Manali
Kudalkar, Gauri
Kulkarni, Gayatri Laxmikant
Kulkarni, Harshita
Kulkarni, Rutuja
Kulkarni, Shreya
Kumar, Ayush
Kumar, Darshita
Kumar, Gourav
Kumar, Sanjeev
Kumar, Sumeet
Kusumawati, Reni Diah

L
Lamkhade, Aarya
Lohani, Rupal
Lotya, Sahil
Luna, Armand Christopher

M
Maghanoy, Joie Ann W.
Magpantay, Abraham
Mahalingam, Srimathi
Majhi, Swagatam
Mali, Shankar M.
Malladi, Kishore
Mamatha, I.
Manasa, Koduganti Sai Sudha
Manna, Asmita
Maqbool, Zahid
Mazumdar, Chandan
McQuire, Lee
Mehta, Nishchay
Mekala, Priyanka
Milton, T.
Miran, Ara
Mohammed Faisal, A.
More, Nitin S.
More, Sharmila S.

Moyeenudin, H. M.
Mufti, Tabish
Mukhopadhyaya, Keka
Mukhopadhyay, Indraneel
Musabe, Richard
Muttath, Abhishek

N
Nagaraja, K. V.
Nag, K. Sowmya
Nair, Lakshmi Suresh
Narain, Bhawna
Navaneethakrishnan, R.
Naveen, S.

O
Obaid, Ahmed J.
Oswari, Teddy

P
Pal, Sanjeeb
Pandey, Bhavna
Pandey, Muskan
Pandey, Shambhavi
Parikh, Satyen M.
Parimi, Sashikala
Pascua, Nicole John
Patel, Hiral R.
Patel, Pooja
Patel, Sina
Pathak, Tejashree
Patil, C. H.
Patil, Rajesh
Patil, Sangita Bapu
Patil, Shankargoud
Patil, Sharanagouda S.
Paul, Bonani
Pawar, Shruti
Payasi, R. P.
Paz, Joan Stephen D.
Phadke, Mayank
Policarpio, Dale R.
Pothina, Harshini
Potnis, Madhura Shekhar
Prabhushetty, Kappargaon S.
Prakash, Shelly
Prasad, N. S. R.
Prateek, M.
Priyatharishini, M.

R
Rabbi, Md Forhad
Rajani, P. K.
Raj, Shubham
Rameshkumar, R.
Rani, K. R. Usha
Ranjith, V.
Raut, Rohit
Rawal, Yashwant Singh
Reddy, S. Sai Satyanarayana
Ribu Hassini, S.
Roy, Pratik
Roy, Sonal Mobar

S
Sachan, Deshna
Sachdev, Karan
Saha, Samapty
Sahukar, P. Yamini
Sairaam, H.
Sankangoudar, Keerti Umesh
Saroha, Kriti
Sathe, Sanjyot Kedar
Sawant, Padmaja
Sengupta, Anirban
Shahab, Saima
Shah, Krishna
Shanthi, M. B.
Sharma, Anshul
Sharma, Ashish
Sharma, Sunil
Shedole, Seema
Sheeja, S.
Shinde, Pooja
Shirsath, Swati
Sibomana, Louis
Singh, Arindam
Singh, Mayank
Singh, Prerna
Singh, R. B.
Singh, Sheenu
Singh, Shivam
Sinha, Arushi
Sohail, Shahab Saquib
So, John Paul
Sonawane, Kavita
Sornam, Madasamy
Sowmya, K.
Sowndarya, S.
Sreeja, A.
Sridevi, R.
Srinidhi, S.

Srinuvas, B.
Srivastava, Rashmi
Srivastava, Shashi Kant
Sudhakar, Vivek John
Suresh, Kuralayanapalya Puttahonnappa
Suresh, L. Padma
Suresh, Vidya
Sutar, Swapnil
Suthar, Amit B.
Swaminathan, J. N.

T
Tamilarasi, A.
Tanuja, V.
Tasnim, Jarin
Teixeira, Marcio Andrey
Thakur, Divyansh
Thamby, Babitha
Thara, S.
Thorat, Chhanam
Tidke, Sonali Kothari
Tiwari, Harshita
Tiwari, Vaibhav
Trajano, Christian
Trivedi, Bhushan
Tugaonkar, Purva Govind

U
Uppal, Aakansha

V
Van, Hoa Doan
Vankadara, Ram
Varghese, Eric George
Varma, S. Praneeth
Vasagam, Swamiraj Nithiyanantha
Vats, Prashant
Veer, Aditya
Venkatesh, Vaman
Verma, Deepika Chandra
Verma, K. S.
Vetriselvi, V.
Vharkate, Minakshi
Vidyasagar, I.
Vyas, Vaibhav

W
Waghmare, L. M.
Wangikar, Vaishal

X
Xuan, Van Luu

Y
Yadav, Janardan Krishna
Yanga, Ansley D.
Yusnitasari, Tristyanti