2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) | 978-1-6654-1262-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICECCME52200.2021.9591011

# Dark Web: A Facilitator of Crime

Rhiannon Cole
*Department of Computer Science*
*East Stroudsburg University of Pennsylvania*
East Stroudsburg, PA, USA
Email: rcole5@live.esu.edu

Shadman Latif
*Department of Computer Science*
*American International University*
Dhaka, Bangladesh
Email: sadmanxp@gmail.com

Md Minhaz Chowdhury
*Department of Computer Science*
*East Stroudsburg University of Pennsylvania*
East Stroudsburg, PA, USA
Email: mchowdhur1@esu.edu

***Abstract*—Anonymity is easy to accomplish on the internet through VPNs and onion routing. Anonymity can be good if you are trying to view pro-democracy content or western news in China, however, not all people are gaining internet anonymity for altruistic reasons. Internet crime has been on the rise and web browsers like TOR are helping to facilitate internet crime. The dark web is helping create online marketplaces for illicit goods, and these web criminals are harder to catch and with globalization even harder to prosecute. Law enforcement has been struggling to curtail internet crime due to a knowledge barrier and further jurisdictional problems once perpetrators are apprehended. The goal of this paper is to analyze how the dark web works, secures anonymity, and how it helps protect criminals and allow illegal marketplaces. It also aims to discuss different strategies law enforcement has been adapting to crack down on internet crime.**

***Keywords—anonymity, blockchain, bitcoin, dark web, deep web, digital currency, onion routing, TCP/IP, TOR.***

## I. Introduction

The internet has helped to connect the world globally in a way many never thought possible. This increased globalization has led to user-to-user global marketplaces like eBay to grow in prominence. It has never been easier to find rare and unique goods online through these global services. However, the internet also is host to many more illicit marketplaces. Websites that deal in arms, drugs, trafficking, information (social security numbers and credit card numbers), and malicious malware. These websites are not as accessible as typing in the domain www.ebay.com, however, to those that know how to use VPNs (Virtual Private Network) and onion routing it is not difficult to find them.

The use of VPNs and onion routing can make you functionally anonymous online. That anonymity makes it easy to commit internet crimes with a relatively low risk of being caught by law enforcement. Law enforcement struggles dealing with internet crimes due to how these sites secure anonymity and from a general lack of knowledge. These problems are compounded with jurisdictional problems that pop up when dealing with global crime organizations.

These online marketplaces are large safe havens for criminals. “In 2017 over 1.4 billion personal records were leaked over the dark web” [1]. A site for child pornography that was taken down in 2015 was discovered to have “200,000 members” [1]. These marketplaces and communities have large user bases and while operational help facilitate international crime.

This paper seeks to explain how the dark web works and secures anonymity online. It will analyze onion routing, specifically TOR (The Onion Router) and how its ease of use has helped make the dark web more mainstream. It will next explain how criminal activities and marketplaces thrive on the dark web. It will also address how these sales are kept anonymous through the TOR browser and digital currencies. If these marketplaces are so secure, how does law enforcement take these sites down? What are law enforcements strategies for cybercrime? Specifically analyzing the struggles that law enforcement faces when dealing with these crimes and how they get around the problem of anonymity.

The second section background will dive into what the dark web means and how it is accessed. Defining basic terminology and giving a basic overview of onion routing and TOR. The third section will be focused on onion routing and how it works. It will be more technical and will analyze the key features that make onion routing a successful way to secure anonymity. The fourth section transitions from the internet protocols that allow anonymity to how they are utilized by criminals. The fourth section will overview criminal activities that take place on the dark web. It will analyze the different illicit operations that have prospered on the dark web from silk road to playpen. As well as discussing digital currencies and why they are exclusively used for payment on these sites. The fifth section will discuss law enforcement strategies. What law enforcement is doing to catch internet crime and how global internet crime is prosecuted. The sixth section will be the conclusion which will tie together all the information presented on dark web crime and offer some introspective on how law enforcement can better crack down on it.

## II. Background

There is a difference between the deep web and the dark web. Deep web is the content of databases and services of the invisible part of the web that for a reason cannot be indexed by normal search engine used by everyone. The deep web is not all bad, but on the other hand, dark web a cyber

978-1-6654-1262-9/21/$31.00 ©2021 IEEE

underground word is the worst part of the deep web. The worst kind of hackers, gangsters, terrorists, pedophile as well as drug dealers can be found in the dark web. Most people don't get the difference between deep web and dark web. Both need to be accessed in a special way, but Dark web is far more dangerous.

This background section explains the basics of what the dark web is and how it is accessed. Along with explaining how cryptocurrencies work and their uses on the dark web.

### *A. Accessing the Darknet*

Criminal activities thrive on the dark web, but what is the dark web and how does it facilitate crime. The part of the internet that most people access daily is considered part of the surface web, websites that can be "found using search engines" [2]. Search engines can catalogue these websites with web crawlers. Websites that can "prevent traditional search engines from indexing them" [2] by putting measures in place to inhibit web crawlers are considered part of the deep web. An example might include the myESU portal which has a login required that prevents indexing. The dark web is an encrypted network and requires special software to be able to access it. On the darknet "websites found [there] are not indexed" [2] making it also a part of the deep web.

The dark web cannot be accessed as simply as surface websites. There is specialized software needed to access it safely. The most common ways people access the darknet is through private networks which will establish restrictions on their users to best secure anonymity. Other than privacy networks peer to peer networks like I2P are also a way to access the dark web. The most popular and well-known privacy network or anonymity network is "The Onion Router" or TOR as its better known. The TOR browser "was created by the U.S. Navy to allow for internet anonymity worldwide" [2]. With how popular TOR is and its ease of access the navy might have outdone themselves. TOR is the most popular way to access the darknet due to how accessible it is. TOR is free to download and can be easily downloaded from your regular browser and be set up in minutes after it is finished downloading.

TOR is easy to set up and very accessible, but why do people use it. The obvious answer is of course for anonymity most people using TOR want the protection a privacy network supplies. There are also ".onion" web addresses that can only be accessed through TOR. Typically, a VPN, virtual private network, is used in conjunction with TOR to better secure the user. Now imagine you are a criminal using TOR to access the darknet's illicit marketplaces how would you pay for goods and services without sacrificing your anonymity. The answer comes in the form of cryptocurrencies and the blockchain.

### *B. Understanding Cryptocurrency and the blockchain*

The blockchain in its simplest explanation is a ledger or as its better classified a "distributed ledger technology (DLT)" [3]. The "blockchain is a public electronic ledger built around a P2P system that can be openly shared among disparate users to create an unchangeable record of transactions" [3]. A key word in that explanation is unchangeable record once new data is entered it is appended to the ledger and becomes another part of the chain. The most used cryptocurrency by far is bitcoin and it works by utilizing the blockchain. All bitcoin transactions are recorded in the blockchain, and a transaction is defined as "a transfer of value between Bitcoin wallets" [4]. Each person's bitcoin wallet has a unique and secret "private key or seed" [4] which is used to sign transactions from the owner's wallet. The signature also helps secure the transaction against unauthorized alterations. After a transaction is initiated, it will be finalized through mining. Mining is a process defined as "a distributed consensus system that is used to confirm pending transactions by including them in the block chain" [4]. Put more simply it makes sure to maintain the blockchains chronological order while also securing the networks' neutrality and getting different computers to agree on the state of the blockchain [4]. The nature of the blockchain makes it close to impossible for someone or a group of someone's to manipulate the blockchain and add things consecutively.

### *C. Bitcoin's Anonymity and Instability*

Purchases made through banks are tracked and regulated through the government. Digital currencies like bitcoin are not regulated which makes securing anonymity much easier. Recorded transactions through bitcoin would not be tied to the user, but to their private key. Bitcoin complicates the old law enforcement motto of following the money. A decentralized currency like bitcoin is great for anonymity, but not for stability. There is "no institution or government backing the value of bitcoin" [3]. The value of bitcoin can fluctuate quite aggressively and is subject to supply and demand. Recently bitcoin has maintained a value of more than 50,000 USD equal to a single bitcoin, in part due to a prop up from investors like Elon Musk. In the past bitcoin has dropped quickly from 40,000 USD highs back down to under 10,000 USD. A bitcoin wallet secures anonymity on the darknet, but outside of it its instability is not worth its risk.

For darknet transactions bitcoin is perfect, and similarly to TOR it is very easy for a person to setup. Bitcoin's website helps people choose a wallet that suits their needs and once its downloaded to their computer or phone they can begin buying bitcoins. At its current inflated rate most people will buy only the slightest percentage of a bitcoin. Due to bitcoin's instability bitcoin wallets can grow or shrink in comparison to USD. Bitcoin is a risky currency; however, it has its uses. Bitcoin is a good to use for "cross-border transactions" due to there being no exchange rates [5]. Depending on where you

live it may also be a more stable currency than your government backed currency. Bitcoin is a good currency for dark net transactions, but that is due to it being a good cryptocurrency in general.

## III. Analysis

This section will cover how onion routing works and how it differs from the TCP/IP protocol (Transmission Control Protocol/Internet Protocol). It will also seek to explain how TOR uses onion routing, and why it is so successful at maintaining anonymity. After covering how these services maintain anonymity the section will branch into misuse. Discussing how internet crime is facilitated on the dark web, and how law enforcement is handling this problem.

### *A. Onion Routing*

Onion routing replaces TCP/IP networks that are used for general Internet browsing. TCP/IP networks break everything into smaller packets which all look for the best route to where they are sent. Implementing TCP/IP into a more anonymous format would involve using a mix network with it. Mix networks were proposed by David Chaum utilizing a public key where "messages will conceptually be letters inside multiple envelopes" [6]. This illustration created by Ververis shows how mix networks work [6].

A mix network is slow and has delays. A message is sent to different nodes and passed on with only the sender and receiver knowing who the message is for. If someone were to watch the network, they would only see exchanges unless they had access to enough participating nodes to see the whole exchange. That scenario is very unlikely as there are far too many nodes to realistically watch. Due to the amount of transfers these networks are slow on purpose as it makes "time-based correlation attacks much harder" [6]. Now back to implementing a mix network with TCP/IP. All those small packets would then have to each go through a mix network. This is a slow process by design, and you would need all your packets to get to a location at similar times to reassemble. There is no realistic way to implement a mix network with the TCP/IP protocol. That is why onion routing was created.

Onion routing works by creating anonymous connections called circuits that work over a mix network. The onion routing system with the largest user base as previously stated is TOR (the onion router) which has "several thousands volunteer-operated nodes" [6] or more commonly called tor relays. These relays process traffic globally from millions of users. The TOR anonymity network processes all "TCP-based applications such as web browsing, email communication, secure shell, instant messaging, and chat services" [6]. A client chooses a path, and a circuit is made to complete that action. A circuit is made up of tor relays where each relay only knows the predecessor and the successor relays that make up the circuit. Traffic going through the circuit is "unwrapped by a symmetric key at each node" [6] before being sent to the next node. It is called onion routing because each node unwraps another layer and onions have layers. Each relay also maintains a transport layer security or TLS-encrypted connection to every other relay in the network which helps the client build circuits through the network. The symmetric keys used at each relay hop is the reason nodes cannot trace connections they help form.

The TOR networks onion routing helps ensure their users anonymity on web applications. The TOR network can help users gain access to information their country censures. It can also be used by criminals to hide illegal actions online. The TOR network is very good at maintaining their user's anonymity what people do with that anonymity is what troubles law enforcement.

### *B. Criminal Activity and Law Enforcement*

Accessing the Dark Web through the TOR browser allows users anonymity and with that anonymity many can misuse it to interact with illegal websites and marketplaces. Everyone has heard of the infamous dark web marketplace Silk Road where illegal goods from drug trafficking to arms deals occurred. After Silk Road was shut down other marketplaces filled its shoes from Agora to Alpha Bay. Law enforcement can shut one website down, but another can pop up just as easily. Information leakage is also prolific on the dark web as stated previously "in 2017 over 1.4 billion personal records were leaked over the darkweb" [1]. Child pornography is easily accessible on the dark web as well. Law enforcement managed to take down Lolita City and Playpen notorious child pornography sites, but many more are sure to pop up. Hitmen also work through the dark web a "hacker named 'bRpsd' breached the website of BesaMafia and leaked its contents online" [1]. The information that leaked showed records of 38 hit records along with close to 200 pictures of victims.

Law enforcement has more to worry about than just these illegal marketplaces. The dark web also helps launch large numbers of cyber-attacks. Ransomware attacks have become quite prolific with "72 attacks [were] reported in the first half of 2016, up 172% from the previous year" [5]. Cryptocurrencies also make it harder to track ransomware attacks with sponsors of attacks able to pay for it and hide their involvement.

The TOR browser and cryptocurrencies like Bitcoin make it hard for law enforcement to shut down these illegal operations. There are many technological challenges faced by law enforcement including: jurisdictional issues, inability to trace money, and combatting anonymity features. Law enforcement does have methods for fighting dark web crime.

The first challenge to overcome is jurisdictional issues. Different countries do have "mutual legal assistance agreements" in place to allow their countries law enforcement to better work together [7]. These agreements require a lot of paperwork and do slow down the process, but in a case involving suspects from multiple countries these processes allow everyone to be brought to justice. Agencies like Interpol and Europol do help fight international crimes; however, they are not well equipped to handle internet crimes. There are no international standards or policies "for ensuring jurisdictions have and are enforcing counter measures that tackle Dark Web crime" [7]. Therefore, nations must develop their own strategies to tackle internet crime.

The next two challenges law enforcement face are anonymity features native to TOR and Bitcoin. Law enforcement uses TOR to help catch internet crime. They do online surveillance, sting operations, and get anonymous tips. They integrate normal police investigation procedure and adapt it for the dark web. However, it is significantly harder than that simplification. Within the United States the FBI (Federal Bureau of Investigation) does have tools at their disposal to help combat internet anonymity. Including the tool memix which was "developed by Department of Defense's Defense Advanced Research Projects Agency (DARPA) which uncovers patterns to identify illegal activity" [1]. The FBI also utilizes hacking tools which was how they took down Playpen. The FBI often uses traffic and timing correlation attacks to overcome anonymity. These attacks work when the "attacker controls the first and the last router in the TOR network and uses the timing and data features to correlate the streams over those routers to break the TOR's anonymity" [1]. Law enforcement can prove successful fighting against cybercrime when they employee effective cyber strategies. The FBI has gotten good at counterattack strategies to enforce dark web crime. That cannot be said for all international law enforcement agencies, but the FBI has shown there is a path forward against internet crime.

## IV. Cryptographic Techniques for Anonymization

Different measures need to be considered for maintaining privacy. Anonymization of personal data can be done to keep one's data private. Different Cryptographic techniques can be used for anonymization through mapping each data to another unique data.

In paper [8], the authors proposed an approach based on cryptography for data anonymization. To preserve privacy, they used a function to map each unique record of raw data to another different unique record but of the same feature space. The function should be one way, so that no one can map back to the raw data which will help preserve privacy. They stated that because of the category numbers and numerical value in the health dataset used, the encryption is entirely feasible. After encryption, normalization of data is the next part of anonymization they. This technique is fulfilled by cryptographic/encryption algorithm which fulfills the privacy preservation criterion. They used encryption algorithm including two symmetric (Advanced Encryption Standard and Data Encryption Standard) and two asymmetric (Rivest-ShamirAdleman and ElGamal). For the utility of data criterion, they experimentally showed the efficiency by comparing the utility of raw data and data after anonymization. It resulted in 3% less classification performance of the proposed methodology anonymized data and the raw data.

In paper [9], authors stated that primary method for privacy protection is authentication. Authentication can be done by confirming the attributes in credentials that only the owner knows which cannot be forged or linked to a former case or transfer to different subjects. These unlikable credentials can be obtained by using the credentials once and use a Blind Signature protocol or use them several times and use Zero Knowledge Proofs for obtaining unlikability. Secure private communication can be used to establish an end-to-end encrypted communication making the content of the communications valueless to attackers. Using mix network which involves routing through multiple relays allows delays which can prevent attacks. A system providing anonymity make use of messages from multiple users, so a large volume of users can be beneficial.

Storage privacy can also be achieved by using authentication. It can also be done by storing the data in encrypted form which can be done by full disk encryption (FDE), file system level encryption (FSE) or it can be done in a steganographic file system which can hide the existence of the encrypted data. For searching such data techniques like Symmetric Searchable Encryption and Public-key Searchable Encryption can be used. Privacy preserving computations can be done by means of homomorphic encryption which allows computations in cyphertexts. Secure multi-party computation method allows sever parties to privately input to compute a function. Privacy in Database can be done in three ways including owners, users, and respondent privacy. User privacy can be done by cryptography protocols such as Private Information Retrieval.

The study presented in this paper describes the way in which the dark web works, and which are the measures taken to eliminate the crimes on the dark web. Additional measures can be planned by studying the different cyber security areas (for example, computation trust), machine learning, data mining [10-41]. Also, statistical analysis applied in other disciplines can be applied to detect such crimes [42-51].

## V. CONCLUSION

Accessing the dark web through the TOR browser is very easy. The TOR browser utilizes onion routing instead of the standard TCP/IP protocol. Onion routing works by creating circuits between tor relays and at each relay, a symmetric key is used. This ensures each node cannot trace the connection hop. Onion routing is an effective way to ensure user anonymity, especially when used in conjunction with a VPN. The cryptocurrency Bitcoin, like TOR, is a very user-friendly service. It is very easy to set up a bitcoin wallet, and once set up, it is very secure. Bitcoin works by using the blockchain which is a ledger. Each bitcoin transaction is added to the blockchain, and the transactions are authenticated using the user's private key. The actual user's identity is not tied to the transaction. This ensures the users anonymity during transaction. Bitcoin is a very good cryptocurrency, but like all it is unregulated. This makes it a very instable currency with bitcoin's value constantly in flux. These services are designed to protect user anonymity. Not everyone that uses them is involved with internet crime. Many people use TOR to circumvent their country's censorship. Law enforcement faces an uphill battle fighting internet crime. There are jurisdictional problems and not all countries will have the same resources and knowledge for fighting internet crime. The FBI has shown they are capable of fighting internet crime using online surveillance tactics and cyber-attacks to infiltrate illegal marketplaces. However, the FBI cannot be the only agency fighting cyber-crime. There needs to be more international involvement on cyber-crime since the internet has no borders.

## REFERENCES


[1] S. Kaur and S. Randhawa, "Dark Web: A Web of Crimes," Wirel. Pers. Commun., vol. 112, no. 4, pp. 2131–2158, Jun. 2020, doi: 10.1007/s11277-020-07143-2.

[2] CTM360, "Understanding the Deep & Dark Web | HackerNoon.com" Accessed Sep. 11, 2021. [Online]. Available: https://medium.com/hackernoon/understanding-the-deep-dark-web-8e4cad356587.

[3] L. Mearian, "FAQ: What is blockchain and how can it help business?," CSO, 2017. [Online]. Available: https://www.csoonline.com/article/3191619/faq-what-is-blockchain-and-how-can-it-help-business.html (accessed Sep. 11, 2021).

[4] T. Economist and T. Economist, "How does Bitcoin work?," Econ., pp. 4–5, 2013, Accessed: Sep. 11, 2021. [Online]. Available: https://bitcoin.org/en/how-it-works.

[5] K. Kirkpatrick, "Financing the dark web," Commun. ACM, vol. 60, no. 3, pp. 21–22, Feb. 2017, doi: 10.1145/3037386.

[6] V. Ververis, "Demistifying the dark web," XRDS Crossroads, ACM Mag. Students, vol. 24, no. 4, pp. 16–19, Jul. 2018, doi: 10.1145/3220544.

[7] M. R. Shillito, "Untangling the 'Dark Web': An Emerging Technological Challenge for the Criminal Law," Information & Communications Technology Law, vol. 28, no. 2, pp. 186-207, June 2019.

[8] A. Aminifar, F. Rabbi, K. I. Pun, and Y. Lamo, "A Practical Methodology for Anonymization of Structured Health Data," pp. 12–13, 2019, Accessed: Sep. 11, 2021. [Online]. Available: https://bora.uib.no/bora-xmlui/handle/1956/21978.

[9] J. Salas and J. Domingo-Ferrer, "Some Basics on Privacy Techniques, Anonymization and their Big Data Challenges," Math. Comput. Sci., vol. 12, no. 3, pp. 263–274, Jun. 2018, doi: 10.1007/s11786-018-0344-6.

[10] M Ahsan, R Gomes, Md Minhaz Chowdhury, KE Nygard, "Enhancing Machine Learning Prediction in Cybersecurity Using Dynamic Feature Selector," Journal of Cybersecurity and Privacy 1 (1), 199-218, 2021.

[11] Kendall E. Nygard, Md Minhaz Chowdhury, Ahmed Bugalwi, Pratap Kotala, "People and Intelligent Machines in Decision Making," International Journal of Computers and Their Applications, 2017.

[12] Michael Pokrinchak, Shadman Latif, Md Minhaz Chowdhury, "Distributed Denial of Service: Problems and Solutions," the 2021 IEEE International Conference on Electro Information Technology, May 14 - 15, 2021, Mount Pleasant, MI, USA.

[13] Derrick Sampson, Md Minhaz Chowdhury, "The Growing Security Concerns of Cloud Computing," the 2021 IEEE International Conference on Electro Information Technology, May 14 - 15, 2021, Mount Pleasant, MI, USA.

[14] Jeremy J. Mayerski, Md Minhaz Chowdhury, "Measures to Protect Cloud Data," the 2021 IEEE International Conference on Electro Information Technology, May 14 - 15, 2021, Mount Pleasant, MI, USA.

[15] Gary Helm, Shadman Latif, Md Minhaz Chowdhury, "Security Issues of Mobile Devices," the 2021 IEEE International Conference on Electro Information Technology, May 14 - 15, 2021, Mount Pleasant, MI, USA.

[16] Mike Mattera, Md Minhaz Chowdhury, "Social Engineering: The Looming Threat," the 2021 IEEE International Conference on Electro Information Technology, May 14 - 15, 2021, Mount Pleasant, MI, USA.

[17] Jeremy Ketterer, Md Minhaz Chowdhury, "RFID in Security and RFID Security", the 2021 IEEE International Conference on Electro Information Technology, May 14 - 15, 2021, Mount Pleasant, MI, USA.

[18] Nikolay Atanassov, Md Minhaz Chowdhury, "Mobile Device Threat: Malware," the 2021 IEEE International Conference on Electro Information Technology, May 14 - 15, 2021, Mount Pleasant, MI, USA.

[19] John A. Khan, Md Minhaz Chowdhury, "Security Analysis of 5G Network," the 2021 IEEE International Conference on Electro Information Technology, May 14 - 15, 2021, Mount Pleasant, MI, USA.

[20] MA Mos, Md Minhaz Chowdhury, "The Growing Influence of Ransomware," the 2020 IEEE International Conference on Electro Information Technology, July 31 - August 1, 2020, Naperville, IL, USA.

[21] A Mos, Md Minhaz Chowdhury, "Mobile Security: A Look into Android", the 2020 IEEE International Conference on Electro Information Technology, July 31 - August 1, 2020, Naperville, IL, USA.

[22] Jacob S. Rae, Md Minhaz Chowdhury, Mike Jochen, "Internet of Things Device Hardening Using Shodan.io and ShoVAT: A Survey," the 18th Annual IEEE International Conference on Electro Information Technology, May 2019, South Dakota, USA.

[23] Matthew R. Yaswinski, Md Minhaz Chowdhury, Mike Jochen, "Linux Security: A Survey," the 18th Annual IEEE International Conference on Electro Information Technology, May 2019, South Dakota, USA.

[24] Jared LaBar, Md Minhaz Chowdhury, Mike Jochen, Krishna Kambhampaty, "Honeypots: Security by Deceiving Threats," the Midwest Instruction and Computing Symposium 2019, April 2018, Fargo, North Dakota.

[25] John Hanley, Md Minhaz Chowdhury, Mike Jochen, Krishna Kambhampaty, "Cloud Security: Challenges, Attacks, and Techniques," the Midwest Instruction and Computing Symposium 2019, April 2018, Fargo, North Dakota.

[26] Emily Ciaravino, Md Minhaz Chowdhury, Mike Jochen, Krishna Kambhampaty, "Security Issues of SCADA Systems," the Midwest Instruction and Computing Symposium 2019, April 2018, Fargo, North Dakota.

[27] Krishna Kambhampaty, Maryam A Maryam Alruwaythi, Md Minhaz Chowdhury, Kendall E. Nygard, "Trust and its Influence on

Technology," the Midwest Instruction and Computing Symposium 2019, April 2018, Fargo, North Dakota.

[28] Krishna Kambhampaty, Maryam A Maryam Alruwaythi, Md Minhaz Chowdhury, Kendall E. Nygard, "Identifying Malicious Users Through Behaviour," Midwest Instruction and Computing Symposium 2019, April 2018, Fargo, North Dakota.

[29] Kendall E. Nygard, Md Minhaz Chowdhury, K Kambhampaty, Pratap Kotala, "Cybersecurity Materials for K-12 Education, Midwest Instruction and Computing Symposium 2018," April 2018, Duluth, Minnesota.

[30] Md Minhaz Chowdhury, Kendall Nygard, "Machine Learning within a Con Resistant Trust Model," The 33rd International Conference on Computers and Their Applications (CATA 2018), March 19-21, 2018, Flamingo Hotel, Las Vegas, Nevada, USA.

[31] Md Minhaz Chowdhury, Kendall E. Nygard, Krishna Kambhampaty, Maryam Alruwaythi, "Deception in Cyberspace: Performance Focused Con Resistant Trust Algorithm," the 4th Annual Conference on Computational Science & Computational Intelligence, December 2017, Las Vegas, Nevada, USA.

[32] Md Minhaz Chowdhury, Kendall E. Nygard, "An Empirical Study on Con Resistant Trust Algorithm for Cyberspace," The 2017 World Congress in Computer Science, Computer Engineering, & Applied Computing, 2017, Las Vegas, Nevada, USA.

[33] Md Minhaz Chowdhury, Kendall E. Nygard, "Deception in Cyberspace: An Empirical Study on a Con Man Attack," the 16th Annual IEEE International Conference on Electro Information Technology, May 2017, Lincoln, Nebraska, USA.

[34] Kendall E. Nygard, Md. Minhaz Chowdhury, Pratap Kotala, "Trust and Purpose in Computing," The 32nd International Conference on Computers and Their Applications, March 2017, Honolulu, Hawaii, USA.

[35] Md Khan, Md Minhaz Chowdhury, Kendall E. Nygard, "Electricity Price Forecasting in a Smart Grid," The 9th International Conference on Future Computational Technologies and Applications, February 2017, Athens, Greece.

[36] Sowjanya Param, Md Minhaz Chowdhury, Damian Lampl, Pranav Dass, Kendall E. Nygard, "Energy Demand Prediction Using Neural Networks," The 28th International Conference on Computer Applications in Industry and Engineering, October 2015, San Diego, California, USA.

[37] Damian Lampl, Md Minhaz Chowdhury, Pranav Dass, Kendall E. Nygard, Vahid Khiabani, "Optimization Modeling in a Smart Grid," The 15th International Conference on Wireless Networks, 2015, Athens, Greece.

[38] Md Minhaz Chowdhury, Jingpeng Tang, Kendall E. Nygard, "An Artificial Immune System Heuristic in a Smart Grid," the 28th International Conference on Computers and Their Applications, 2013, Honolulu, Hawaii, USA.

[39] Kendall E. Nygard, Steve Bou Ghosn, Md Minhaz Chowdhury, Ryan McCulloch, Davin Loegering, Anand Panday, Md. Khan, Prakash Ranganathan, "Decision Support Independence in a Smart Grid," The 2nd International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies, March 2012, Saint Maarten, Netherlands Antilles.

[40] Kendall E. Nygard, Steve Bou Ghosn, Davin Loegering, Md Minhaz Chowdhury, Ryan McCulloch, Mohammad Khan, Anand Panday, Prakash Ranganathan, "Implementing a Flexible Simulation of a Self-Healing Smart Grid," The 2011 International Conference on Modelling, Simulation and Visualization Methods, July 2011, Las Vegas, USA.

[41] Kendall E. Nygard, Steve Bou Ghosn, Md Minhaz Chowdhury, Davin Loegering, Ryan McCulloch, Prakash Ranganathan, "Optimization Models for Energy Reallocation in a Smart Grid," The IEEE Conference on Computer Communications Workshops, April 2011, Shanghai, China.

[42] Silvey Shamsi, Mian Adnan, Asif Shams Adnan, "Arithmetically and/or Geometrically Progressed Discrete Probability Distributions, Stochastic Processes and the Generalized Linear Models. Function/Process in a Mixture Probability Distribution/Process," Joint Statistical Meetings (JSM) Proceedings 2019, Alexandria, VA.

[43] Silvey Shamsi, Mian Adnan, "A Least Deviation Estimation Approach for Time Series Models," JSM Proceedings 2019, Alexandria, VA.

[44] Silvey Shamsi, Mian Adnan and Rahmatullah Imon, "A Least Deviation Estimation Approach for Multiple Regression," JSM Proceedings 2017, Business and Economic Section, Pp 760 – 771.

[45] Silvey Shamsi, Mian Adnan and Rahmatullah Imon, "Least Deviation Approach of Fitting Regression Line: An Alternative Approach to Least Square Estimates," JSM Proceedings 2016, Business and Economic Section, Pp 304 – 317.

[46] Silvey Shamsi, Mian Adnan and M. Shamsuddin, "A Class of Advanced Probabilistic and Time Series Models for Assessing Economic/Business Mobility," JSM Proceedings 2014, Business and Economic Section, Pp 3227 – 3241.

[47] Mian Adnan, Silvey Shamsi and Rahmatullah Imon, "Unique Regression Model for both Symmetric and Asymmetric Distribution," JSM Proceedings 2017, Business and Economic Section. Pp 267 – 273.

[48] Srikant Devaraj, Michael J. Hicks and Silvey Shamsi, "Indiana Healthy, Wealthy, Wise Index. Published in Indiana Chamber of Commerce," Indiana Chamber Foundation and Wellness Council of Indiana, 2016.

[49] Mian Adnan, Humayun Kaiser, Asif Adnan, Silvey Shamsi, "A Class of Folded Gamma Mixture Distributions," Far East Journal of Theoretical Statistics 2020, 60(1-2), Pp 1-23.

[50] Pranav Dass, Yang Lu, Md. Minhaz Chowdhury, Damian Lampl, Janani Kamalanathan, Kendall E. Nygard, "Gender Differences in Perceptions of Genetically Modified Foods," The 31st International Conference on Computers and Their Applications, April 2016, Las Vegas, Nevada, USA.

[51] Pranav Das, Md Minhaz Chowdhury, Damian Lampl, Kendall E. Nygard, "Risk Perceptions for Genetically Modified Organisms: An Empirical Investigation," the Software Engineering and Applications 2015, Marina Del Rey, CA.