REVIEW OF INTERNATIONAL GEOGRAPHICAL EDUCATION

ISSN: 2146-0353 ● © RIGEO ● 11(7), SPRING, 2021

www.rigeo.org

Research Article

Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models

Paschal Uchenna Chinedu[1]
Department of Computer Engineering, Edo State University Uzairue Nigeria

Wilson Nwankwo[2]
Department of Computer Science, Edo State University Uzairue Nigeria

Florence U Masajuwa[3]
Faculty of Law, Edo State University Uzairue, Nigeria

Simon Imoisi[4]
Faculty of Law, Edo State University Uzairue, Nigeria

Abstract

According to a report titled "cyberwarfare in the c-suite" released on January 21 2021 by Steve Morgan of the cybercrime magazine, cybercrime is projected to unleash global damages to the tune of six(6) trillion United States Dollars in 2021thereby becoming the third largest economy in the world as well as the greatest problem humanity has ever had to contend with. As virulent and damaging as it is, cybercrime is also the most complicated globalized crime of the 21st century. The menace is felt and appreciated across different jurisdictions. In the last two decades, it has been interestingly observed that as advanced and supposed secure information technologies are deployed in the cyberspace their hidden vulnerabilities are promptly uncoveredunconscionably following exploits by not only attackers but hobbyistsand cybersecurity apologists who are either interested in discovering the vulnerabilities inherent in the system or discrediting and dicountenancingthe claims put forward by the system manufacturers or service providers on grounds of security. To curb this menace, different approaches have been adopted including political, legislative, social, economic and technology-based solutions. Technology-based solutions for combatting cybercrime have been in the forefront and may be categorized into intelligent, traditional, and hybrid solutions. This paper reviews the developments in the last decade in the use of machine learning models (MLMs) to foster the creation of intelligent solutions targeted at curtailing the menace of cybercrimes. It follows an exploratory viewpoint and dwells on published materials from notable databases. It underscores the applicability and potentials of some of the documented intelligent anti-cybercrime strategies while discountenancing the purported merits of some. The paper concludes that while tremendous efforts had been expended in designing intelligent approaching to fighting cybercrime in the last decade, no overwhelming successes may be claimed owing to the fact that the cost of cybercrime has continued to surge consistently. To this end, this paper proposes a new integrated approach tagged the single window anti-cybercrime strategy that does not emphasize technology alone but the includion of social and intuitive elements in the detection and management of cybercrimes.

Keywords

Cybercrime, Machine Learning, Machine Learning Models, Cyberattack.

To cite this article: Chinedu P, U, Nwankwo W, Masajuwa F, U, and Imoisi S. (2021). Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. Review of International Geographical Education (RIGEO), 11(7), 956-974. Doi: 10.48047/rigeo.11.07.92

Submitted: 07-11-2020 ● **Revised:** 14-02-2021 ● **Accepted:** 05-03-2021

Introduction

Cybercrime is emerging the most complicated societal challenge of the information age. Unlike a tradional crime, an instance of cybercrime may cut across different jurisdictions and geography. Its virility makes it a nightmare in modern economies driven by the Internet. Simply stated, cybercrime is anycriminal wrong that involves the computer, digital devices, and the internet as its channel of execution (Wilson Nwankwo & Ukaoha, 2019; Okeshola & Adeta, 2013).It belongs to the category of modern crimes created by advancements in Internet and allied technologies. They may be classified as hybrid offenses in that unlike the traditional criminal wrongs such as stealing and robbery with clear localization in space and time of occurrence, these crimes may have a nexus that may be quite difficult to localize. In the light of the foregoing some authors have decribed it as a composite crime comprising cyber-enabled crimes such as fraud, organized crime, forgery, theft, money-laundering, etc, and cyber-dependent wrongs aided by the Internet and digital technologies (Akay, 2020; Jahankhani, 2018; Wall, 2007). Typical examples include internet fraud, misrepresentation, forgery, cyberbullying, cyberstalking, cyberterrorism, spam mails, cyber violence, to name a few. Cybercrime is invasive, pervasive and ubiquitous in the society and its nature appears almost infinite and consequently has altered the sociopolitical and behavioural characteristics of conventional crimes as they exertgreater economic losses in the society (Wilson Nwankwo & Ukaoha, 2019). Cybercrime is a complex and consistently changing phenomenon and cyber criminals aregetting more sophisticated and are focusing on public and private organizations thus necessitating additional layers of defense (Brewer, de Vel-Palumbo et al., 2019). S. W. Brenner and Koops (2006) had identified the social, monetary, and political repercussions of cybercrimes to the world when they pointed out that: "Cybercrime constitutes an essential case of cross-fringe wrongdoing as computer systems are the bedrock of a global network connecting all nations, and criminals have potentials of causing huge mischief in any jurisdiction hence location may be inconsequential. The potential damage is amazingly fluctuated, extending from people not having the option to get to their computer for a couple of hours or unearthing a supremacist or revolting material on the Internet, to an organization's privatenetworkdisconnected for hours or competitive advantages being taken, and to an administration's open sites being blocked…" Cybercrimes may be broadly categorized as briefly captured below.

(a) Cyber Warfare**:**Cyber warfare is the employment of computer viruses or denial-of-service (DOS) attacks by a nation-state or international organisation to inflict harm on the computers or information networks of another country. Cyberwarfare is a kind of conflict fought without the use of firearms and instead via cyberattacks. Over the past two decades, there have been many cyberwars. There have been many cyberwars between Israeli and Arab hackers, for example. "Time is running out," for example, was written in Arabic next to a cartoon depicting the death of a Hamas commander that was aired by Al-Aqsa, a Hamas-affiliated TV station in December 2008. If you have a (Carr, 2012). Several Estonian government websites were also compromised by hackers in 2007. This assault was put down to Russian aggression, according to the Estonian administration in charge. Throughout Ukraine, electricity was cut off on December 23, 2015. Malicious assaults knocked down more than 50 electrical power substations, including those of three regional distribution firms named oblenergos (CISA, 2020). For a short period of time, about 225,000 subscribers were impacted. Due to the assault, no consumers were able to call the centre to report power failures. An independent investigation discovered malware in three separate businesses in various infrastructure sectors, although their operations were unaffected, according to the same source.

(b) Cyber Terrorism:For political or ideological purposes, this means utilising the Internet to commit violent actions that result in the death or serious physical injury of others, or threaten to do so. Some people consider this to be an act of cyber terrorism when they employ malicious software and hardware to disrupt computer networks on a wide scale, particularly personal computers that are connected to the Internet using tools like computer viruses, computer worms, and phishing. The phrase "cyber terrorism" has generated a lot of debate. There are some writers that use a very limited definition, referring to the deployment of disruption assaults against information systems by well-known terrorist groups with the main goal of causing alarm, panic, or physical disturbance. Some writers, however, advocate using a more inclusive term that include cybercrime as well. Even if you don't use violence, taking part in a hack has an impact on how people perceive the terror threat (Canetti, Gross et al., 2017). The Ukrainian assault on a power

system in December 2015, which started with a phishing email, is an example of cyber terrorism. Certain cyber-terrorist sequences instil anxiety among the public about their own safety. Sequences like these have the potential to affect political outcomes. Because of cyber terrorism's severe financial costs, property destruction, and violence, it may be deadly and have a negative impact on social cohesion (Akhgar, Staniforth et al., 2014).

(c) Cyber Bullying:Bullying that occurs via digital devices such as a computer, a smartphone, or a tablet is known as cyberbullying. People may read, engage in, or post material on social networking sites, forums, or in games where cyberbullying can occur. Bullying mostly affects children, adolescents, and women. Bullying has the potential to cause significant emotional and psychological damage as well as physical changes in victims (Sibi Chakkaravarthy, Sangeetha et al., 2018). Victims may be subjected to abusive tweets, messages, or postings that make violent suggestions, harass, or even threaten the victims' lives. Identity theft, credit card theft, bullying, stalking, and psychological manipulation are all types of cybercrime that fall under the umbrella term "cyberbullying" (Sibi Chakkaravarthy, Sangeetha et al., 2018).

(d) Cyber Child Pornography**:**Even before the internet, there was child pornography, but technological advances have led to a fast growth in the creation, dissemination, and marketing of this kind of pornography throughout the world. Children's pornography is a broad term that encompasses everything from photos and films of naked youngsters to audio recordings of children in improper situations, such as sexual ones. Several research projects have been carried out in order to reduce the amount of child pornography instances that are reported (Halder & Karuppannan, 2009).

(e) Cyber Epsionage:Breaking into computer systems and networks with the goal of obtaining sensitive government or business information is an example of this approach in action. Other than that, the main aim is to better understand competitor nations' capabilities and intentions, or in the instance of industrial espionage, to obtain confidential corporate information in order to better understand a rival company's business plan or to steal intellectual property from them.. About 300 British businesses were the victims of Chinese cyber espionage operations in December 2007. (Carr, 2012).

(f) Denial-of- Service (DOS) Attack**:**DoS attacks degrade service availability and are a serious cyber security risk. Typical denial-of-service (DoS) attacks aim to deplete the target system's network bandwidth, CPU cycles, or memory so that services are inaccessible to genuine customers (Durcekova, Schwartz et al., 2012). It has been claimed that adversaries are increasingly using application layer assaults to increase the effect of denial-of-service (DoS) attacks on a target system (B. Brenner, 2010; Mantas, Stakhanova et al., 2015). By sending carefully designed legal requests to the target, these attackers hope to consume that resource and move on to the next one.

(g) Phishing:This is essentially a social engineering method designed to mislead clients and users and obtain their private information. Phishing, on the other hand, is closely linked to classical "Fishing" since it is based on the fisher troller method of communication. Fish trollers utilise bait to catch fish in rivers in traditional fishing. Phishing attacks employ similar social engineering methods to persuade the end user to divulge their personal credentials, which then allows the intruder to seize control of the system. There are a variety of ways to circumvent network security measures. Phishing attacks enable end users to disclose their credentials to attackers by convincing them to commit a security violation on the network in order to take over security settings (Adil, Khan et al., 2020)

(h) SQL Injection Attack:In a SQL injection attack, the attacker compromises databases by inserting SQL queries into the system. Before changing or destroying the data, the attacker may examine the database and recover its contents (W Nwankwo, 2020; W. Nwankwo & Njoku, 2019). Adopting a consistent authentication and authorization policy for access credentials, such as username and password, for all users is one protection strategy for this kind of attack (Sibi Chakkaravarthy, Sangeetha et al., 2018)

(i) Hacking: This involves the use of illegitimate efforts to gain unauthorized access to resources in the cyberspace. Hacking is globally frowned and often criminalized in most jurisdictions.

(j) **Identity Theft:** this is intended to hijack credentials used for conducting monetary transactions in the cyberspace. Here, the cybercriminal attempts to retrieve sensitive personal data from the victim's bank account,debit/credit cards, and similar documents that would aid in masquerading as the victim while carrying out purchases online. The victim is painfully

deprived of his funds as well as wreaking havoc on the credit worthiness and/or history of the victim.

(k) Cyber Stalking: with the growth of social networks, online harassment is taking centre stage as a source of rights abuses. The victims of cyber stalking are vulnerable individuals who are wellknown to the cyber stalkers and hence the target of abusive online messages,texts, and emails. Their intention is often to create chaotic and depressive feelings on the part of their victims.

According to International Telecommunication Union (2014), defeating cybercrime constitutes an integral part of any nations' cybersecurity protection strategy for its critical information infrastructure. Specifically, curtailing or elimination of cybercrime in the cyberspace would entail the promulgation of appropriate legislations, and other mechanisms that would aid in controlling and preventing cybercrimes. It may be recalled that the international telecommunications union (ITU) states that cybercrime and cybersecurity are inseparable entities hence this review focuses on cybercrime detection and prevention efforts over the past decade particularly as it affects the use of machine learning models. In recent times, technology has been a major contributor towards remedying the menace of threats and attacks. Vital technologies in this context include: routers, antivirus protection, firewalls, intrusion detection systems, audit and monitoring solutions, intrusion protection systems,etc.Technological techniques have also been found to provide some protective remedies and such technoquesinclude: defence in depth, and access management.

Methodology

A secondary exploratory approach designed to extracting and validating the relevant data on cybercrime detection and prevention solutions, and intelligent cybersecurity models respectively was adopted. The target data inclusion criterion was based on topics related to the stated titles and available online. The target sources were sci-direct, researchgate and scopus. This review adopted the activity framework shown in Figure 1 which depicts the procedures proposed by W Nwankwo (2020) for conducting a systematic review. In this review, the procedures adoptedare outlined as follows:

a. Definition of exclusion and inclusion criteria
b. Delineation of search strategies
c. Selection of online sources
d. Conducting search on published material in selected online sources
e. Screening and collation of retrieved titles and abstracts
f. Removal of duplicates
g. Download full texts of screened titles and abstracts
h. Selection of relevant materials using random sampling
i. Review of selected materials
j. Extraction of data and validation of data quality vis-à-vis the inclusion criteria
k. Verification of the extracted data

The target studies and papers include those that were wholly or partly connected to:

a. Cybercrimes
b. Cyber risk management
c. Intelligent cybercrime detection and prevention tools
d. Machine learning algorithms for cybersecurity applications
e. Cybersecurity and cybercrime
f. Hybrid cybersecurity models
g. Strengths and weaknesses of machine learning models in cybercrime applications

Materials were included in the collection if and only if those materials were from sources that were considered trusted published sources i.e. published materials with known publisher names, websites, and possible doi numbers. No materials outside the trusted sources were included. The direct google search was used and the searches were done against the target sources stated earlier. Two popular web browsers: The researchers used Google chrome and Mozilla Firefox for all their search operations and abstracts and titles of published papers were extracted and collated. The collated titles and abstracts were tabulated and compared across the

team(authors) and all duplicates were removed. Following the removal of all duplicates, there were five hundred and fifty titles covering all periods. From the pool of collated titles, further screening was performed to eliminate all titles that did not satisfy the period under review i.e. 2010-2021. Subsequently, a purposive sampling was applied to select 60 titles that cover the period under reference from the residue of 120 titles. The purposive sampling was based on expressive relevant features of the content of the materials vis-à-vis the selection strategy.

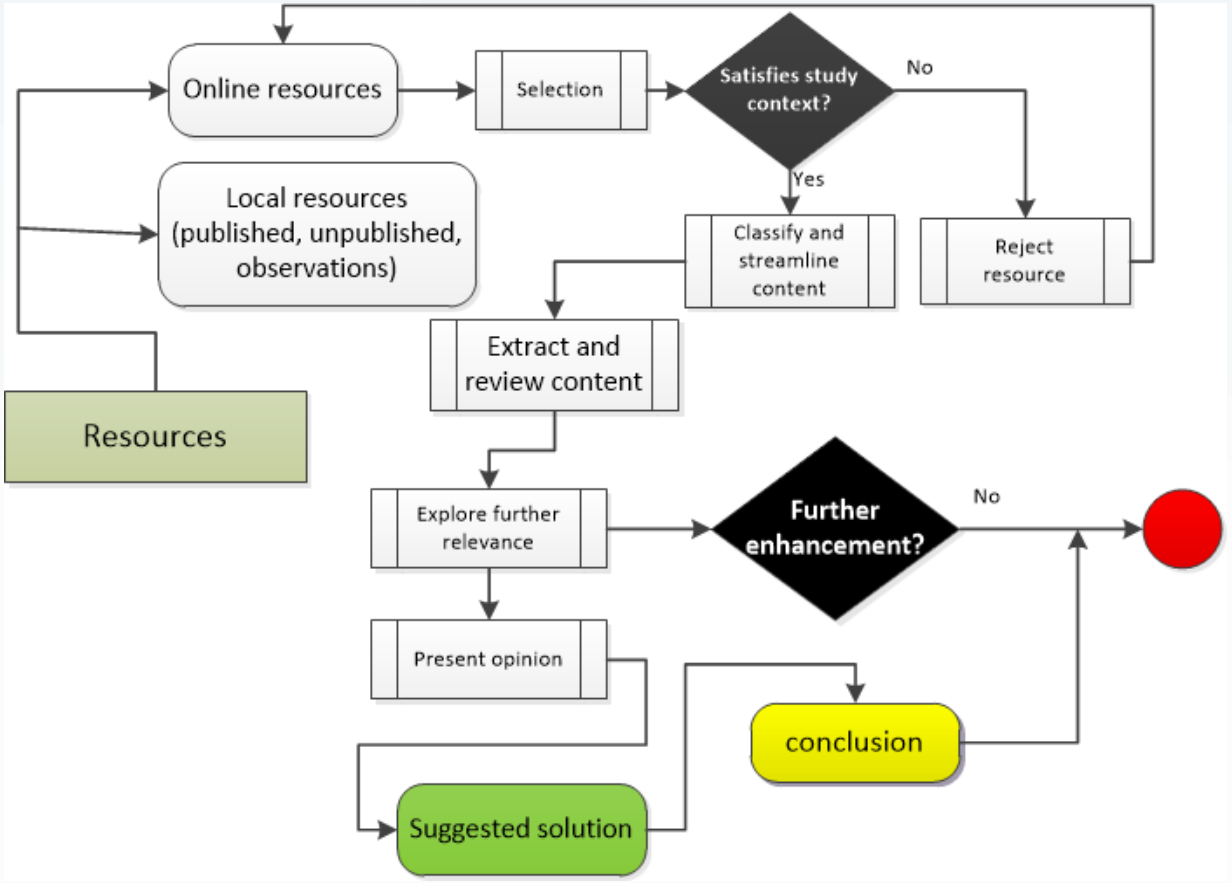

Fig. 1: Activity framework

Cybercrime Detection and Prevention Using Mlms

Machine Learning (ML) involves the training of a system by feeding large amounts of data into an algorithm the result of which is a model that could deployed for performing intelligent tasks not amenable to traditional programming. ML often use statistical, probabilistic and other optimization tools that enable the construction of models that learn from patterns in a training dataset in order to classify new data presented after training (Kotsiantis, Zaharakis et al., 2006). While the foundation of ML is in statistics and probability, it has evolvedinto more powerful technology that enables the construction of intelligent inference and decision support system using predictive models which may not be possible with conventional techniques (Alpaydin, 2020). Statistical models are limited by datasets which contain non-linear, interdependent and conditional variables typical of most real world datasets. MLMs promise more efficient results (Michie, Thomas et al., 2020). Over the years ML has evolved to be the most fundamental building blocks in Artificial Intelligence(AI) solutions used in the last decade to detect and prevent cybercrimes including Cyber Bullying, Cyber Terrorism, Child Pornography, Phishing, Denial-of-Service attack and similar threats to the enterprise and the society. Some literature abound that address the applications of ML in the predication of cyber threats, attacks, and various cybercriminal activities. For detecting cybercrimes, researchers have used a variety of MLMs drawn from supervised and unsupervised learning models. To get excellent performance and great accuracy, researchers have experimented with a variety of algorithms. This section summarises a few of the studies that were considered for inclusion in the review. Almukaynizi, Grimm et al. (2017) used ML models to assess darkweb hackers' social networks in order to anticipate cyber risks. The results of their investigation shed light on the tactics used by hackers to infiltrate social media sites. Like Sarkar, Almukaynizi et

al. (2019), they used a set of social network characteristics and ML models to determine whether or not a certain organisation will be attacked at the anticipated time. They've done research by collecting information from 53 darkweb forums. Cloud security threats, viruses, and intrusions were detected using MLMs in the early part of the last decade. However, with the growing progress in deep learning, the tendency has accelerated tremendously. The current state of cyber security uses machine learning and deep learning models nearly universally in order to identify and react to assaults Prasad and Rohokale (2020). Chen, Wawrzynski et al. (2020) developed a machine learning-based method for detecting and categorising cyber assaults that take use of security flaws. Cybercrime detection and analytics were made possible via the use of data analysis, machine learning, and other techniques. Classification, clustering, and supervised algorithms were used in the development and implementation of the suggested system. For classification, the nave bayes method was utilised, and for clustering, k-means was used. Data grouping and classification were combined with prediction analysis as part of the methodology's fourth phase: reconnaissance. Classifying cyber assaults was a cinch with the model's help. Researchers Soomro and Hussain (2019) examined a wide range of cybercrimes that target social media platforms. They offered some advice on how to avoid being a victim of a cybercrime on social media. Different kinds of cybercrimes were discovered, along with preventive suggestions and methods, by the researchers. There was no model or prototype shown for identifying and/or forecasting cybercrime instances, thus the study seems to be primarily focused on research. A two-level categorization system for cybercrime crimes was suggested by Tsakalidis and Vergidis (2017) on the basis of the European Union's original typology and subsequent study that took into consideration the current state and new types of cybercrime. Using this technology, law enforcement authorities would be able to track down the most frequent types of computer-related crimes. In addition, the system has a component for classifying a cybercrime event under a related criminal charge as part of its feature-based description. Through the consolidation and elaboration of current techniques, Tsakalidis, Vergidis et al. (2018) created a classification system for cybercrime-related offences that results in a visual extension of schema-primarily based incident descriptions that depict the interrelationships of various cybercrime elements toward a specific type of offence. According to Aslan, Sağlam et al. (2018), an online social network (OSN) consisting of Twitter has cybersecurity-related accounts. When it came to identifying suspicious accounts on the Twitter network (OSN), the researchers used machine learning methods including SVM, decision trees, and Random Forest. The anonymous account was subsequently dealt with in a particular manner by removing certain behavioural, profile, and content characteristics from the tweets. However, the authors primarily focused on Twitter-based suspect account identification while putting their approach into practise. All cybercrimes on all OSN platforms cannot be detected or predicted using this methodology. Prabakaran and Mitra (2018) identified diverse data mining strategies and machine learning methods in their study. They classified the different wrongdoings like violent crime, activity savagery, sexual attack, and cybercrimes. They examined common procedures that offer assistance to identify different violations. A genetic algorithm, a covered up Markov model, neural network, kernel predetermination calculation, logistic regression, random forest, and k-means were utilized. Siadaty and Knaus (2006) presented a technique for uncovering previously unknown patterns. They examined the database's cybercrime data, which consists of several data fields pulled from various Internet web sites. For example, there are data boxes for cyberbullying and stalking as well as robbery and identity theft. Cybercrime offences are divided into two categories: violent and nonviolent. They may also be divided into other kinds of cybercrimes, such as terrorism and stalking, pornography and cyberbullying, fraud and theft. Khan, Gani et al. (2018) described a system that used data mining techniques such as pattern recognition and Breadth-First Search to identify the presence of Denial of Service (DoS) assaults in the network (BFS). In this case, the model simply looked at the log files and ignored the data that were sent over the network. Chauhan and Sehgal (2017) presented a review report on crime analysis using data mining techniques. It discussed how the data mining approaches like k-means algorithm, random forest, etc. can help to identify the criminals. Dambo, Ezimora et al. (2017) identified some of the encryption models or tools that can help in crime detection and prevention; like Triple DES which is encryption software that was designed to replace the first developed Data Encryption Standard (DES). The triple-DES make use of three known keys with 32 bits in each of them. Another encryption tool is RSA. RSA is an open-source encryption tool. RSA uses the standard for encryption for data or information sent on a network. Unlike Triple DES, RSA is considered an asymmetric algorithm tool due to its use of a pair of keys. The results from the use of the RSA encryption tool take attackers quite a bit of time and processes

to breakthrough. Blowfish is yet another algorithm toll for combating cybercrime it was designed to replace DES. This symmetric tool splits messages into blocks of 64 bits and encrypts them individually. Blowfish when tested was very fast in execution and very effective. Meanwhile, vendors have taken full advantage of its free availability in the public domain in combating cybercrime. Blowfish tools can be explored in e-commerce platforms especially for securing payments and password management. Nouh, Nurse et al. (2016) developed an intelligent cybercrime framework system with many purposes. This structure's main goal was to keep people's intellectual tendencies under check while conducting the inquiry. These stages include identifying the issue, developing hypotheses, gathering information, and assessing those hypotheses. They also include selecting other hypotheses that are linked to the original hypothesis. Its major flaw is a lack of specificity, despite the fact that it was built to do just a few tasks. In addition, it's restricted to a narrow range of analytical tasks. Agana and Inyiama (2015) designed a model CUICDS (Cyber User Identification and Crime Detection System) intending to identify every user of the internet. It is common knowledge that once a criminal is identified, it is easier to prosecute the individual. According to Prasanthi and Ishwarya (2015), a feature extraction-based approach for cybercrime prevention and detection was suggested. TFIDF (Term Sustainability 2020, 12, 4087 3 of 16 frequency-inverse document frequency) weighted vectors contained in the cybercrime data were used to extract characteristics such as event and crime type (online or offline). Most importantly, we wanted to learn about cybercrime crimes and how they are classified by feature extraction depending on when they occur and how serious they are. In order to detect recurrent cybercrime offences and prevent them, the model was tested by comparable clustering of cybercrime offences using characteristics retrieved. A fuzzy model for intrusion detection was described by Chaudhary, Tiwari et al. (2014). In mobile ad hoc networks, the model was designed to identify packet dropping attacks. This simulation was used in the detection process, and it was shown that the model could identify packet attacks that dropped with a higher percentage of true positives and a lower percentage of false positives at all mobile node speed levels. Benaicha, Saoudi et al. (2014) demonstrated a network intrusion detective system using Genetic Algorithm with an improved selection operator capable of optimizing the search of attack scenarios in audit files and to provide the subset of possible attacks within real-time processing. The design employed a genetic algorithm approach because it can boost performance and reduce the false-positive rate. Padmadas, Krishnan et al. (2013) presented a layered genetic algorithm intrusion detection system for monitoring the legitiсy of activities in a specified environment and to determine whether or notthey are malicious based on the information resources provided. The evaluation was based on confidentiality, availability, and integrity of the organizational resources. They segregated the attack groups (DOS,U2R,R2L, and Probe) into four layers and deployed genetic algorithm tocompute filtering parameters that would improve the security of the system. The experiment revealed that the system efficiently detects R2L attacks with 90% accuracy. Kumar and Reddy (2014) developed an agent-based intrusion detection system applicable to wireless networks. This system collects information from various nodes and uses the information collected with an evolutionary AIS to detect and prevent the intrusion by bypassing or delaying the transmission over the intrusive paths. The results from the experiment carried out revealed that the system is well suited for intrusion detection and prevention as to wireless networks. Barani (2014) designed a GAAIS, a dynamic intrusion detection system in Mobile Networks with the use of artificial AIS and possibly the use of a genetic algorithm. TheGAAIS was built to adapt changes in network topology as it processes traffic. The viability of the system was applicable for detecting routing attacks like Neighbor, Rushing, Flooding, Blackhole, and Wormhole attacks. The results showed that it is more efficient when compared to similar approaches. Patel, Qassim et al. (2010) developed an IDPS with possible detection rate in network intrusion and prevention in the cloud computing environment. They could identify the requirements for an ideal cloud-based IDPS; that is, autonomic computing self-management, ontology, risk management, and fuzzy theory. Frank and Odunayo (2013) proposed three models that can help in cybercrime detection and prevention.

a. Address Verification System (AVS) which could be used to guarantee the address entered in an ordering form is the same as the address where the goods or services are mailed from;
b. Interactive Voice Response (IVR): Although it is new this technology is reported to have reduced chargebacks and fraud by collecting a voice stamp or voice authorization and verification from the customer who is ordering or receiving particular goods before the merchant ships the order.

c. IP Address tracking: Software that could track the IP address of orders can be designed in this regard. This software works by checking that the IP address of an order is from the same country included in the billing and shipping addresses in the orders made.

James and Jang (2013) propose an all-encompassing training development model - particularly centered on cybercrime examination - that's based on progressing investigator capability whereas also considering the capacity of the examiner or unit. They built a Cybercrime investigation capacity expansion framework with an emphasis on resource training which all members have a similar degree of information and skills in a particular area. Hassan and Md (2013) and Jongsuebsuk, Wattanapongsakorn et al. (2013), designed an IDS which made use of fuzzy logic as well as a genetic algorithm for the detection of various intrusion activities in a network. An experimental evaluation revealed that the proposed system achieved a reasonable intrusion detection rate. Fuzzy rules functions as to classify network attack data and the genetic algorithm finds appropriate fuzzy rule in order to obtain the optimal solution. The experimental evaluation revealed that the IDS system can detect attacks on the network in an actual time that is, within 2-3 seconds. The detection system with a detection rate of more than 97.5%. Mavee and Ehlers (2012) presented an artificial immune system(AIS)model that would aid in protecting a Smart Grid system. Their intention was to evolve a bio-inspired model for anomaly and intrusion detection, and access control in essential systemplatformsthat are rapidly emerging dependent on the cyberspace. Ojugo, Eboka et al. (2012) designed a Genetic Algorithm Rule-Based Systemto aid inachievinga better system security, confidentiality, and integrity and resource availability in networked environment. Their system uses a set of classification rules acquired from network audit data and the support-confidence framework was used as a fitness function to evaluate the quality of each rule. Their system provided some insights into the prospects of machine learning algorithms in the development of cutting-edge security models however, the integration of this model in active enterprise environment with different access structure may be somewhat difficult. Wattanapongsakorn, Srakaew et al. (2012) presented a simple network IDSusing machine learning algorithms. The system was intended to detect and classify network attacks. Their work was tested in an online network and the outcome showed that the IDS offers a high detection rate for the main attack types (Probe and DoS) within seconds and automatically protects the computer network from the attacks. Their design also incorporated the detection of other types of network attacks. Aziz, Salama et al. (2012) designed an AIS based network intrusion detection model. Their system detects attacks using a genetic algorithm. The designed project achieved an average detection rate of 81.74%. Al-Janabi and Saeed (2011) and Barman and Khataniar (2012) developed an IDS that in real-time detect and classify various attacks using neural network. The result of their work revealed that the system designed has intrusion detection rates as the same with already existing available IDSs. However, it was observed that at least it was 20% times better or faster in the detection of DoS attacks. Doelitzscher, Reich et al. (2011) hosted a cloud incident detection system Security - SAaaS. This framework depends on an intellectual independent agent that is mindful of underlying business flows of deployed cloud instances; this provides flexibility and supported cross customer event monitoring of cloud infrastructure. Yang, Wang et al. (2011) introduced a network security evaluation model to determine the degree of intrusion based using AIS theory. The model results demonstrated a few advantages over existing traditional models which is being used for network security evaluation. Liu, Yang et al. (2011) integratedan intrusion detection system based on the artificial immune concept into an Internet of Things platform. Their work simulates self-adjustment and self-learning instruments through the unique adjustment to the environment and their work provided a new effective intrusion detection for the Internet of Things. Zhang, Wang et al. (2011) proposed a system for IDS based on a distributed hierarchical model. The system is intended to improvesecurity in the Smart Grid system. Their proposed system employs AIS to distinguish and group noxious information and potential cyber-attacks. Simulation results showed an improved version as their system is valid to identify suspicious network traffic and improved system security. Dove (2011) explored abnormal behavior detection and the restrictions of looking only for known attack patterns in the cyber domain and suggested that these issues can be addressed by having a software package based on continuous learning and re-profiling of normal behavior and uses a sense-making hierarchy to decrease false-positive rates. Jiang, Frater et al. (2011) projected a bio-inspired multilayered intrusion detection model that uses multiple detection engines and sequential pattern recognition. The results of the projected work showed that the model classifies unknown behaviors and malicious attacks and that it can identify the region where abnormalities are likely to occur with little or no false-positive alert compared to

other existing models. They also claimed that their study provides the basis for an intelligent and computationally simple real-time approach for detecting unknown malware and malicious attacks in large-scale complex networks. Ferreira, Carrijo et al. (2011) examined IDS by applying wavelet to knowledge discovery and mining of datasets from network traffic patterns. Their proposed model demonstrated some appreciable success in intrusion detection. Ngafeeson (2010) examined the crime theory using two primary motivation models and four others to evolve a motivational framework for cybercrime classification. The proposed model exposed a more holistic perspective on the topic and proved a useful tool for all the stakeholders in the battle against cybercrime. The robust nature of the model makes it to incorporate the motivational dimension as a beginning component, while the classification is incorporated in the last component. This work would prove useful in contributing to a more holistic perspective on cybercrime classification. Though this model is theoretically validated and assessed, its limitation is it only looked at cybercrime from a purely motivational standpoint. Zeng, Govindan et al. (2011) proposed the Reciprocal Channel Variation-based Identification technique, an identity-based attack detection technique for mobile wireless networks. The technique exploits the reciprocity of the wireless fading channel and the received signal strength(RSS) variations naturally incurred by mobility. The technique was evaluated through hypothetical investigation considering estimation mistakes and approved its possibility through tests utilizing off-the-shelf 802.11 gadgets beneath diverse assaulting designs and indoor and open air portable scenarios. Operating under varying attacking patterns in real mobile scenarios, it was shown that the technique detects with a high precision identity-based attacks. According to Benferhat, Kenaza et al. (2008), they suggested using a nave Bayesian method to monitor alert correlation and identify cyberattacks as early as feasible before they occur by looking at the attack strategy..... An assault strategy is a set of steps used by an assailant to reach his or her objective. Using the given history of observations, the suggested system identifies the assault strategy. The authors discovered that their approach minimises false reports of attacks using the DAPRA 2000 data set and does not need an attack scenario or an expert skilled in assaults to utilise. The simplest version of a Bayesian learning network is called a nave Bayes. Consequently, it is plagued by a similar problem: it is based on probability. It's referred to as "naive" since it makes the erroneous assumption that the variables are independent of one another. To identify phishing emails, Smadi, Aslam et al. (2015) used the Random Forest (RF) algorithm. Preprocessing the email content yielded the feature metric, which was then retrieved from the body using 32 features. They have a 98.87 percent accuracy rate. Nandhini and Sheeba (2015) developed a cyberbullying detection tool utilising the Levenshtein algorithm and a naive Bayes classifier for FormSpring.me, a question-and-answer website. A C4.5 decision tree learner and an instance-based learner were utilised by Reynolds et al. 78.5 percent of the time, both students correctly recognised real positive outcomes. Text categorization was used by Uzel, Eşsiz et al. (2018) to detect acts of cyber terrorism and extremism (CTE). To find words associated with CTE in literature, the researchers applied numerical weights to keywords. The text was turned into a scalable vector format. To computerise the vector, the researchers used four different weighting methods: term frequency-based, binary, term frequency, and inverse document frequency-based weighting. There has been a proposal and implementation of a fuzzy set based on weighting techniques. As classifiers for CTE detection, the researchers utilised support vector machines (SVMs) and a nave Bayes multinomial. In addition, they made use of the data on antisocial conduct in their investigation. With an accuracy rate as high as 99 percent, the fuzzy set-based weighting technique with SVM beat out the competition. It was suggested by Vijayanand, Devaraj et al. (2018) to use a genetic algorithm for feature selection and a support vector machine (SVM) as a classifier to create an IDS for safeguarding wireless mesh networks. Network Simulator 3 was used to simulate a wireless mesh network and evaluate the proposed technology (NS3). Detection of attacks was very accurate thanks to their efforts (95.5 percent). Using feature vectors, Ma, Yearwood et al. (2009) developed a hybrid detection method for phishing emails. Feature vector creation, machine learning, method selection, and inductor and feature assessment are all part of this tool's processing pipeline. Another effort was made by Zulkefli, Singh et al. (2017), who looked at how to conduct APT assaults on smartphones. APT assaults combine social engineering and malware in a premeditated attack. Phishing is a common kind of APT attack. The authors used a decision tree classifier to accurately identify 90% of genuine websites from fraudulent ones. In light of the fact that most IDS are capable of preventing known pattern assaults, Ahn, Kim et al. (2014) suggested a new paradigm for anticipating unexpected attacks. When an attacker watches a victim's computer to gather information, discover weaknesses, and hunt for highly privileged individuals like administrators, APT

assaults are more hazardous than other types of attacks. Data mining, machine learning, and artificial intelligence all rely heavily on the paradigm system they utilised. Researchers used a variety of techniques, including regression analysis to make predictions, classification using SVM or logistic regression analysis, and the relation rule to find hidden relationships in the data. They also used atypical data mining to examine data that cannot be represented numerically, like text (e.g., text, images and videos). As a result of Android's recent popularity, various kinds of malware have been developed to target it and steal sensitive information from smartphone users' cellphones, according to Coulter, Pan et al. (2019). By transforming APK files to 8-bit greyscale pictures, the authors used visualisation methods to identify new kinds of malware. The transformed pictures were sent through a GIST descriptor, which extracted characteristics from them. As a holistic filter for images, GIST descriptors offer some information to comprehend the image's perspective in low-dimensional space (Oujaoura, Minaoui et al., 2014). KNN, decision trees, and random forests (RF) were all used in the analysis. KNN and decision trees were shown to be less accurate when compared to RF. There are no characteristics identified as significant or more relevant in the KNN algorithm since all features in the dataset have equal importance and are utilised in the same quantities. This makes it difficult to identify cybercrimes with numerous worthless features (Daumé, 2017). Making pictures was a challenge, since only half of the malware samples were able to be turned into photos due to faulty or missing ".dex" classes in their APK files. According to Vuong, Loukas et al. (2015), a technique for detecting assaults on mobile devices, such as robots, takes into account the devices' mobility, energy consumption, and the physical effect of the attack. The categorization procedure is implemented using the Decision Tree C 5.0 algorithm. Mobile robotic cars using the suggested approach are vulnerable to four kinds of attacks: denial-of-service, SQL injection, and malware (one attacking the network, the other the CPU) (Vuong, Loukas et al., 2015).

Strengths and Weaknesses of Anti-Cybercrime Mlms

From the articles on control and preventative cybersecurity techniques, seven popular MLMs have been identified: Support Vector Machine (SVM), Nave Bayes, Decision Trees, Random forests, Logistic Regression, Neural Networks, and Hybrid approaches. In this part, we'll take a quick look at the advantages of each of the MLMs we've already discovered. Predictive rules are used by the vast majority of MLMs to detect abnormalities in datasets automatically. In order to reduce the amount of false alarms, these sophisticated algorithms may help by filtering out instances that were wrongly reported and by discovering additional overlooked values using traditional criteria. The nave Bayes classifier is the most basic of the Bayesian network classifiers since it relies on the nave assumption that all attributes are free of constraints. Since this classifier's assumption characteristic is conditionally independent, numerous writers have found success with it in a wide variety of investigations. There have been reports that this classification method performs poorly with datasets like the KDD'99 dataset, which contain complicated attribute relationships, because of unfulfilled assumption characteristics (Yassin, Udzir et al., 2014). Leaf nodes and decision nodes make up decision trees, another common categorization method. Decision trees are evaluated in part by the amount of categorization error. The proportion of incorrectly categorised instances is what we've come up with as an erroneous definition. The classification accuracy decreases significantly as there are more class categories in the decision tree (Yassin, Udzir et al., 2014). Decision tree-based algorithms, particularly the J48, have shown higher weighted recall and overall accuracy, according to certain researchers, who believed they were superior than SVM. As a consequence of improved findings, the authors of the study stated that decision tree-based algorithms offer a better knowledge of different types of harmful behaviour (Aiyanyo, Samuel et al., 2020). The Random Forest model is another popular categorization method in cybersecurity. Using this method, a forest of trees would be formed from the training data, and each dataset would traverse the forest to be categorised, with the results calculated by average the predictions from all the trees. This method of categorization has a well-deserved reputation for precision. False alarms and processing times may be cut in half using it (Yassin, Udzir et al., 2014). Logistic regression is a classifier that uses input vectors to project them onto hyperplanes in a probabilistic manner. There's a correlation between the distance between an input and a hyperplane and the likelihood that the input belongs to a certain class. There is some training time required for the logistic classifier, but it is an effective classifier that has been put to use in cyberthreat detection applications. As a result of this, noisy data produced by security risks and assaults may be handled

efficiently (Alrawashdeh & Purdy, 2016). Many IDS programmes have made use of neural networks. Deep learning, supported by several layers of interconnected networks, is ones of the classification technique's most sophisticated versions. Using this classification method, complex data issues may be solved by extracting sophisticated patterns from simple characteristics (Aiyanyo, Samuel et al., 2020). Hybrid cyber security detection methods have been suggested in many peer-reviewed MLMs research. It was also found that the detection accuracy was higher than the single random tree algorithm's detection accuracy when random forest and NBTree algorithms, which integrate naveBayes and decision tree classifiers, were applied cooperatively on the sum rule scheme (Kevric, Jukic et al., 2017). Though the proposed MLMs have shown remarkable promises in dealing with the menace of cybercrime and cyberthreats, someof the proposed MLMs for preventing cybercrime have been shown to be mere propositions and prototypes that are not easilily implementable in the mainstream cyberspace. More so, the quality of cybersecurity datasetsis important asthe datasets might be noisy, incomplete, insignificant, imbalanced, or may contain inconsistent instances related to a particular security incident. Such problems in a dataset may affect the quality of the learning process hence would degrade the performance of the MLMs (Sarker, 2019a).To make a data-driven intelligent decision for cybersecurity solutions, such problem in data must be dealt with effectively before building the cyber models. Therefore, understanding such problems in cyber data and effectively handling such problems using existing algorithms or newly proposed algorithms for a particular problem domain like malware analysis or intrusion detection and prevention is needed, which could be another research issue in cybersecurity data science (Sarker, Kayes et al., 2020). Unarguably, datasets are major components in any project involving the implementation of MLMs. Most of the existing datasets are old and might be insufficient in terms of understanding the recent behavioral patterns of various cyber-attacks and threats. Although the data can be transformed into a meaningful understanding level after performing several processing tasks, there is still a lack of understanding of the characteristics of recent attacks and their patterns of occurrence (Sarker, Kayes et al., 2020). Context-awareness in cybersecurityis a major concern in developing and deploying cybersecurity solutions and existing cybersecurity works mainly originate from the relevant cyber data containing several low-level features (De Bruijn & Janssen, 2017). When data mining and machine learning techniques are applied to such datasets, a related pattern can be identified that describes it properly. However, a broader contextual information like temporal, spatial, relationship among events or connections, and dependencies can be used to decide whether there exists a suspicious activity or not (Aleroud & Karabatis, 2017; Sarker, 2019b; Sarker, Colman et al., 2018). With the progress attained in the cybersecurity domain especially in approaches designed to curtail cybercrime, the attack and threatdomain is also evolving rapidly. Consequent upon the foregoing, two challenges have been noted in applying MLMs to handle such new attacks. First, the MLMs are applied to locate such activities that may not be previously seen (Sommer & Paxson, 2010). Secondly, newer attacks may be technically and structurally distinguishable from older ones. Since models are more often trained with past features in a dataset, latest attacks may exhibit differentfeature set. The latest attacks may evade these classifiers and generate false alarms or reduce the detection rates. Third, cybercrime is a conglomerate of many factors not just the technology alone. Identifying, prevention and detection of a breach is could be linked to the extant legislation(s) within the jurisdiction, organizational policy, knowledge of the user, etc.

The Single Window Anti-Cybercrime Strategy

Having studied the strengths and lapses in the MLMs, a 'single window' approach is proposed. The proposed single window is an abstraction that represents a model of anti-cybercrime strategy that encompasses different disparate techniques and mechanisms for containing the menace of cybercrime. The other side of the single window is enterprise rality in the sense that it would provide a kind of cyber platform that connects different stakeholders within an economy or beyond especially businesses and public organizations that provide useful services to the public(e.g. the judiciary,etc.) through electronic platforms. The electronic platform would use protocols other than web protocols. Prior to the deployment of MLMs in the detection and control of cybercrimes there has been efforts that utilize independent or collection of anticybercrime techniques such as:

a. Cybercrime legislation e.g. General Data Protection Regulation in Europe,HIPAA,Cybercrime Prevention Act 2015, etc. (Wilson Nwankwo & Ukaoha, 2019). Legislations provide legal framework for regulating and controlling cybercrime. While legislations are great vehicles they may not have a uniform global recognition, force, and application respectively. This is because what is considered a cybercrime in one jurisdiction may not be a crime afterallin another jurisdiction. However, due to the transnational nature of many cybercrimes, those globally recognized and legislated cybercrimes would need be encapsulated into a partition of a 'cybercrime domain'. In the said domain, the characteristics of known cybercrimes would be defined and captured in such a way that they are accessible possibly through a secure electronic data interchange channel and somewhat actionable for decision making purposes. The implication is that businesses and organizations on a public network such as the Internet could get connected to the said cybercrime EDI platform. Such a platform may helpin strengthening the existing national laws by exploring areas of harmonization across international stakeholders i.e. between one country or jurisdiction and another thereby promoting the concept of dual criminality which would be mutually beneficial to the participating parties, as well as in the evolution of more efficient laws. The platform would also strengthen private public partnership and international collaborations (Kifordu, Nwankwo et al., 2019; Wilson Nwankwo & Kifordu, 2019)

b. Policy/Strategy e.g. National Cybersecurity Strategy in Nigeria (Wilson Nwankwo & Ukaoha, 2019). The proposed single window model would incorporate the fine grains or measurable elements of a regional or national cybersecurity strategy in a manner that would reflecta benchmark and baseline response/effortto be employed either individually or collectively to existing or contemplated cyber threats/attacks and crimesthat target breaching the integrity of e-transactions, privacy,critical infrastructure, consumer protection, and data protection. The benchmarks could be reviewed from time to time based on the actual responses(successes and failures) to cyber infringements documented or reported by the participating stakeholders.

c. Law enforcement: using public and private agencies and groups (Apau & Koranteng, 2020; Chang, 2020; Hunton, 2011; Peters & Jordan, 2019). For instance, the Economic and Financial Crimes Commission is popular in Nigeria in the fight against cybercrimes. Cybercrime as a transnational menace requires a participatory platform that drives investigations, and possible interventions from any location in the world. The single automated window would provide a cooperative platform for interested enforcement agents from different jurisdictions to investigate and prosecute cybercrimes. The platform can evolve a critical global infrastructure that supports collaboration among law enforcement agencies.

d. Technology and Technical knowhow e.g. Firewalls, intrusion detection, intrusion prevention, passwords, biometrics, antivirus software, anti-spam software, regular software updates, etc. Technologies and techniques are the hallmark of cybersecurity from a technical perspective. Though these tools have been deployed and have proved indispensable for enterprises and governments in the last decade, it is instructive to note that these technological would yield more results when they are complemented with socio-legal compoents such as legislations, policies and enforcement. MLMs may be further enhanced by the data gathered from the single window repository. Furthermore, the development of new tools would also depend on the responses gathered from the platform.

e. Risk management: cybercrime is one of the risks arising from ICT devices and solutions, for instance, the use of proxy servers though intended to be used legitimately may also be hijacked by criminals who exploit the anonymization feature of these servers to inflict deadly attacks on their victims or targets without any trace ofthe perpetrator's identity (Chow, 2012; Jahankhani, 2018). There are many other scenarios where cyber risks are prevalent, for instance, social media, blogs, websites, etc. In such circumstances, potential users may need toreduce their exposure to social media, avoid downloads from unknown sources, withdraw from insecure websites, and protect their accesscredentials,etc.are good risk management approaches. Risk management controls could be preventive and and could also be used for control in organizations as they streamline what needs be protected, criticality of resources, and measures to be activated to prevent or mitigate any threat or attack from cybercriminals (Levi, Doig et al., 2017; Okutan, 2019; Taveras, 2019). The proposed single window by its nature contemplates risk management in which cases every communication is graded as either trusted or untrusted. All participants would be alerted of any untrusted communications on the platform and such would also be logged for use in tracing and tracking of threats.

f. Capacity building: Training of personnel on cyber security best practices,etc.

g. Cyber awareness programs

h. Vulnerability disclosure: wherein professionals and/or researchers may discover and publish hardware and/or software vulnerabilities on the Internet to alert the vendor to fix the vulnerability. Disclosure may be full or responsible disclosure (Burgess & Knox, 2019).

As International Telecommunication Union (2008) notes, cybercrime and breaches in the cyberspaceare complex in the sense that no one method or strategy listed above can curb it. The proposed single window model would afford a holistic integrated approach to tackling the problem. This model would integrate all the basic anti-cybercrime strategies and technologies in such a manner that enables threats, vulnerabilities, and attacks to be documented and logged as they are noticed on any platform or device connected to the EDI infrastructure. The EDI infrastructure would host acyber 'threatbank' a kind of databank for automatic threats and attack registration. The threatbankcould be used for MLMs for building dynamic self-adaptive anti-cybercrime solutions. More so, since cybercrime has both national and internationational dimensions, the single integrated strategy could provide impactful insights to all stakeholders in driving the legislation, policy formulation, and implementation of practical mechanisms for prevention, detection, and management of these complex phenomenon across various jurisdictions. To this end, a self-adaptive system would be very helpful as it would adjust to the dynamics of cyber threats and attack patterns.

Conclusion

The various categories of cybercrimes have been highlighted in this paper.Moreso, a comprehensive review of cybercrime detection and precention models in the last decade using various the MLMs and other intelligent systems had beenpresented with the view to identifying the effectiveness of MLMs. Following the identification ofareas of strengths of these detection and prevention models as well as the challengesconfronting the utilization of these models in real world scenarios that are prone to threats, attacks and breaches, this review concludes that insofar as the applicability of MLMs to modeling and implementing intelligent systems for curtailing or containing cybercrimes in the cyberspace, there are some setbacks which include unavailability of adequate cybercrime datasets across the various threat and attack domains, limited scope, adaptability, reproducibility in real world environments, etc. hence there is a need for the stakehoders to collaborate towardsevolving a single window infrastructure which would enable profiling of cybercriminal activities as much as possible to address the dearth of dataset in this all important research domain, collaboration, and enforcement.

References

Adil, M., Khan, R., & Ghani, M. A. N. U. (2020). Preventive techniques of phishing attacks in networks. Paper presented at the 2020 3rd International Conference on Advancements in Computational Sciences (ICACS). Doi:https://doi.org/10.1109/ICACS47775.2020.9055943

Agana, M. A., & Inyiama, H. C. (2015). Cyber Crime Detection and Control Using the Cyber User Identification Model IRACST - International Journal of Computer Science and Information Technology & Security, 5(5), 354-368. Retrieved from https://www.researchgate.net/publication/324774119

Ahn, S.-H., Kim, N.-U., & Chung, T.-M. (2014). Big data analysis system concept for detecting unknown attacks. Paper presented at the 16th International Conference on Advanced Communication Technology. Doi:https://doi.org/10.1109/ICACT.2014.6778962

Aiyanyo, I. D., Samuel, H., & Lim, H. (2020). A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning. Applied Sciences, 10(17), 5811. Doi:https://doi.org/10.3390/app10175811

Akay, Y. V. (2020). Computer Forensics and Cyber Crime Handling. Jurnal Teknik Informatika, 15(4), 291-296. Doi:https://doi.org/10.35793/jti.15.4.2020.32601

Akhgar, B., Staniforth, A., & Bosco, F. (2014). Cyber crime and cyber terrorism investigator's handbook: Syngress.

Al-Janabi, S. T. F., & Saeed, H. A. (2011). A neural network based anomaly intrusion detection system. Paper presented at the 2011 Developments in E-systems Engineering. Doi:https://doi.org/10.1109/DeSE.2011.19

Aleroud, A., & Karabatis, G. (2017). Contextual information fusion for intrusion detection: a survey and taxonomy. Knowledge and Information Systems, 52(3), 563-619. Doi:https://doi.org/10.1007/s10115-017-1027-3

Almukaynizi, M., Grimm, A., Nunes, E., Shakarian, J., & Shakarian, P. (2017). Predicting cyber threats through hacker social networks in darkweb and deepweb forums. Paper presented at the Proceedings of the 2017 International Conference of The Computational Social Science Society of the Americas. Doi:https://doi.org/10.1145/3145574.3145590

Alpaydin, E. (2020). Introduction to Machine Learning: MIT Press. Retrieved from https://books.google.com.pk/books?id=tZnSDwAAQBAJ

Alrawashdeh, K., & Purdy, C. (2016). Toward an online anomaly intrusion detection system based on deep learning. Paper presented at the 2016 15th IEEE international conference on machine learning and applications (ICMLA). Doi:https://doi.org/10.1109/ICMLA.2016.0040

Apau, R., & Koranteng, F. N. (2020). An overview of the digital forensic investigation infrastructure of Ghana. Forensic Science International: Synergy, 2, 299-309. Doi:https://doi.org/10.1016/j.fsisyn.2020.10.002

Aslan, Ç. B., Sağlam, R. B., & Li, S. (2018). Automatic detection of cyber security related accounts on online social networks: Twitter as an example. Paper presented at the Proceedings of the 9th International Conference on Social Media and Society. Doi:https://doi.org/10.1145/3217804.3217919

Aziz, A. S. A., Salama, M. A., ella Hassanien, A., & Hanafi, S. E.-O. (2012). Artificial immune system inspired intrusion detection system using genetic algorithm. Informatica, 36(4), 347-358. Retrieved from http://informatica.si/index.php/informatica/article/download/417/421

Barani, F. (2014). A hybrid approach for dynamic intrusion detection in ad hoc networks using genetic algorithm and artificial immune system. Paper presented at the 2014 Iranian Conference on Intelligent Systems (ICIS). Doi:https://doi.org/10.1109/IranianCIS.2014.6802607

Barman, D. K., & Khataniar, G. (2012). Design of intrusion detection system based on artificial neural network and application of rough set. International Journal of Computer Science and Communication Networks, 2(4), 548-552.

Benaicha, S. E., Saoudi, L., Guermeche, S. E. B., & Lounis, O. (2014). Intrusion detection system using genetic algorithm. Paper presented at the 2014 Science and Information Conference. Doi:https://doi.org/10.1109/SAI.2014.6918242

Benferhat, S., Kenaza, T., & Mokhtari, A. (2008). A naive bayes approach for detecting coordinated attacks. Paper presented at the 2008 32nd Annual IEEE International Computer Software and Applications Conference. Doi:https://doi.org/10.1109/COMPSAC.2008.213

Brenner, B. (2010). Layer 7 increasingly under DDoS gun. Retrieved from https://www.csoonline.com/article/2124801/report--layer-7-increasingly-under-ddos-gun.html

Brenner, S. W., & Koops, B.-J. (2006). Cybercrime and Jurisdiction: A Global Survey: TMC Asser Press.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). Cybercrime prevention: Theory and applications: Springer. Retrieved from https://link.springer.com/book/10.1007%2F978-3-030-31069-1

Burgess, J. T. F., & Knox, E. J. M. (2019). Foundations of Information Ethics: American Library Association. Retrieved from https://books.google.com.pk/books?id=hUOgDwAAQBAJ

Canetti, D., Gross, M., Waismel-Manor, I., Levanon, A., & Cohen, H. (2017). How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks. Cyberpsychology, Behavior, and Social Networking, 20(2), 72-77. Doi:https://doi.org/10.1089/cyber.2016.0338

Carr, J. (2012). Inside Cyber Warfare: Mapping the Cyber Underworld: O'Reilly Media, Incorporated. Retrieved from https://books.google.com.pk/books?id=nFP9wrNmGhcC

Chang, W.-J. (2020). Cyberstalking and Law Enforcement. Procedia Computer Science, 176, 1188-1194. Doi:https://doi.org/10.1016/j.procs.2020.09.115

Chaudhary, A., Tiwari, V., & Kumar, A. (2014). Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks. Paper presented at the 2014 IEEE International Advance Computing Conference (IACC). Doi:https://doi.org/10.1109/IAdCC.2014.6779330

Chauhan, C., & Sehgal, S. (2017). A review: crime analysis using data mining techniques and algorithms. Paper presented at the 2017 International Conference on Computing,

Communication and Automation (ICCCA). Doi:https://doi.org/10.1109/CCAA.2017.8229823
Chen, D., Wawrzynski, P., & Lv, Z. (2020). Cyber security in smart cities: A review of deep learning-based applications and case studies. Sustainable Cities and Society, 66, 102655. Doi:https://doi.org/10.1016/j.scs.2020.102655
Chow, P. (2012). Surfing the Web Anonymously - The Good and Evil of the Anonymizer: SANS. Retrieved from https://www.sans.org/white-papers/33995/
CISA. (2020). Critical Infrastructure Sectors. Cybersecurity & Infrastructure Security Agency. Retrieved from https://www.cisa.gov/critical-infrastructure-sectors
Coulter, R., Pan, L., Zhang, J., & Xiang, Y. (2019). A visualization-based analysis on classifying Android malware. Paper presented at the International Conference on Machine Learning for Cyber Security. Doi:https://doi.org/10.1007/978-3-030-30619-9_22
Dambo, I., Ezimora, O., & Nwanyanwu, M. (2017). Cyber Space Technology: Cyber Crime, Cyber Security and Models of Cyber Solution, A Case Study of Nigeria. International Journal of Computer Science and Mobile Computing, 6(11), 94-113. Retrieved from https://ijcsmc.com/docs/papers/November2017/V6I11201734.pdf
Daumé, H. (2017). A course in machine learning: Hal Daumé III. Retrieved from http://ciml.info/dl/v0_9/ciml-v0_9-ch03.pdf
De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1-7. Doi:https://doi.org/10.1016/j.giq.2017.02.007
Doelitzscher, F., Reich, C., Knahl, M., & Clarke, N. (2011). An autonomous agent based incident detection system for cloud environments. Paper presented at the 2011 IEEE Third International Conference on Cloud Computing Technology and Science. Doi:https://doi.org/10.1109/CloudCom.2011.35
Dove, R. (2011). Self-organizing resilient network sensing (sorns) with very large scale anomaly detection. Paper presented at the 2011 IEEE International Conference on Technologies for Homeland Security (HST). Doi:https://doi.org/10.1109/THS.2011.6107917
Durcekova, V., Schwartz, L., & Shahmehri, N. (2012). Sophisticated denial of service attacks aimed at application layer. Paper presented at the 2012 ELEKTRO. Doi:https://doi.org/10.1109/ELEKTRO.2012.6225571
Ferreira, E. W. T., Carrijo, G. A., de Oliveira, R., & de Souza Araujo, N. V. (2011). Intrusion detection system with wavelet and neural artifical network approach for networks computers. IEEE Latin America Transactions, 9(5), 832-837. Doi:https://doi.org/10.1109/TLA.2011.6030997
Frank, I., & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: challenges and solution. International Journal of Cognitive Research in science, engineering and education, 1(1). Retrieved from https://core.ac.uk/reader/162155890
Halder, D., & Karuppannan, J. (2009). Cyber socializing and victimization of women. The Journal on Victimization, 12(3), 5-26. Retrieved from https://ssrn.com/abstract=1561774
Hassan, M., & Md, M. (2013). Current Studies On Intrusion Detection System, Genetic Algorithm And Fuzzy Logic. International Journal of Distributed and Parallel Systems (IJDPS), 4(2), 35-47. Doi:https://doi.org/10.5121/ijdps.2013.4204
Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. Computer Law & Security Review, 27(1), 61-67. Doi:https://doi.org/10.1016/j.clsr.2010.11.001
International Telecommunication Union. (2008). Recommendation ITU-T X.1205 Retrieved from https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-E&type=items
International Telecommunication Union. (2014). Understanding cybercrime: Phenomena, challenges and legal response. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx
Jahankhani, H. (2018). Cyber criminology: Springer. Retrieved from https://link.springer.com/book/10.1007%2F978-3-319-97181-0
James, J. I., & Jang, Y. J. (2013). An Assessment Model for Cybercrime Investigation Capacity. 1-8. Retrieved from https://arxiv.org/abs/1307.0076
Jiang, F., Frater, M., & Hu, J. (2011). A bio-inspired host-based multi-engine detection system with sequential pattern recognition. Paper presented at the 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing. Doi:https://doi.org/10.1109/DASC.2011.46

Jongsuebsuk, P., Wattanapongsakorn, N., & Charnsripinyo, C. (2013). Network intrusion detection with fuzzy genetic algorithm for unknown attacks. Paper presented at the The International Conference on Information Networking 2013 (ICOIN). Doi:https://doi.org/10.1109/ICOIN.2013.6496342

Kevric, J., Jukic, S., & Subasi, A. (2017). An effective combining classifier approach using tree algorithms for network intrusion detection. Neural Computing and Applications, 28(1), 1051-1058. Doi:https://doi.org/10.1007/s00521-016-2418-1

Khan, S., Gani, A., Wahab, A. W. A., & Singh, P. K. (2018). Feature selection of denial-of-service attacks using entropy and granular computing. Arabian Journal for Science and Engineering, 43(2), 499-508. Doi:https://doi.org/10.1007/s13369-017-2634-8

Kifordu, A., Nwankwo, W., & Ukpere, W. (2019). The Role of Public Private Partnership on the Implementation of National Cybersecurity Policies: A Case of Nigeria. Journal of Advanced Research in Dynamical and Control Systems, 11(8), 1386-1392.

Kotsiantis, S. B., Zaharakis, I. D., & Pintelas, P. E. (2006). Machine learning: a review of classification and combining techniques. Artificial Intelligence Review, 26(3), 159-190. Doi:https://doi.org/10.1007/s10462-007-9052-3

Kumar, G. P., & Reddy, D. K. (2014). An agent based intrusion detection system for wireless network with artificial immune system (AIS) and negative clone selection. Paper presented at the 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies. Doi:https://doi.org/10.1109/ICESC.2014.73

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2017). Cyberfraud and the implications for effective risk-based responses: themes from UK research. Crime, Law and Social Change, 67(1), 77-96. Doi:https://doi.org/10.1007/s10611-016-9648-0

Liu, C., Yang, J., Chen, R., Zhang, Y., & Zeng, J. (2011). Research on immunity-based intrusion detection technology for the Internet of Things. Paper presented at the 2011 Seventh International Conference on Natural Computation. Doi:https://doi.org/10.1109/ICNC.2011.6022060

Ma, L., Yearwood, J., & Watters, P. (2009). Establishing phishing provenance using orthographic features. Paper presented at the 2009 eCrime Researchers Summit. Doi:https://doi.org/10.1109/ECRIME.2009.5342604

Mantas, G., Stakhanova, N., Gonzalez, H., Jazi, H. H., & Ghorbani, A. A. (2015). Application-layer denial of service attacks: taxonomy and survey. International Journal of Information and Computer Security, 7(2-4), 216-239. Doi:https://doi.org/10.1504/IJICS.2015.073028

Mavee, S. M., & Ehlers, E. M. (2012). A Multi-agent Immunologically-inspired Model for Critical Information Infrastructure Protection--An Immunologically-inspired Conceptual Model for Security on the Power Grid. Paper presented at the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. Doi:https://doi.org/10.1109/TrustCom.2012.40

Michie, S., Thomas, J., Mac Aonghusa, P., West, R., Johnston, M., Kelly, M. P., . . . O'Mara-Eves, A. (2020). The Human Behaviour-Change Project: An artificial intelligence system to answer questions about changing behaviour. Wellcome open research, 5, 1-5. Doi:https://dx.doi.org/10.12688%2Fwellcomeopenres.15900.1

Nandhini, B. S., & Sheeba, J. (2015). Cyberbullying detection and classification using information retrieval algorithm. Paper presented at the Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015). Doi:https://doi.org/10.1145/2743065.2743085

Ngafeeson, M. (2010). Cybercrime classification: a motivational model. Paper presented at the Proceedings of Southwest Decision Sciences Institute Conference. Retrieved from http://www.swdsi.org/swdsi2010/sw2010_preceedings/papers/pa168.pdf

Nouh, M., Nurse, J. R., & Goldsmith, M. (2016). Towards designing a multipurpose cybercrime intelligence framework. Paper presented at the 2016 European Intelligence and Security Informatics Conference (EISIC). Doi:https://doi.org/10.1109/EISIC.2016.018

Nwankwo, W. (2020). A Review of Critical Security Challenges in SQL-based and NoSQL Systems from 2010 to 2019. International Journal of Advanced Trends in Computer Science and Engineering, 9(2). Doi:https://doi.org/10.30534/ijatcse/2020/174922020

Nwankwo, W., & Kifordu, A. (2019). Strengthening private sector participation in public infrastructure projects through concession policies and legislations in Nigeria: A Review. Journal of Advanced Research in Dynamical and Control Systems, 11(Special Issue-08), 1360-1370. Retrieved from https://ssrn.com/abstract=3565156

Nwankwo, W., & Njoku, C. C. (2019). Adoption of Internet Voting Platform Containing Data Injection Threats with Structured LINQ. Nigerian Research Journal of Engineering and Environmental Sciences, 4(2), 724-739. Retrieved from http://www.rjees.com/download/?file=V04-N02-724-739.pdf

Nwankwo, W., & Ukaoha, K. C. (2019). Socio-Technical perspectives on Cybersecurity: Nigeria's Cybercrime Legislation in Review. International Journal of Scientific and Technology Research, 8(9), 47-58. Retrieved from https://www.researchgate.net/publication/337033615

Ojugo, A., Eboka, A., Okonta, O., Yoro, R., & Aghware, F. (2012). Genetic algorithm rule-based intrusion detection system (GAIDS). Journal of Emerging Trends in Computing and Information Sciences, 3(8), 1182-1194. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.649.8808&rep=rep1&type=pdf

Okeshola, F. B., & Adeta, A. K. (2013). The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state, Nigeria. American International Journal of Contemporary Research, 3(9), 98-114. Retrieved from http://www.aijcrnet.com/journals/Vol_3_No_9_September_2013/12.pdf

Okutan, A. (2019). A framework for cyber crime investigation. Procedia Computer Science, 158, 287-294. Doi:https://doi.org/10.1016/j.procs.2019.09.054

Oujaoura, M., Minaoui, B., Fakir, M., El Ayachi, R., & Bencharef, O. (2014). Recognition of isolated printed tifinagh characters. International Journal of Computer Applications, 85(1), 1-13. Doi:https://doi.org/10.5120/14802-3005

Padmadas, M., Krishnan, N., Kanchana, J., & Karthikeyan, M. (2013). Layered approach for intrusion detection systems based genetic algorithm. Paper presented at the 2013 IEEE International Conference on Computational Intelligence and Computing Research. Doi:https://doi.org/10.1109/ICCIC.2013.6724120

Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. Information Management & Computer Security, 18(4), 277-290. Doi:https://doi.org/10.1108/09685221011079199

Peters, A., & Jordan, A. (2019). Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. Journal of National Security Law and Policy, 10(3), 487-524. Retrieved from https://www.jstor.org/stable/resrep20150

Prabakaran, S., & Mitra, S. (2018). Survey of analysis of crime detection techniques using data mining and machine learning. Paper presented at the Journal of Physics: Conference Series. Doi:https://doi.org/10.1088/1742-6596/1000/1/012046

Prasad, R., & Rohokale, V. (2020). Artificial intelligence and machine learning in cyber security. In Cyber Security: The Lifeline of Information and Communication Technology (pp. 231-247): Springer. Doi:https://doi.org/10.1007/978-3-030-31703-4_16

Prasanthi, M. M. L., & Ishwarya, T. A. S. K. (2015). Cyber Crime: Prevention & Detection. International Journal of Advanced Research in Computer and Communication Engineering, 4(3), 45-48. Doi:https://doi.org/10.17148/ijarcce.2015.4311

Sarkar, S., Almukaynizi, M., Shakarian, J., & Shakarian, P. (2019). Predicting enterprise cyber incidents using social network analysis on dark web hacker forums. The Cyber Defense Review, 87-102. Retrieved from https://www.jstor.org/stable/26846122

Sarker, I. H. (2019a). Context-aware rule learning from smartphone data: survey, challenges and future directions. Journal of Big Data, 6(1), 1-25. Doi:https://doi.org/10.1186/s40537-019-0258-4

Sarker, I. H. (2019b). A machine learning based robust prediction model for real-life mobile phone data. Internet of Things, 5, 180-193. Doi:https://doi.org/10.1016/j.iot.2019.01.007

Sarker, I. H., Colman, A., Kabir, M. A., & Han, J. (2018). Individualized time-series segmentation for mining mobile phone user behavior. The Computer Journal, 61(3), 349-368. Doi:https://doi.org/10.1093/comjnl/bxx082

Sarker, I. H., Kayes, A., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 7(1), 1-29. Doi:https://doi.org/10.1186/s40537-020-00318-5

Siadaty, M. S., & Knaus, W. A. (2006). Locating previously unknown patterns in data-mining results: a dual data-and knowledge-mining method. BMC Medical Informatics and Decision Making, 6(1), 1-13. Doi:https://doi.org/10.1186/1472-6947-6-13

Sibi Chakkaravarthy, S., Sangeetha, D., Venkata Rathnam, M., Srinithi, K., & Vaidehi, V. (2018). Futuristic cyber-attacks. International Journal of Knowledge-based and Intelligent Engineering Systems, 22(3), 195-204. Retrieved from https://content.iospress.com/articles/international-journal-of-knowledge-based-and-intelligent-engineering-systems/kes180384

Smadi, S., Aslam, N., Zhang, L., Alasem, R., & Hossain, M. A. (2015). Detection of phishing emails using data mining algorithms. Paper presented at the 2015 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA). Doi:https://doi.org/10.1109/SKIMA.2015.7399985

Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. Doi:http://dx.doi.org/10.1109/SP.2010.25

Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. Appl. Comput. Syst., 24(1), 9-17. Retrieved from https://sciendo.com/downloadpdf/journals/acss/24/1/article-p9.pdf

Taveras, P. (2019). Cyber Risk Management, Procedures and Considerations to Address the Threats of a Cyber Attack. Paper presented at the Proceedings of the ForenSecure: Cybersecurity and Forensics Conference, Chicago, Illinois April 12th, 2019. Retrieved from https://www.researchgate.net/publication/332411201

Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(4), 710-729. Doi:https://doi.org/10.1109/TSMC.2017.2700495

Tsakalidis, G., Vergidis, K., & Madas, M. (2018). Cybercrime Offences: Identification, Classification and Adaptive Response. Paper presented at the 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT). Doi:https://doi.org/10.1109/CoDIT.2018.8394816

Uzel, V. N., Eşsiz, E. S., & Özel, S. A. (2018). Using fuzzy sets for detecting cyber terrorism and extremism in the text. Paper presented at the 2018 Innovations in Intelligent Systems and Applications Conference (ASYU). Doi:https://doi.org/10.1109/ASYU.2018.8554017

Vijayanand, R., Devaraj, D., & Kannapiran, B. (2018). Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection. Computers & Security, 77, 304-314. Doi:https://doi.org/10.1016/j.cose.2018.04.010

Vuong, T. P., Loukas, G., & Gan, D. (2015). Performance evaluation of cyber-physical intrusion detection on a robotic vehicle. Paper presented at the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing. Doi:https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.313

Wall, D. (2007). Cybercrime: The Transformation of Crime in the Information Age.: Polity Press.

Wattanapongsakorn, N., Srakaew, S., Wonghirunsombat, E., Sribavonmongkol, C., Junhom, T., Jongsubsook, P., & Charnsripinyo, C. (2012). A practical network-based intrusion detection and prevention system. Paper presented at the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. Doi:https://doi.org/10.1109/TrustCom.2012.46

Yang, J., Wang, T., MingLiu, C., & Li, B. (2011). Improved Agent Model for Network Security Evaluation Based on AIS. Paper presented at the 2011 Fourth International Conference on Intelligent Computation Technology and Automation. Doi:https://doi.org/10.1109/ICICTA.2011.46

Yassin, W., Udzir, N. I., Abdullah, A., Abdullah, M. T., Zulzalil, H., & Muda, Z. (2014). Signature-Based Anomaly intrusion detection using Integrated data mining classifiers. Paper presented at the 2014 International Symposium on Biometrics and Security Technologies (ISBAST). Doi:https://doi.org/10.1109/ISBAST.2014.7013127

Zeng, K., Govindan, K., Wu, D., & Mohapatra, P. (2011). Identity-based attack detection in mobile wireless networks. Paper presented at the 2011 Proceedings IEEE INFOCOM. Doi:https://doi.org/10.1109/INFCOM.2011.5934990

Zhang, Y., Wang, L., Sun, W., Green, R. C., & Alam, M. (2011). Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid. Paper presented at the 2011 IEEE Power and Energy Society General Meeting. Doi:https://doi.org/10.1109/PES.2011.6039697

Zulkefli, Z., Singh, M. M., Shariff, A. R. M., & Samsudin, A. (2017). Typosquat cyber crime attack detection via smartphone. Procedia Computer Science, 124, 664-671. Doi:https://doi.org/10.1016/j.procs.2017.12.203