IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 23, 2020, accepted July 12, 2020, date of publication July 22, 2020, date of current version August 5, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3011259

Comprehensive Review of Cybercrime Detection Techniques

WADHA ABDULLAH AL-KHATER[1], (Graduate Student Member, IEEE), SOMAYA AL-MAADEED[1], (Senior Member, IEEE), ABDULGHANI ALI AHMED[2], (Senior Member, IEEE), ALI SAFAA SADIQ[3,4], (Senior Member, IEEE), AND MUHAMMAD KHURRAM KHAN[5], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Qatar University, Doha, Qatar
[2]School of Computer Science and Informatics, Cyber Technology Institute, De Montfort University, Leicester LE1 9BH, U.K.
[3]School of Mathematics and Computer Science, Wolverhampton Cyber Research Institute, University of Wolverhampton, Wolverhampton WV1 1LY, U.K.
[4]Center of Artificial Intelligence Research and Optimization, Torrens University, Brisbane, QLD 4006, Australia
[5]Center of Excellence in Information Assurance, King Saud University, Riyadh 11653, Saudi Arabia

Corresponding author: Abdulghani Ali Ahmed (aa.ahmed@ieee.org)

This work was supported by the NPRP from the Qatar National Research Fund (a member of the Qatar Foundation) under the National Priorities Research Program (NPRP) under Grant PRP12S-0312-190332. The statements made herein are solely the responsibility of the authors.

ABSTRACT Cybercrimes are cases of indictable offences and misdemeanors that involve computers or communication tools as targets and commission instruments or are associated with the prevalence of computer technology. Common forms of cybercrimes are child pornography, cyberstalking, identity theft, cyber laundering, credit card theft, cyber terrorism, drug sale, data leakage, sexually explicit content, phishing, and other forms of cyber hacking. They mostly lead to a privacy breach, security violation, business loss, financial fraud, or damage in public and government properties. Thus, this study intensively reviews cybercrime detection and prevention techniques. It first explores the different types of cybercrimes and discusses their threats against privacy and security in computer systems. Then, it describes the strategies that cybercriminals may utilize in committing these crimes against individuals, organizations, and societies. It also reviews the existing techniques of cybercrime detection and prevention. It objectively discusses the strengths and critically analyzes the vulnerabilities of each technique. Finally, it provides recommendations for the development of a cybercrime detection model that can detect cybercrimes effectively compared with the existing techniques.

INDEX TERMS Security, cybercrime detection techniques, neural network, fuzzy logic, machine learning, data mining.

I. INTRODUCTION

Cybercrime is defined as any crime conducted using computers or other communication tools to cause fear and anxiety to people or damage, harm, and destroy properties. Cybercrimes have two categories, namely, computer-assisted and computer-focused cybercrimes. Examples of computer-assisted cybercrimes are child pornography, fraud, money laundering, and cyber stalking, whereas examples of computer-focused cybercrimes are hacking, phishing, and website defacement [1].

Obtaining correct and official statistics on cybercrimes is challenging because of the culture in which the crimes were committed, the severity of the offences, and the unreported incidents due to the lack of knowledge or societal constraints. Law enforcement plays an important role in these cases because it controls the level of detail that is reported [1].

The first cybercrime incident, in which computer codes were replicated, took place in the 1960s [2]. Many fraud and forgery cases were reported after 1970 when a bank teller at New York's Union Dime Savings Bank embezzled over $1.5 million from customer accounts. A creeper virus was developed by Bob Thomas in 1971 to infect the systems of the Advanced Research Project Agency Network (ARPANET), which was the first network with

The associate editor coordinating the review of this manuscript and approving it for publication was Luis Javier Garcia Villalba.

packet-switching technology and the TCP/IP protocol [2], [3]. In early 1977, an employee at Imperial Chemical Industries stole hundreds of computers and their backups from the company and asked for 275,000 pounds sterling as a ransom [2]. In 1988, Robert T. Morris developed the first computer worm via a computer at the Massachusetts Institute of Technology [4]. In 1994, Russian hackers transferred huge amounts of money from a city bank to bank accounts in Russia, Finland, Israel, Germany, the United States, the Netherlands, and Switzerland [2].

The first phishing attempt was made in 1995 [2]. The Electronic Disturbance Theater was established in 1997, which was responsible for creating electronic versions of site-in tools that are used in protests. Protesters in 1998 used a tool called FloodNet to perform a denial-of-service attack on the website of the president of Mexico.

In January 1998, a revenger system operator remotely changed the Supervisory Control and Data Acquisition (SCADA) system of a coal-fired power plant to its emergency mode, and the SCADA system software was then removed; the SCADA system is utilized to control and monitor equipment or a plant in an industrial field d [5]. In 2005, computer systems in a European bank were shut down due to an attack against air conditioning systems, causing the increased temperature in its computer room. In 2006, the Russian Business Network organization was established [2]. This illegal organization conducted many cybercrimes and offered many cybercrime tools and services related to Trojans, spam, and phishing. It specialized in personal identity theft for resale. In 2011, British intelligence agencies replaced a webpage that described how to make bombs with one that described how to make cupcakes.

The literature review of this study covered studies that have been conducted to develop techniques for the detection and prevention of cybercrimes. The existing techniques have been reviewed and analyzed by many review and survey studies. However, the existing review studies either focused on studying certain cybercrimes, such as cyberbullying [6], botnets [7], fake profiles [8], phishing [9], and email spam [10], or reviewing particular detection techniques such as data mining [11], [12], machine learning [13], and deep learning [14].

This study provides a comprehensive review of cybercrime detection techniques, which are categorized based on the use of different detection methods. The study first presents the different types of cybercrimes and discusses their consequences against individuals, organizations, and societies. Second, it comprehensively reviews the existing techniques of cybercrime detection and classifies them into the following categorized techniques: 1) Statistical-based techniques, which focus on analyzing and extracting information from research data to develop effective methods for cybercrime detection; 2) machine learning techniques, which focus on predicting outputs according to a given input data; 3) neural network-based techniques, which are used to find reasonable solutions for cybercrimes; 4) fuzzy logic classifier and genetic algorithm, which intends to minimize possible false alerts that rise during the detection of cybercrimes; and 5) data-mining-based techniques, which are developed to detect cybercrimes using apriori algorithm. Third, this study also covers other techniques that have been developed to detect cybercrimes based on other detection methods, such as computer vision, biometric, cryptography, and forensic tools. Fourth, this study critically analyzes the strengths and drawbacks to evaluate the detection efficiency of the reviewed techniques in terms of accuracy, response time, and false-alarm rates. Lastly, the study provides some recommendations to enhance the efficiency of the existing techniques and increase their detection accuracy.

The rest of this paper is organized as follows. Section 2 introduces and defines some types of cybercrimes. Section 3 discusses previous studies on cybercrime detection techniques that use different technologies, such as machine learning and data mining technology. Section 4 discusses datasets. Section 5 presents the conclusions and future work.

II. CYBERCRIME TYPES

Cybercrimes can be divided into several categories [1]. The following subsections name and explain these categories in detail.

A. CYBER TERRORISM

Cyber terrorism is an unlawful action that involves violence against people and properties. It often has political, and racial or ideological purpose. Besides, this type of cybercrimes can spread fear, anxiety, and violence amongst people or sabotage as well as destroy properties (e.g. computers and networks). Cyber terrorism can also affect the availability and integrity of information [2]. Terrorists utilize the Internet for disseminating of propaganda, recruiting individuals, influencing public opinion, and shutting down national infrastructure (e.g., transportation, dams, traffic lights, and energy facilities). An example of cyber terrorism is the Ukrainian attack on a power grid in December 2015, which began with a phishing email. Certain sequences of cyber terrorists create fear and disruption amongst citizens regarding their safety. Such sequences can also influence political decision-making. Serious economic loss, property damage, and violence as a result of cyber terrorism can lead to death and affect the cohesion of society [2].

B. CYBER WARFARE

Cyber warfare is a type of warfare that does not use weapons, but cyberattacks. It can be performed by organizations or groups of hackers without permission from the government, and it can lead to political problems amongst countries [15]. Today, cyberwarfare and cyberattacks are the most common type of warfare. Many cyberwars have taken place in the last 20 years. For example, Russia and Georgia were engaged in a cyberwar in 2008, which have involved several attacks on the Georgian government websites via structured query language (SQL) injection, distributed denial-of-service (DDoS), and cross-site scripting [15].

Both Israel and Arab hackers have committed many cyberwars against each other. For example, in December 2008, Israel attacked a Hamas TV station, Al-Aqsa, to broadcast a cartoon movie of Hamas' leader being killed, which was tagged with Arabic comments that stated, "Time is running out" [15]. In 2007, a group of hackers hacked several Estonian government websites. The Estonian government blamed Russia for these attacks.

In Ukraine, on December 23, 2015, electrical power was disconnected all over the country. Three regional electrical power distribution companies, called oblenergos, and more than 50 substations were affected by malicious attacks and went offline [16]. Approximately 225,000 customers were affected for a few hours. All customers were unable to contact the center via the phone to report electricity outages due to the attack. Power was manually brought back after six hours. Malware was found in three different companies in different infrastructure sectors, but their operations were not affected [16].

Another attack on a Ukrainian power station occurred one year later, cutting electricity to certain ministries and the national railway system [17]. All the affected oblenergos proceeded to work under restricted conditions and manually attempted to recover after the attack. However, the attackers implemented techniques to slow down and stop the recovery process [18]. One such technique is remote disconnection of the uninterruptable power supply system [19]. The attackers also have changed the passwords of legitimate users. Therefore, they were not able to log-in to the system during the recovery process. It took the power stations off for six months to recover from the attack. The attackers replaced legitimate firmware with malicious firmware, which destroyed gateways and caused them to be unrecoverable. Thus, the decision maker of the power stations had to buy new devices and integrate them into the system, but this has involved a very high cost [20].

C. CYBER ESPIONAGE

Espionage refers to any action that involves spies and the theft of important and sensitive information for the benefit of rival companies or foreign governments. Cyber espionage uses computers to conduct missions [15]. In December 2007, approximately 300 British companies suffered from cyber espionage attacks by Chinese organizations [15]. In addition, many organized attacks were made on the computers and networks of the US Department of Defense from 2003 to 2006 by China. These organized series of attacks were called "Titan Rain."

D. CHILD PORNOGRAPHY

Child pornography refers to pictures, videos, and audio recordings of children wearing inappropriate, few, or no clothes who are in inappropriate positions, specifically sexual positions. Many studies have been conducted to minimize the number of child pornography cases [21]. In general, child pornography contents are distributed for two purposes either for profit or non-profit. For profit purposes, the child pornography are sold in many websites. For non-profit purposes, P2P network can be used to share and distribute those child pornography contents.

The law considered any production, possession, or distribution of any type of digital content of child pornography as a serious crime. This is including self-image, trusting others, and disruptions in sexual development. On the other hand, the consequences of this crime on the child side are very harmful and it could last for long time especially the psychological consequences. Those types of consequences and problems will increase if the digital content distributed in the Internet and the child could be a victim for cyber-criminals who are targeting children for sexual purposes.

E. CYBER BULLYING

The increased usage of social media and technology by people of different ages and genders increases the likelihood of unwanted behaviors such as bullying. Bullying is one of the most negative experiences that a person can be faced with, especially during childhood. Most people who experience bullying are children, teenagers, and women. Bullying can inflict emotional and mental harm, and it can affect people's personality [22]. Victims may receive harmful and rude tweets, messages, or posts that suggest violence, harass the victims, or threaten their lives.

Cyberbullying is a type of cybercrime that includes any activity that is harmful to a person, including identity theft, credit card theft, bullying, stalking, and psychological manipulation [22]. Table 1 describes some of the cyber bullying types that could victim go through.

TABLE 1. Cyberbullying types.

Cyberbullying type	Definition
Cyber verbal abuse	The perpetrator's hatred for the victim is expressed on the victim's social media.
Cyber libel	Also called malicious gossip, the perpetrator attempts to spread lies about the victim on his/her social media or online groups.
Morphing	The perpetrator takes the victim's photograph from his/her profile and uses it for pornographic purposes.
Blackmailing	The perpetrator illegally uses personal information taken from the victim's social media account. Women are particularly vulnerable to blackmail and threats, both of which may involve physical threats, from enemies, ex-spouses, and stalkers.
Copying and cloning	The victim's profile, which includes his/her personal information and photographs, is stolen and copied to contact the victim's friends and obtain private information.

After children, women are most vulnerable to cybercrimes because, women tend by nature to be sociable. They easily acquaint themselves with virtual friends or online groups with whom they can discuss cooking techniques, children and family issues as well as post-pregnancy tips. Halder and Karuppannan [22] have suggested that this acquaintanceship can lead to cybercrimes, which highlighting different types of victimization.

F. PHISHING

Phishing is one of the most popular attacks due to its direct connection to the end user. In such cases, the attacker attempts to fool the end user to provide him/her with sensitive information. Phishing involves a combination of spoofing techniques and social engineering. The victim receives an email asking him/her about sensitive information, warning him/her about an attack, and persuading him/her to install new protection software that is actually malware. Alternatively, a phishing email may contain a link to a fake website [9]. One of the important defensive methods is not to click on a link that appears in a suspicious email. Other ways to protect yourself from phishing attacks are to only visit safe websites that have 'https' in their URL and to install anti-virus software, firewalls, and anti-phishing toolbars [23].

G. DENIAL-OF-SERVICE ATTACK

Denial-of-service (DoS) attacks are a major online threat in which the attacker compromises the availability of services. DoS crashes compromised systems with a huge number of requests, such as Internet Control Message Protocol (ICMP) and SYN floods, causing the systems to get crashed and stop providing the intended service. Another type of DoS attack called a distributed denial-of-service (DDoS) attack, the attacker has access to many channels in a network, and each victim becomes an agent to attack another system, like a zombie [24]. Figure 1 illustrates an example of a DDoS attack. DoS and DDoS attacks take place through the following methods:

1) ICMP FLOOD ATTACK OR SMURF ATTACK

ICMP is a connectionless protocol used to diagnose networks and identify errors. The attacker overwhelms the target server with a huge number of ICMP messages, and the victim server deals with each message and processes it until the server becomes overwhelmed and crashes [25], [26].

2) SYN FLOOD ATTACK

The attacker overwhelms the target system with a flood of SYN attacks to prevent the targeted system from responding to legitimate users [26].

3) TEARDROP ATTACK

The attacker overwhelms the target system with disorganized and overlapped packets. Legitimate senders break messages into organized packets, but the attacker manipulates packets to make them large with large payloads. This causes the target system to become overwhelmed and attempt to reassemble the manipulated and overlapped packets until the system can no longer respond to legitimate users [25]. DDOS attacks can be prevented or mitigated using two methods: the first is to implement DDOS attack prevention services, and the second is to increase the traffic bandwidth of the company's website [23].

H. SQL INJECTION ATTACK

The SQL injection attack is a type of attack in which the attacker compromises databases using some SQL queries. The attacker can look at the database and retrieve its content before altering or deleting the data [27]. One of the best prevention strategies for this type of attack is to set a high standard level of credentials, such as username and password, for all users [23].

I. FUTURISTIC IN CYBER ATTACKS

Futuristic cyber-attacks can target many new and recent technologies and devices, such as WiFi, health care devices, robots, and drones. These new technologies are highly vulnerable to cyber-attacks. WiFi technology is widely used among users and industries; this can jeopardize the security for such users and companies. Some examples of attacks that could affect WiFi users are the man-in-the-middle attack, the key reinstallation attack (KRACK), and the signal jamming attack [23].

In the health care sector, implantable medical devices (IMDs) suffer from security vulnerabilities that can cause harmful consequences to people's health if exploited. IMDs are electronic devices implanted inside the human body to treat or control disease [28]. Examples of IMDs devices include the following:

- Implantable cardioverter defibrillators (ICDs) are devices implanted to monitor the heart rate of the patient [28]. Insulin pumps are devices implanted to deliver insulin regularly [28]. Implantable nerve stimulators that are devices to treat chronic pain via sending electrical current in the human body [28].

Robots are also vulnerable to attacks; those targeted include industrial robots and elder care robots. Drones and unmanned aerial vehicles (UAV) are another target for the attackers. UAVs can be hacked since their on-board chips are not encrypted and they are connected to the ground controller through WiFi. Therefore, they are vulnerable to all of the attacks applied on WiFi technology, including man-in-the-middle attacks and signal jamming attacks [23].

Table 2 lists the current cybercrimes and summarizes their features, level of crime, and targets.

III. CYBERCRIME DETECTION TECHNIQUE

The number of cybercrimes has rapidly increased as none of the traditional cybercrime detection systems implemented by forensics researchers can completely stop or mitigate them. This is because the victims or targets of cybercrimes (e.g., people, banks, properties, and governments) differ depending on the motivation for the crime (e.g., money, fame, sex, curiosity), and cybercriminals improve their methods and

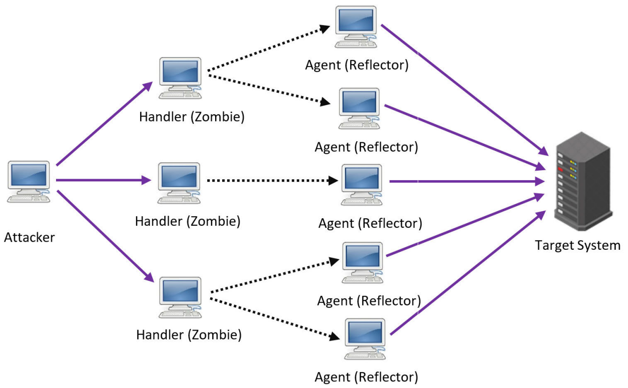

FIGURE 1. An example of a DDoS attack.

TABLE 2. Cybercrime types.

Cyber Crime	Features	Level Of Crime	Target
Cyber Terrorism	- Often has a political, racial, or ideological purpose. - Can spread fear, anxiety, and violence among people or sabotage and destroy property.	Major crime	- People - Property
Cyber Warfare	- Can be performed by organizations or groups of hackers without permission from the government. - Can lead to political problems within countries	Major crime	- Government - National infrastructur
Cyber Espionage	- Any action that involves spies and the theft of important and sensitive information for the benefit of rival companies or foreign governments.	Major crime	- Government - Companies.
Child Pornography	- Refers to pictures, videos, and audio recordings of children wearing inappropriate clothes for sexual purposes.	Major crime	- Children.
Cyber Bullying	- Activities those are harmful to a person, including rude messages or tweets. - Posts that suggest violence, harass the victims, or threaten their lives.	Minor crime	- Children. - Teenagers. - Women.
Phishing	- Attempts to deceive the end user to obtain their sensitive information.	Depends on its consequences.	- Children. - Teenagers. - Women.
Denial-of-Service Attack	- An attacker compromises the availability of services. - DoS crashes compromised systems with a huge number of requests, such as ICMP and SYN floods. - Causes systems to crash and stop working.	Major crime	Systems.
SQL Injection Attack	- An attacker can retrieve data from a database. - The attacker can alter or delete data from the database.	Major crime	Databases
Futuristic Attacks	- Can target many new and recent technologies and devices.	Major crime	- WIFI. - Health care devices - Robots - Drones

utilize new technologies to commit crimes and achieve their goals.

Many prior studies have been conducted to develop methods for detecting cybercrimes. The main categories of these methods are shown in Figure 2 and described in the following subsections.

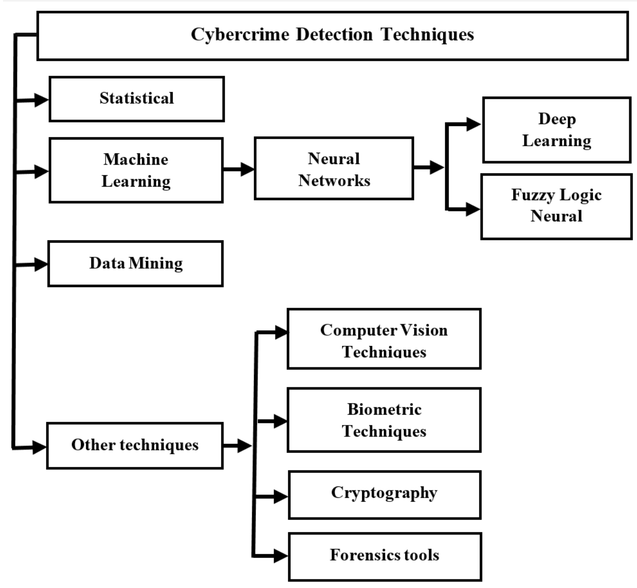

FIGURE 2. Categorization of cybercrime detection techniques.

A. CYBERCRIME DETECTION USING STATISTICAL METHODS

The Hidden Markov Model is one of the best models for detecting cyberattacks. However, it is a time-consuming process. Sultana *et al.* [29] improved the Hidden Markov Model by minimizing the time required for data training to detect cyberattacks using the N-gram extraction algorithm. This improved Hidden Markov Model utilizes recurrent or repeated patterns in trace files instead of whole trace events. The N-gram extraction algorithm was used during data mining to extract common patterns. As a result, the data training time for constructing a system was reduced by 31.96–48.44%.

Liang *et al.* [30] proposed a filter for an intrusion detection system (IDS) to detect attacks in vehicle ad hoc networks (VANETs) are a special type of networks responsible of monitoring the movement of a group of vehicles without utilizing a base station. It also arranges and manages the communication between the vehicles [31]. This filter was intended to decrease the response time and overhead in the detection process without affecting detection accuracy. The authors utilized the Hidden Markov Model to implement the filter.

On the other hand, Qiao *et al.* [32] proposed an IDS that utilized the Hidden Markov Model and was based on the University of New Mexico (UNM) dataset. Rasmi and Jantan [33] developed a new algorithm for an IDS based on cosine similarity to predict attack intentions. This new algorithm, called the similarity of attack intentions (SAI) algorithm, generates a similarity matrix of previous and known attack intentions that is used to calculate the probability ratio for each attack intention. Similarity is calculated based on the ratio of new attacks to known and predefined attacks.

Harrou *et al.* [34] designed an anomaly detection system to detect TCP SYN flood attacks based on the 1999 DAPRA dataset. TCP SYN floods are utilized in DoS and DDoS attacks. The researchers used the CRPA measure because of its sensitivity to any changes in common patterns of packet flow. They merged the CRPA measure with two statistical methods— Exponentially Weighted Moving Average (EWMA) and Shewhart—to identify the best anomaly detection system. The researchers compared the performance of four mechanisms: EWMA, Shewhart, CPRA-EWMA, and CPRA-Shewhart. The experiment showed that merging the CPRA with the EWMA and Shewhart achieved superior results. The CPRA-Shewhart mechanism detected attacks with many false alarms, while the CPRA-EWMA mechanism detected attacks without false alarms. Therefore, the CPRA-EWMA mechanism outperformed the CPRA-Shewhart, EWMA, and Shewhart mechanisms.

Abouzakhar *et al.* [35] developed a system to detect network cybercrimes using a Bayesian learning network approach. The authors have applied their proposed system to a DARPA 2000 dataset of DDoS attacks generated by the Massachusetts Institute of Technology (MIT) Lincoln Laboratory. They evaluated the results using the Life Chart Method. However, it should be noted that the Bayesian network relies on probabilistic models, which are only work well in noisy environments but are unsuitable in real environments. Additionally, this approach is not as feasible as deterministic correlation methods in reality.

Wang *et al.* [36] detected and mitigated a new type of DDoS attack called a link-flooding attack (LFA). LFA attacks can cut off service in very critical areas of a network by flooding them with legitimate low-speed flows. Therefore, normal IDSs, such as an anomaly detection system or signature-based detection system, cannot detect this type of attack. The researchers proposed a new defense system called LFADefender. While a traditional IDS is installed in a fixed location in a network, LFADefender is adjustable and can change its location in the network in real time. LFA attackers attack the target with high-flow-density links. Therefore, the first task of LFADefender is to find high-flow-density links in the network through software defined networking (SDN) [37], [38]. Software defined networking (SDN) is an architecture that abstracts a control plane from data to achieve more flexibility in network management [39]. After high-density or congested links are detected, rerouting is initiated to avoid the congested links and mitigate—but not stop—the LFA attack. The link density or congestion is monitored by sFlow traffic analyzer software [40]. To stop LFA attacks, the researchers proposed a malicious traffic blocking approach to identify the bot and stop it from affecting the network. This approach monitors and traces the traffic in the network. After rerouting, the attacker will update his or her link map, which contains the target links. If the flow packets appear in the new links again, then they are identified as bot flow packets and the source IP address is identified. Finally, a block flow message will be sent from the SDN controller to block those packets from the network. The traced packet is then utilized to define the bot packets using statistical methods, including calculation of the variance and average of packet numbers and an outlier detection algorithm called, the local outlier factor, to specify the time that the packets suddenly increased in the network. To evaluate this framework, the researchers implemented a test bed using CloudLab, an open platform used to simulate attacks and implement new systems.

TABLE 3. Summary of statistics-based cybercrime detection methods.

Ref.	Technique	Task	Dataset source	Results
[29]	Hidden Markov Model	Detect cybercrime	Traces of routine calls in target system	Data training time was reduced by 31.96–48.44%, but there was less accuracy.
[34]	CPRA-EWMA, CPRA-Shewhart	Detect TCP SYN flood attacks	1999 DAPRA dataset	The CPRA-EWMA mechanism outperformed the others.
[35]	Bayesian learning network approach	Detect network cybercrime	DARPA 2000 dataset	The major attacks were detected, but the results were not clear.
[36]	Outlier detection algorithm called local outlier factor	Detecting link-flooding attacks	Simulated attacks in a simulated network topology from a global Highwinds network provided by the Topology Zoo database	In the first experiment, the algorithm detected 60% of bot traffic. After several experiments, the detection rate was 90%, with some misjudgments of normal and legitimate traffic.

Birkinshaw *et al.* [41] implemented an IDS using software-defined networking (SDN). The authors have targeted two types of attacks: DoS and port scanning, for which they implemented Credit-Based Threshold Random Walk (CB-TRW) and Rate Limiting (RL). A CB-TRW algorithm detects worm infection on a host, whereas an RL algorithm is used to prevent DoS attacks and to detect the number of requests sent and received from a network interface controller (NIC) [42], [43]. Table 3 summarizes the statistics-based methods of cybercrime detection developed in prior studies.

B. CYBERCRIME DETECTION USING MACHINE LEARNING

Machine learning is the science of predicting outputs based on given input data, also called training data. The machine (i.e., computer) learns how to predict correct and appropriate outputs for specific inputs using the training data. This learning process can be supervised or unsupervised. In the supervised learning method, the training data contain pairs: an input and its corresponding output. The outputs are called labeled outputs because the correct output is already known. The machine tries to learn how pairs are built in order to make its own predictions later. In unsupervised learning methods, the outputs are unlabeled. Therefore, the machine does not know the correct output for each given input. This makes the learning process difficult [44].

One of the basic learning models is the decision tree, which is a classic form of decision-making that is similar to the divide-and-conquer method. There are two types of decision trees: binary and multi-class classification. In a binary classification tree, the response is either "yes" or "no." The question that is asked is called a "feature," the response to the question is called the "feature value," and the rating is called a "label." Preference for one response over the other is called inductive bias [45].

Researchers have utilized different algorithms from the supervised learning algorithm category, including naïve Bayes and the K-nearest neighbor (KNN), and the unsupervised learning algorithm category, such as K-means, to detect cybercrimes. Several algorithms have been tried to achieve high accuracy and good performance. Some of these studies are presented below.

To detect cyberbullying on FormSpring.me, a question-and-answer website, Nandhini and Sheeba [46] have proposed a cyberbullying detection tool using the Levenshtein algorithm and naïve Bayes classifier. While, Reynolds *et al.* [47] used a C4.5 decision tree learner and instance-based learner. Both learners identified true positive results with an accuracy of 78.5%.

On the other attempt, as a way to detect cyberbullying in YouTube comments, Dinakar *et al.* [48] used three supervised machine learning methods: JRip, J48, and a support vector machine (SVM). The authors also compared a binary classifier and multi-classifier. In contrast, Al-garadi *et al.* [49] proposed a tool to detect cyberbullying in tweets. They extracted different types of features from each tweet to be utilized in the classifier to detect cyberbullying. Several classifiers—namely, the support vector machine, naïve Bayes, KNN, and decision tree—were tested to determine the best classifier. The authors concluded that naïve Bayes shows the best performance and has sufficient strength [49].

Uzel *et al.* [50] utilized text classification to identify cyber terror and extremism (CTE). The researchers assigned numerical weights to terms in order to detect vocabulary related to CTE in texts. The document was converted to a vector. The researchers utilized four weighting methods— namely, term frequency-based, binary, term frequency, and inverse document frequency-based weighting—to computerize the vector. A fuzzy set based on the weighting methods was proposed and implemented. The researchers used SVM and a naïve Bayes multinomial as classifiers to detect CTE. They have also used the antisocial behavior data set in their experiment. The results showed that the fuzzy set-based weighting method with SVM outperformed the other methods, with accuracy of up to 99%.

To date, most works have examined cyberbullying only in English-language texts. Only Haider *et al.* [51] focused on the Arabic language. The researchers used Waikato Environment for Knowledge Analysis (WEKA) because it supports the Arabic language, and they utilized naïve Bayes and SVM to classify texts as either cyberbullying or not cyberbullying.

Benferhat *et al.* [52] proposed a naïve Bayes approach to observe alert correlations and detect cyberattacks as soon as possible before the attack occurs by observing the attack plan. An attack plan is a series of procedures that an attacker follows until he or she achieves the goal. The proposed system detects the attack plan by using the available history of observations. Using the DAPRA 2000 data set, the authors have found that their system reduces false reporting of attacks and does not require an attack scenario or knowledgeable expert to use.

Naïve Bayes is a simple form of a general Bayesian learning network. Therefore, it has the same problem of being probabilistic. It is called "naïve" because it assumes that the variables are independent of each other, which is not correct in reality [53].

Hee *et al.* [54] implemented a system to automatically detect signals of cyberbullying content in social media texts. They contributed to the field by developing a system to detect cyberbullying with not only aggressive language, but also implicit content, which they explained as difficult as many types of implicit cyberbullying; such as curses, defamation, and encouragement, that may have different types of attitudes. To do so, they utilized binary and linear support vector machine classifiers. They applied the proposed system to texts in English and Dutch, working with a dataset of 113,698 English and 78,378 Dutch ASKfm posts. An SVM classifier was implemented using the LIBLINEAR library in Python due to its high ability to perform large linear classification. After optimization, the new model achieved maximum F1-scores of 58.72% and 64.32% for Dutch and English, respectively.

Vijayanand *et al.* [55] proposed a new IDS for securing a wireless mesh network using a genetic algorithm for feature selection and SVM as a classifier. The proposed system was tested using a simulated wireless mesh network dataset in Network Simulator 3 (NS3). They achieved high accuracy of attack detection (95.5%).

Ofoghi *et al.* [56] proposed a tool with hybrid features that detects phishing emails by extracting feature vectors. This tool uses four processes: feature vector generation, machine learning, method selection, and inductor and feature evaluation. As another attempt, Zulkefli *et al.* [57] investigated the methods for making advanced persistent threat (APT) attacks on smartphones. APT attacks are planned attacks combining social engineering and malware; one of the most popular types of APT attacks is phishing. The authors have utilized a decision tree classifier to distinguish legitimate websites from fake websites, achieving accuracy of 90%.

As most IDSs can prevent known pattern attacks, Ahn *et al.* [58] proposed a new paradigm system to predict unknown attacks. The authors focused on APT attacks, which are more dangerous than normal attacks because the attacker monitors the victim to collect information, identify vulnerabilities, and search for the most privileged users, such as the administrator. Their paradigm system was based on big data techniques, which are used in fields such as machine learning, data mining, and artificial intelligence. The techniques applied by the researchers included prediction using regression analysis, classification using SVM or logistic regression analysis, the relation rule for discovering hidden relationships amongst data, and atypical data mining for analyzing the data that cannot be represented with numbers (e.g., text, images and videos).

Darus *et al.* [59] focused on the Android platform; the popularity of the Android operating system in recent years has encouraged criminals to target it with many types of malware intended to steal sensitive information from users' smartphones. The authors utilized visualization techniques to detect new types of malware by converting APK files to 8-bit greyscale images. A GIST descriptor was used to extract features from the converted images. A GIST descriptor is a holistic filter for an image, it provides a low dimensional image with some information to understand the view in an image [60]. Three types of classification algorithms—KNN, decision tree, and random forest (RF)—were utilized. The authors discovered that RF has better accuracy than the KNN and decision tree methods. In the KNN algorithm, all features in the dataset are equally important and are used in same amounts; thus, no features are labeled as important or more relevant, which is not helpful for detecting cybercrimes with many useless features [45]. Generating images was difficult; half of the malware samples were not converted to images as the APK files were corrupted or did not have the ".dex" class, which is necessary for conversion.

Vuong *et al.* [61] proposed a method to detect cyberattacks on mobility devices, such as robots, that considers the devices' mobile nature and energy consumption as well as the physical impact of the attack. Decision tree C 5.0 algorithm is used in this study to implement the classification process. The proposed method on mobile robotic vehicles faces four types of attacks: DoS, SQL injection, and two types of malware (one targeting the network and one targeting the central processing unit) [61].

Al-diabat [62] investigated phishing attacks and ways to minimize this problem. As every phishing attempt is linked to a fake website, Al-diabat tried to detect fake websites by analyzing the features that distinguish between legal and illegal websites, including a lengthy URL, IP address, and an "@" symbol within the URL. The author tested the possibility of reducing the number of website features through feature selection, which filters out the training data to identify specific attributes that best represent the training data and all attributes. The most effective attributes are selected to minimize computational time and resources, reduce the search space by omitting irrelevant features, and ease the classification process. Al-diabat used information gain and symmetrical uncertainty. This type of selection method should not affect the detection of illegal websites. After the most relevant features are selected, the classification process is initiated to test the efficiency of the selected features. The researcher used the C4.5 algorithm, which is a tree-based algorithm, and the incremental reduced error pruning (IREP) algorithm, which is a greedy algorithm. The WEKA software tool was used, and the data were real data obtained from the University of Irvine Repository, Phishtank website, and Yahoo! Directory [62].

Using decision trees to detect cybercrimes has certain drawbacks. For example, detection of cybercrime cannot be applied when the tree is full of leaves, because detailed questions were asked during the investigation process due to the type of crime or incomplete information about the cybercrime or cybercriminal. All machine-learning algorithms are generally affected by noise in the training data, which may be observed at the feature or label level. Table 4 summarizes the machine-learning-based techniques of cybercrime detection.

Nath [63] used a clustering algorithm with K-means clustering for data mining to help detect crime patterns. Clusters (of crime) have a special meaning, referring to a geographical group of crimes (i.e., a lot of crimes in a given geographical region). Additionally, the K-means clustering algorithm is sensitive to outliers and noise in data. K-means methods could converge data quickly, but they would not guarantee that when the data get converged would achieve the correct answer. Furthermore, K-means is an unsupervised learning algorithm, and therefore, the correct answers are not known [45].

C. CYBERCRIME DETECTION USING NEURAL NETWORK

A neural network is a simulation of how the human brain works. The brain consists of nerve cells that can learn, which are represented by neurons in the neural network. These neurons can do training and learn by themselves based on previous knowledge. This allows the neural network to find a reasonable solution for similar problems of a similar class for which it is not explicitly trained. Neural networks have a high degree of fault tolerance against noisy input data which is considered an advantage in comparison to machine learning algorithms [64].

Raiyn [65] described some types of cyberattacks as well as some of the strategies that have been used to detect cybercrimes, such as embedded programming, agent-based methods, software engineering, and artificial intelligence approaches. The researcher discussed the detection of cybercrimes in the cloud, presenting some studies that have been done on this topic, and introduced the concept of utilizing IP addresses to determine users' geographical location (i.e., country, city, and street) as well as for real-time cyberattack detection.

TABLE 4. Summary of cybercrime detection techniques using machine learning.

Ref.	Technique	Task	Data set source	Results
Nandhini and Sheeba [46]	Levenshtein distance algorithm and naïve Bayes classifier	Detect cyberbullying	FormSpring.me, MySpace.com	95% confidence interval.
Reynolds *et al.* [47]	C4.5 decision tree and instance-based learner	Detect cyberbullying	FormSpring.me	Both learners achieved accuracy of 78.5%.
Dinakar *et al.* [48]	Naïve Bayes, JRip, J48, and support vector machine	Detect cyberbullying	YouTube comments	In terms of accuracy, JRip obtained the best results. In terms of reliability, SVM was the most reliable, according to KAPPA statistics.
Al-garadi *et al.* [49]	SVM, naïve Bayes, KNN, and decision trees	Detect cyberbullying	Twitter	Naïve Bayes showed the best performance.
Uzel *et al.* [50]	A fuzzy set based on weighting methods; SVM and naïve Bayes multinomial as classifiers	Detect CTE in the context	Antisocial behavior data set	Fuzzy set-based weighting method with SVM outperformed the other methods with an accuracy of detection of up to 99%.
Haider *et al.* [51]	Naïve Bayes and SVM	Detect cyberbullying in the Arabic language	Facebook, Twitter	Naïve Bayes achieved 90.1% accuracy with a high rate of misclassification (64.7%). SVM achieved 93.4% accuracy with a high rate of false alarms (67.6%).
Benferhat *et al.* [52]	Naïve Bayes	Observe attack plans	DAPRA 2000 dataset	The system reduced the false reporting of attacks and did not require an attack scenario or a knowledgeable expert to use.
Hee *et al.* [54]	Binary classifier and linear SVM classifier	Detect implicit cyberbullying	Data set of 113,698 English and 78,378 Dutch ASKfm posts	Maximum F1 scores of 58.72% and 64.32% for Dutch and English texts, respectively.
Vijayanand *et al.* [55]	Genetic algorithm for feature selection and SVM as a classifier	Develop IDS for wireless mesh network	Simulated wireless mesh network using Network Simulator 3	The system achieved 95.5% accuracy.
Ofoghi *et al.* [56]	Feature vector generator, machine learning, method selection inductor, feature evaluation	Detect phishing emails	Nazario datasets, phishing emails from 2004–2007, SpamAssassin	The tool achieved 97% accuracy.
Ahn *et al.* [58]	Prediction using regression analysis, classification using SVM or logistic regression analysis, relation rule	Predict unknown attacks	Not implemented	N/A
Darus *et al.* [59]	KNN, decision tree, RF	Detect cybercrimes on the Android platform	APK files	RF had higher accuracy than the KNN and decision tree methods.
Al-diabat [62]	Feature selection through information gain and symmetrical uncertainty, classification via the C4.5 and IREP algorithms	Investigate phishing attacks	Real data from the University of Irvine Repository, Phishtank website, Yahoo! Directory	C4.5 achieved accuracy of 96% and the IREP algorithm achieved accuracy of 95%.
Nath [63]	K-means clustering and weighting technique to measure the significance of cybercrime attributes	Detect crime patterns	A sheriff's office.	A geo-spatial plot was used to determine cybercrime regions on a map.

Jiang and Cybenko [66] discussed a distributed correlation IDS. A distributed system consists of web servers, a Domain Name Server (DNS), a database server, routers, and switches. Attacks can occur in different places and affect several components in the network during different times. Places are referring to different locations in the network, such as servers, firewalls, etc., while time refers to when an attack is initiated inside the network.

Zhang and Yuan [67] utilized a neural network to detect phishing attacks. The authors have used multilayer feedforward neural network, achieving accuracy of 95% for detecting phishing attacks.

Manzoor and Kumar [68] proposed an IDS that utilized a feedforward neural network model trained using the Levenberg-Marquardt training model. The proposed IDS reduced the number of features when it is tested using Knowledge Discovery from Data (KDD '99) dataset. Accuracy of 99.93 % was achieved for detecting DoS attacks and accuracy of 96.51% was achieved for detecting user to root (U2R) attacks. U2R attacks happen when a normal user gain access to privileged super (root) user [69]. On the other hand, Shenfield *et al.* [70] proposed an IDS that uses an artificial neural network (ANN) to detect shell code using a network traffic dataset. They achieved accuracy of 98%. While, Liang *et al.* [71] proposed an IDS to detect attacks in VANETs, which are wireless and dynamic networks. The authors utilized a growing hierarchical SOM (GHSOM) classifier, which is a neural network algorithm, to improve the IDS. The system was tested with a Network Simulator (NS2) and a simulation of urban mobility (SUMO) on two data sets: (1) a normal scenario in which all the simulated vehicles are legitimate and (2) a rogue scenario in which some rogue vehicles were simulated in the data set. When rogue vehicles accounted for up to 40% of all vehicles, 99.69% performance was achieved. A summary of the neural network-based cybercrime detection techniques is provided in Table 5.

TABLE 5. Summary of cybercrime detection techniques using neural network methods.

Ref.	Technique	Task	Data Set Source	Results
[65]	Utilize IP addresses to determine the user's geographical location	Detect cyber-crimes in the cloud	Not implemented	N/A
[66]	Distinguish attacks using different signatures based on time and space in the network.	Discuss the distributed correlation IDS and develop a process query system	Not implemented	N/A
[67]	Develop a multilayer feedforward neural network	Detect phishing attacks	Data set of real-world examples of spam and phishing email	Achieved 95% accuracy for detecting phishing attacks
[68]	Feedforward neural network model	Develop IDS	KDD '99 dataset	Achieved accuracy of 99.93% for detecting DoS attacks and 96.51% for detecting U2R attacks
[70]	ANN	Develop IDS to detect shell code	Network traffic dataset	Achieved accuracy of 98%

D. CYBERCRIME DETECTION USING DEEP LEARNING

Haider *et al.* [72] used a feedforward neural network to detect Arabic cyberbullying, using tweets as the data set. The authors changed different parameters in the neural network to detect changes and achieve better accuracy. The parameters include the number of hidden layers, the number of epochs, and batch size. The authors have discovered after several training experiments that after few epochs have obtained better performance. The optimal batch size is 16, and 7 hidden layers are also found to be an optimal choice to achieve good accuracy and performance. The best accuracy achieved using their proposed method was 94.56%.

Dadvar and Eckert [73] detected cyberbullying on different social media platforms (i.e., Twitter, Wikipedia, and Formspring). The authors have used four deep neural network-based models: the convolutional neural network (CNN), long short-term memory (LSTM), bidirectional LSTM (BLSTM), and BLSTM with attention. The CNN is useful for text and image classification, while the LSTM neural network is useful for text classification. BLSTM encodes information in two directions: backward and forward. The authors applied models that transferred training at different levels, such as the complete, feature, and model levels. Complete-level transfer allows any model used to train one dataset to transfer training to another dataset without additional training. The authors tried to overcome the imbalance in cyberbullying posts by increasing the dataset. It was discovered that the CNN model outperforms machine-learning models for detecting cyberbullying.

AlShammri [74] noted that a preprocessing technique should be conducted on datasets to achieve high accuracy when categorizing Arabic texts. The author has investigated the impact of using preprocessing techniques on the performance of three machine learning algorithms: C4.5, naïve Bayes, and Discriminative Multinomial Naive Bayes classifier (DMNBText). DMNBText has better results than the two other algorithms.

Most studies on the detection of cyberbullying have adopted a text-based view. However, Cheng *et al.* [75] tried to consider different types of data, such as images, videos, and likes/shares. An XBully tool was used to detect cyberbullying in a multi-modal context among multiple types of data using a cross-modal correlation learning approach.

Aksu and Aydin [76] implemented IDS models to detect port scan attempts using deep learning and support vector machines. The new systems are based on the CICIDS2017 data set, which was developed by Canadian Institute for Cyber Security. The authors compared the performance of two systems: deep learning and SVM. The systems achieved accuracies of 97.80% and 69.79%, respectively. Whereas, Karie *et al.* [77] presented a framework for cyber forensics investigations using deep learning. This framework consists of five stages: initialization, identification of digital evidence sources, a deep learning investigation, forensics reporting, and decision-making by law enforcement.

Almiani *et al.* [78] developed an IDS for the Internet of Things (IoT) and FOG security. IoT is a novel model based on wireless telecommunication that allows interaction between different schemes using special unique addressing in order to achieve a common goal. Examples of those schemes include radio frequency identification (RFID), mobile phones, and sensors [79]. Almiani *et al.* utilized a deep recurrent neural network on the NSL-KDD data set; they measured the new system's performance using two matrices: Cohen's kappa coefficient and the Matthews correlation coefficient.

Kasongo and Sun [80] proposed an IDS for a wireless network using deep long short term memory as a classifier. The proposed IDS was evaluated using the NSL-KDD data set, and it achieved 86.99% accuracy on the test data.

Lim *et al.* [81] utilized deep reinforcement learning (DRL) techniques to predict the missing and hidden relationship between the criminal in criminal network due to the lack of criminal databases. Given, only small criminal databases are available, therefore, normal machine learning algorithms are not sufficient in such cases and DRL algorithm provides better performance. Another research tackled this issue in [82] presented by Lim *et al.* utilizing time evolving deep reinforcement learning (TDRL) and comparing it with meta-data fusion model (FDRL), where meta data fusion is extracted from the real environment such as recordings and arrest warrants. Table 6 summarizes the deep-learning-based cybercrime detection techniques applied in previous studies.

TABLE 6. Summary of cybercrime detection techniques based on deep learning techniques.

Ref.	Technique	Task	Data Set Source	Results
[72]	Feedforward neural network	Detect Arabic cyber-bullying	Twitter	The best accuracy achieved was 94.56%
[73]	CNN, LSTM, BLSTM, BLSTM with attention	Detect cyber-bullying	Twitter, Wikipedia, and Formspring	DNN model out-performed the other models
[74]	Investigate the performance of three machine learning algorithms: C4.5, naïve Bayes, and DMNBText	Achieve high accuracy for categorization of Arabic texts	BBC data set and CNN data set	DMNBText achieved better results than the other two algorithms
[76]	Deep learning and SVMs	Detect port scan attempts	CI-CIDS2017 data set	Accuracy of 97.80% and 69.79%, respectively

E. CYBERCRIME DETECTION USING FUZZY LOGIC NEURAL NETWORK

Fuzzy logic is a combination of classical and fuzzy sets. It measures the degree of truth, or the degree to which we can say that an item belongs to the set. It does not categorize items into 0 and 1, where 0 indicates that a lack of belonging to a set and 1 indicates belonging to a set. Rather, in fuzzy logic, 0 and 1 indicate extreme cases of truth [83]. This logic is needed for detecting cybercrimes because of the uncertainty and doubt related to collecting evidence. Flexibility is required to assign items to the appropriate group and thus identify the case as a cybercrime or not and the perpetrator as a cybercriminal or not.

Fatima *et al.* [84] defined the soft computer application technique, which is used when a solution cannot be predicted due to lack of supportive and detailed information. Soft computer techniques help deal with and adapt to uncertainty in emotional and physical characteristics. The researchers focused on two soft computing applications: neuro-fuzzy logic and ANN. They compared the two soft computing applications, and the results showed that neuro-fuzzy logic is superior for detecting cybercrimes.

Ahmed and Mohammed [85] have utilized the fuzzy min-max approach to detect the attackers' intentions in real time. The process involved two steps. In the first step, the pattern of the attack is determined. While in the second step, the intention of the attack is identified by investigating the similarities between the characteristics of the pattern and the evidence that was collected from the attack by utilizing a fuzzy min-max neural network.

Chandrashekhar and Kumar [86] proposed an IDS using a fuzzy min-max neural network and tested it with the KDD '99 data set. In contrast, Aldubai *et al.* [87] proposed an IDS to detect cybercrimes utilizing a fuzzy min-max neural network classifier and Principal component analysis (PCA) as a feature extraction algorithm. They tested this system using KDD '99 and NSL-KDD.

Azad and Jha [88] proposed a new IDS utilizing a fuzzy min-max neural network as a classifier and a genetic algorithm to optimize the hyberbox. This IDS was tested using KDD '99. A year later, Azad and Jha [89] proposed another IDS utilizing a fuzzy min-max neural network as a classifier and particle swarm for optimization, again testing it with KDD '99.

Shalaginov *et al.* [90] emphasized the importance of utilizing soft computing applications in forensics investigations due to the large amount of data that must be analyzed to identify evidence to help investigators. In normal methods, this process consumes time and resources. Soft computing applications, such as fuzzy logic, machine learning and data mining, facilitate big data analytics to assist investigators in detecting cybercrimes and criminals. On the other hand, Barraclough *et al.* [91] utilized fuzzy logic to detect phishing attacks using five different tables in which 288 features were stored with two-fold cross validation. They achieved high accuracy.

Saidi *et al.* [92] aimed to identify cyberterrorist committees amongst other committees. They used an evidential C-means (ECM) algorithm to cluster network data from the John Jay ARTIS Transnational Terrorism (JJATT) database and Global Terrorism Database (GTD). The researchers tried to improve Constrained Evidential C-Means (CECM) clustering process using two constraints: must-link and cannot-link. Must-link means that two objects must be classified in the same cluster, while cannot-link means that two objects cannot be allocated to the same cluster. After these constraints were applied, a new algorithm, called the constrained ECM algorithm, was proposed. Table 7 summarizes the cybercrime detection techniques that use fuzzy logic neural network.

F. CYBERCRIME DETECTION USING DATA MINING

Sindhu and Meshram [93] have proposed a system for detecting cybercrimes that uses an a priori (i.e., data mining)

TABLE 7. Summary of fuzzy logic neural network-based cybercrime detection techniques.

Ref.	Technique	Task	Data set	Results
[84]	Neuro-fuzzy logic and an ANN	Compare the two methods for detecting cybercrimes	DAPRA data set	Neuro-fuzzy logic is superior for detecting cyber-crimes compared to the ANN
[85]	Fuzzy min-max approach	Detect the attacker's intention in real time	Page blocks data set	Accuracy ≈ 94% with training data sets of different sizes
[86]	Fuzzy min-max neural network	Develop IDS	KDD '99	Accuracy: 95.17%
[87]	Fuzzy min-max neural network and PCA	Develop IDS	KDD '99	Accuracy: 99.96%
			NSL-KDD	Accuracy: 99.05%
[88]	Fuzzy min-max neural network and genetic algorithm	Develop IDS	KDD '99	Accuracy: 95.9391%
[89]	Fuzzy min-max neural network and particle swarm	Develop IDS	KDD '99	Accuracy: 97.46%
[91]	Fuzzy logic	Detect phishing attacks	Data set generated via a program that can automatically generate phishing websites	High accuracy
[92]	Evidential C-Means algorithm	Identify cyber terrorist committees among other committees	JJATT database and GTD	High accuracy of 84.81% with medium complexity

algorithm. The researchers started from case reports, extracting and determining the attributes/variables of the cases. The a priori algorithm was applied to the set of variables to identify frequent item sets. Although the proposed algorithm was not implemented, the algorithm is useful for detecting the attributes and variables of cybercrime case reports. The researchers utilized visualizations, such as bar chart or graphs, to make analysis easier for investigators.

Shahresani *et al.* [94] proposed a new system called a visual threat monitor, which combines data mining and visualization to detect botnet behavior in a network. Data mining is applied to analyze patterns of network packets using packet trace files to distinguish between regular and irregular packets. It can extract adequate data for analysis even when a large amount of data is contained in packet trace files. The authors have used several visualization techniques, such as histograms, grid visualizations, and scatter plots, to help the network administrator detect botnets easily. They have also implemented data mining techniques to achieve accurate results for classification, clustering, aggregation, statistical analysis, and flow correlation. They finally have clarified the differences between the techniques to determine which was able to most accurately detect cybercrimes.

However, the study presented by Shahresani *et al.* was limited to botnets, and the authors did not practically test the methodology. In addition, they could not apply visualization techniques to all data due to the large amount of time that would be required. Thus, they visualized data selected from the data mining process. Yet, utilizing their proposed method could miss some true botnet attacks that were not detected by the data mining process. Additionally, some of the data mining algorithms have drawbacks inherently. For example, the flow correlation algorithm only uses one attribute for comparison, which is not sufficient for proper decision-making. In addition, the basic function of classification is comparison of incoming packets with previous patterns, and thus this technique cannot detect new attacks.

Chen *et al.* [95] examined general crimes rather than focusing on cybercrimes. They have implemented a framework to identify the association between crimes and effective data mining techniques to categorize crimes. One category included cybercrimes. The authors utilized data mining because it has the power to analyze large amounts of data quickly and efficiently. The researchers explained the different data mining techniques used for different types of crime, including their strengths and weaknesses.

Khan *et al.* [96] discussed several data mining techniques, such as association, clustering, and outlier detection. The researchers applied a data mining technique (i.e., pattern recognition) to detect DoS attacks as examples of cybercrimes. They applied pattern recognition to log files and checked the log files against a threshold to identify whether activities were normal or abnormal.

Lekha and Prakasam [97] have focused on the banking sector, which is a natural target for cybercriminals. Banking cybercrimes include credit card fraud, hacking, DoS attacks, money laundering, phishing, and ATM card cloning. The researchers proposed a system and applied it to police reports available on the Internet. The researchers attempted to find the most common patterns in the cybercrime data set to produce association rules via rule association mining. Then, they applied clustering using the K-means partition algorithm. Thereafter, they have applied classification to create several models with unknown patterns. For classification, the researchers utilized a J48 algorithm to create classified output in the form of a decision tree and rule sets. Finally, the researchers applied influenced association classification to achieve precision. However, the proposed system was not experimentally tested and thus obtained no results.

In another attempt, Smadi *et al.* [98] utilized the Random Forest (RF) algorithm to detect phishing emails. Using 32 features, the authors extracted the feature metric from the email content in the preprocessing stage. They have achieved accuracy of 98.87%.

Kwon *et al.* [99] focused on how players earn money in online games. In such games, an unofficial market sells recently raised money, creating gold farming groups (GFGs). GFGs are organizations that sell virtual goods to online game players for profit. The researchers proposed a technique to detect GFGs based on some behavioral attributes and a rule-based community, attempting to differentiate real players from bots. They constructed a graph to describe the characteristics of virtual economy transactions, and they traced and monitored all abnormal transactions to extract features to help detect GFGs.

Fatima *et al.* [100] investigated the effectiveness of utilizing dynamic data fusion and visualization in forensic investigations. Their study was based on banking systems and focused on IP spoofing. Data fusion is the science of merging data from different sources to achieve accurate, high-quality data by clearing insignificant information, transforming raw data from different sources (e.g., PCs, routers, firewalls, and servers) into useful data, and breaking data into small portions of useful information to ease the analysis process. The researchers implemented the system using Matlab via a neural network toolbox, which included self-organizing maps, to model and cluster the data. Visualization techniques and bar charts were used to represent the data.

Data mining is generally sensitive to the quality of input data, but the data may be inaccurate, have missing information, or have data entry errors. Moreover, mapping real data to data mining attributes is not always easy, and it often requires skilled data miners and crime data analysts with good domain knowledge. The techniques for cybercrime detection that use data mining are summarized in Table 8.

TABLE 8. Summary of cybercrime detection techniques using data mining techniques.

Ref.	Technique	Task	Data set source	Results
[93]	A priori algorithm	Detect the attributes and variables of cybercrime case reports	Not implemented	N/A
[94]	Various data mining techniques used to achieve accurate results, such as classification, clustering, aggregation, statistical analysis, and flow correlation	Detect botnet behavior in the network	Not implemented	N/A
[96]	Pattern recognition in the log files and a priori algorithm	Detect DoS	Log files	No results shown in this research
[97]	Clustering using a K-means partition algorithm and J48 algorithm	Detect cybercrimes	Banking sector and police reports available on the Internet, articles, blogs, and news	No results shown in this research
[98]	RF algorithm	Detect phishing emails	Not mentioned	Accuracy of 98.87%

G. CYBERCRIME DETECTION USING OTHER TECHNIQUES

This subsection covers other techniques that have been developed to detect cybercrimes based on other detection methods such as computer vision, biometric, cryptography, and forensic tools. Computer vision techniques focus on analyzing and interpreting images [101]. Computer vision techniques have been used to detect cybercrimes, especially phishing, by analyzing the URLs of websites to determine whether they are legitimate or fake. An example of such research was conducted by Rao and Ali [102], who suggested a technique to detect phishing websites by combining a whitelist and visual similarity-based technique. They utilized a speeded-up robust features (SURF) detection tool to extract features from fake and phished websites. The whitelist, which contains all legitimate URLs, was used to check URLs. Then, a visual similarity-based technique was used to identify the legitimacy of URL via finding the most similar scores either it is legitimate or suspicious URLs.

Another researchers used biometric techniques to defend cyber crimes such as Ahmed *et al.* in [103] proposed an approach to be applied in Bangladesh to detect cybercrimes over the Internet. The new framework requires each Internet's user to register a national ID and password to gain access to the Internet, and foreigners can gain access using their visa's number. Then, the users' faces and fingerprints are scanned and saved into the cloud for biometric verification. Next, users must provide their birth certificate number. Finally, either a phone number or email address is required to complete the activation process. This process would ensure that only legitimate users could gain access to the Internet. The Bangladesh Telecommunication Regulatory Commission will verify users' Internet ID and password in the cloud, and users will gain access to the Internet. All of their activities will be saved in an activity log in the cloud to detect potential cybercrimes. The proposed architecture was tested on 16 volunteers using a network simulator called Packet Tracer. The results showed that the proposed framework could accurately detect cybercrimes.

Cryptography is another methodology that has been utilized to detect cyber crimes, where Derhab *et al.* [104] tackled the spam botnet detection problem via presenting a security framework called Spam Trapping System (STS) which is responsible for providing a third line of detecting and preventing the spam botnet from spreading to the other hosts. Spam Trapping System uses encrypted emails to distinguish between the legitimate emails and spam emails. This distinguish process uses cryptographic key in legitimate email. The users, the email application, and STS system know the cryptographic key. On the other hand, spam emails are not encrypted with known key. Therefore, those spam emails are not sent outside the host. By this procedure, the third line of protection is created and the spam email is prohibited from going outside the host.

Forensics tool-based analysis techniques have also been utilized to detect cyber-crimes; for instance, Meera *et al.* [105] attempted to investigate cybercrimes using a virtual machine called VMware. Today, criminals use virtual hard disks to hide evidence. Thus, the researchers used VMware files to find criminal evidence located in a virtual hard disk via live internal data acquisition and extraction of raw data from various grains. A grain is a block of sectors that contains data in a virtual hard disk. Raw data are retrieved and then processed using several forensic techniques to extract useful information. The retrieved files are labeled ''.vmdk'', which stands for virtual hard disk file of VMware.

Another research by Mutawa *et al.* [21] used a combination of forensic technical skills and a Bureau d'Enquetes et d' Analyses's (BEA) investigation system to investigate child pornography transmitted through a peer-to-peer (P2P) file-sharing network. They have applied a BEA analysis methodology to analyze the evidence they obtained in each of the 15 cases obtained from the Department of Electronic Evidence of the Dubai police. The data contain images from each case and some related electronic files, such as log files, contact lists, emails, history files, and pictures. The researchers have investigated each case separately with a deductive approach. Thus, they needed to understand each case individually and analyze the digital evidence using four BEA strategies: crime scene characteristics, equivocal forensic analysis, offender characteristics, and victimology. The researchers found that the offenders attempted to conceal their crimes using naïve methods, such as nested folders to hide pornographic images, file deletion, and uninstallation of the P2P sharing software they used. The offenders that were investigated in this study did not exhibit any technical expertise and they did not use any wiping tools. Private or anonymous web browsers, such as The Onion Router (TOR) or passwords that are difficult to guess have been used while attempting their cybercrime attack. Only one user showed some technical expertise, as he encrypted his hard drive and installed VMware. The study indicates that utilizing BEA in forensics investigations will help detectives find criminals and analyze the scene and digital evidence of the cybercrime to obtain reliable data. Table 9 summarizes the cybercrime detection techniques that use different types of techniques.

IV. CYBERCRIME TESTING DATASETS

A review of benchmark datasets was presented in [106]. The KDD '99 data set was generated in 1999 by Stolfo *et al.* [107]. This dataset focuses on four types of attacks: DoS, U2R, remote to local, and probing attacks. However, Abubakar *et al.* [106] mentioned that the KDD '99 dataset is no longer efficient for IDSs due to the fact that it is an old dataset, and there have been many cybercrimes happened within the psat 20 years, hence it will provide inaccurate results. In addition, Tavallaee *et al.* [108] stated that about 78% and 75% records in the training set and test set, respectively, are duplicates, which will affect the evaluation process for the detection algorithm. Thus, NSL-KDD was created in 2009 by Tavallaee *et al.* [108]. This dataset consists of KDD dataset records, minus all the duplicate or redundant records in the training and testing data sets.

On the other hand, DAPRA 2000, which includes DDoS attacks, was generated in 2000 by the MIT Lincoln Laboratory [109]. While, Abubakar *et al.* [85] also reviewed the University of New Mexico (UNM) dataset, which was proposed in 2004 [110]. UNM has several limitations, including a limited scope of cybercrimes, a focus on a single process, and an incomplete sampling of the target operating system [111].

Creech and Hu [111] generated a new benchmark dataset called Australian Defence Force Academy Linux (ADFA-LD12) in 2013. It consists of system call traces and focuses on six types of attacks: Hydra-FTP, Hydra-SSH, Adduser, Java-Meterpreter, Meterpreter, Webshell [112].

TABLE 9. Summary of cybercrime detection techniques using other techniques.

	Ref.	Technique	Aim	Data Set Source	Results
Computer Vision	[102]	Combination of whitelist and visual similarity-based technique	Detect phishing websites.	Phishtank: 20 legitimate and 400 phishing web pages.	System fails when there is big difference between real and fake website.
Biometric Technique	[103]	Biometric verification (face and fingerprint)	Detect cybercrimes over the Internet.	16 volunteers from Bangladesh	N/A
Cryptography	[104]	Encrypted emails	Spam botnet detection.	N/A	N/A
Forensics tools	[21]	BEA investigation system	Investigate child pornography	15 cases collected from Dubai Police	Help investigators to analyze evidences.
	[105]	Several forensic tools	Detect cybercrimes.	.vmdk files	N/A

Moustafa and Slay [113] presented the UNSW-NB15 dataset, which is network-based. This dataset focuses on nine types of attacks: fuzzers, backdoors, DoS, exploits, reconnaissance, shellcode, worms, analysis (port scan, HTML

TABLE 10. Review of cybercrime datasets.

Dataset	Advantages (features)	Deficiencies
KDD Cup '99 [68] [86] [87] [88] [89]	- Created in 1999. - Includes 4,900,000 single-connection vectors. - It has 41 features. - It was the first attempt to initiate a benchmark for an intrusion detection system (IDS). - Used to evaluate new IDSs for research purposes.	- It does not fit newer techniques that utilize machine learning, data mining, etc. Those fields are sensitive to data impurity [108, 111]. - It does not account for the current type of attacks, which will have an impact on the evaluation process for new IDSs and will lead to inaccurate results [111, 113]. - It has duplicate records in both the training and testing stages, which cause inaccurate evaluating results [108, 113]. - Because of the pre problem, researchers will achieve a high detection rate in evaluating their IDS when they use the KDD dataset [108].
NSL-KDD [78] [80] [87]	- Created in 2009. - Includes KDD '99 without redundant records [108]. - It has 41 features. - Redundant records between training and testing set in KDD dataset were removed without affecting the number of records in both datasets [108].	- It is an old dataset and it does not fit the new techniques utilizing machine learning, data mining, etc [111]. - It does not account for the current type of attacks, which will have an impact on the evaluation process for new IDSs and will lead to inaccurate results [113]. - It inherits some of the drawbacks of KDD dataset, such as missing records [113].
ADFA-LD	- Created in 2013. - Includes 5,951 traces [111], and 2,747,550 system calls. - It has 175 features. - It covers the latest attacks type. - It is available as a free online dataset.	The lack of defined meanings and descriptions of its attributes (input and output attributes) means that the dataset is not easy to understand [106].
UNSW-NB15	- Created in 2015. - Includes Four CSV files: three contain 700,000 records each, and the fourth contains 440,044 records [113]. - It has 49 features. - It is a newer dataset. - Contains the most modern attack types. - Freely available for research purposes [113].	- The dataset is complex due to behavior similarity in the new type of attacks [114].
CICIDS2017 [76]	- Created in 2017. - Includes 3,119,345 records. - It has 83 features. - A modern dataset containing new types of attacks that have not been considered by other datasets. - Fulfills all the requirements for an IDS dataset, including labelled dataset, a complete network configuration, available protocols, complete traffic, complete capture, attack diversity [115].	- It is divided to eight files, which require more effort from the researchers to process the files individually [115]. - It has a huge amount of data that increases the overhead for data loading and data processing [115]. - There are some missing class labels and missing data information [115]. - It has a high-class imbalance. Therefore, the IDS will be biased towards the majority class in this dataset, thus increasing the false detection rate [115].

file penetration, spam), and generic (a technique that works against all block ciphers). The CICIDS2017 dataset was presented in 2017 by the Canadian Institute of Cyber Security [93]. It contains 14 types of attacks. A summary of the cybercrime datasets is provided in Table 10.

V. CONCLUSION

The comprehensive review in this paper has covered several types of cybercrimes and analyzed numerous studies regarding their achieved detection rates as well as some of their limitations. The presented state of the arts in this paper has been evaluated and a comparison was carried out via some tabulated information as a way to demonstrate their results to identify their respective advantages and disadvantages. This study has also intensively discussed the available datasets that have been used by previous studies. Finding the proper dataset for testing and evaluating the research's method for cybercrime detection are critical challenges. The unavailability of benchmark datasets is an inevitable consequence of the lack of cooperation between law enforcement and researchers in terms of cybercriminal data collection. Another challenge is the diversity of cybercrimes, as they may happen within different platforms such as Twitter, YouTube, Instagram, or through networks; which involve different types of datasets.

To overcome the availability challenge of cybercrime datasets, it is recommended to create cybercriminal profiling that can be used by the researchers as cybercrime datasets. However, creating cybercriminal profiling requires a serious collaboration between law enforcement and researchers as well as governmental regulators. Since the information that can be included in the cybercriminal profiling, which is mostly critical, sensitive, and private, the legality for revealing this information is questionable. For this reason, researchers should find a method to protect data privacy; by these means, they may benefit from the data of cybercriminals provided by law enforcement for research purposes while also maintaining their privacy.

REFERENCES

[1] M. Yar and K. F. Steinmetz, *Cybercrime and Society*. Newbury Park, CA, USA: Sage, 2019.

[2] B. Akhgar, A. Staniforth, and F. Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Rockland, MA, USA: Syngress, 2014.

[3] M. Rouse. (2017). *Arpanet*. Accessed: Apr. 26, 2020. [Online]. Available: https://searchnetworking.techtarget.com/definition/ARPANET

[4] (2018). *The Morris Worm*. Accessed: Jan. 28, 2020. [Online]. Available: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

[5] V. Beal. (Apr. 27, 2020). *SCADA—Supervisory Control and Data Acquisition*. [Online]. Available: https://www.webopedia.com/TERM/S/SCADA.html

[6] S. Nadali, M. A. A. Murad, N. M. Sharef, A. Mustapha, and S. Shojaee, "A review of cyberbullying detection: An overview," in *Proc. 13th Int. Conf. Intellient Syst. Design Appl.*, Dec. 2013, pp. 325–330.

[7] A. Karim, R. B. Salleh, M. Shiraz, S. A. A. Shah, I. Awan, and N. B. Anuar, "Botnet detection techniques: Review, future trends, and issues," *J. Zhejiang Univ. Sci. C*, vol. 15, no. 11, pp. 943–983, Nov. 2014.

[8] D. Ramalingam and V. Chinnaiah, "Fake profile detection techniques in large-scale online social networks: A comprehensive review," *Comput. Electr. Eng.*, vol. 65, pp. 165–177, Jan. 2018.

[9] A. N. Shaikh, A. M. Shabut, and M. A. Hossain, "A literature review on phishing crime, prevention review and investigation of gaps," in *Proc. 10th Int. Conf. Softw., Knowl., Inf. Manage. Appl. (SKIMA)*, Dec. 2016, pp. 9–15.

[10] W. Z. Khan, M. K. Khan, F. T. B. Muhaya, M. Y. Aalsalem, and H.-C. Chao, "A comprehensive study of email spam botnet detection," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2271–2295, 4th Quart., 2015.

[11] H. Hassani, X. Huang, E. S. Silva, and M. Ghodsi, "A review of data mining applications in crime," *Stat. Anal. Data Mining, ASA Data Sci. J.*, vol. 9, no. 3, pp. 139–154, Jun. 2016.

[12] M. BinJubier, A. A. Ahmed, M. A. B. Ismail, A. S. Sadiq, and M. K. Khan, "Comprehensive survey on big data privacy protection," *IEEE Access*, vol. 8, pp. 20067–20079, 2019.

[13] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, "Intrusion detection by machine learning: A review," *Expert Syst. Appl.*, vol. 36, no. 10, pp. 11994–12000, 2009.

[14] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowl.-Based Syst.*, vol. 189, Feb. 2020, Art. no. 105124.

[15] J. Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*. Newton, MA, USA: O'Reilly Media, 2011, p. 316.

[16] (2016). *ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure*. Accessed: Jan. 9 2019. [Online]. Available: https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

[17] (2017). *Ukraine Power Cut 'Was Cyber-Attack'*. Accessed: Jan. 9 2019. [Online]. Available: https://www.bbc.com/news/technology-38573074

[18] V. Butrimas. (2016). *Threat Intelligence Report Cyberattacks Against Ukrainian ICS*. Accessed: Sep. 9, 2019. [Online]. Available: https://www.sentryo.net/wp-content/uploads/2017/10/EBOOK-UKRAINIAN-CYBERATTACKS-OCT-2017.pdf

[19] K. J. Higgins. (2016). *Lessons From The Ukraine Electric Grid Hack*. Accessed: Sep. 9, 2019. [Online]. Available: https://www.darkreading.com/vulnerabilities—threats/lessons-from-the-ukraine-electric-grid-hack/d/d-id/1324743

[20] K. Zetter. (2016). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[21] N. A. Mutawa, J. Bryce, V. N. L. Franqueira, and A. Marrington, "Behavioural evidence analysis applied to digital forensics: An empirical analysis of child pornography cases using P2P networks," in *Proc. 10th Int. Conf. Availability, Rel. Secur.*, Aug. 2015, pp. 293–302.

[22] D. Halder and K. Jaishankar, "Cyber socializing and victimization of women," *Temida*, vol. 12, no. 3, pp. 5–26, 2009.

[23] S. S. Chakkaravarthy, D. Sangeetha, M. Venkata Rathnam, K. Srinithi, and V. Vaidehi, "Futuristic cyber-attacks," *Int. J. Knowl.-based Intell. Eng. Syst.*, vol. 22, no. 3, pp. 195–204, Nov. 2018.

[24] C. Douligeris and D. N. Serpanos, *Network Security: Current Status and Future Directions*. Hoboken, NJ, USA: Wiley, 2007.

[25] (Nov. 26, 2019). *DoS (Denial of Service) Attack Tutorial: Ping of Death, DDOS*. [Online]. Available: https://www.guru99.com/ultimate-guide-to-dos-attacks.html

[26] H. Dalziel. (Nov. 26, 2019). *5 Major Types of DOS Attack*. [Online]. Available: https://www.concise-courses.com/5-major-types-of-dos-attack/

[27] (May 6, 2020). *SQL Injection*. [Online]. Available: https://portswigger.net/web-security/sql-injection

[28] A. Tabasum, Z. Safi, W. AlKhater, and A. Shikfa, "Cybersecurity issues in implanted medical devices," in *Proc. Int. Conf. Comput. Appl. (ICCA)*, Aug. 2018, pp. 1–9.

[29] A. Sultana, A. Hamou-Lhadj, and M. Couture, "An improved hidden Markov model for anomaly detection using frequent common patterns," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 1113–1117.

[30] J. Liang, M. Ma, M. Sadiq, and K.-H. Yeung, "A filter model for intrusion detection system in vehicle ad hoc networks: A hidden Markov methodology," *Knowl.-Based Syst.*, vol. 163, pp. 611–623, Jan. 2019.

[31] S. U. Rehman, M. A. Khan, T. A. Zia, and L. Zheng, "Vehicular ad-hoc networks (VANETs)-an overview and challenges," *J. Wireless Netw. Commun.*, vol. 3, no. 3, pp. 29–38, 2013.

[32] Y. Qiao, X. W. Xin, Y. Bin, and S. Ge, "Anomaly intrusion detection method based on HMM," *Electron. Lett.*, vol. 38, no. 13, pp. 663–664, Jun. 2002.

[33] M. Rasmi and A. Jantan, "A new algorithm to estimate the similarity between the intentions of the cyber crimes for network forensics," *Procedia Technol.*, vol. 11, pp. 540–547, Jan. 2013.

[34] F. Harrou, B. Bouyeddou, Y. Sun, and B. Kadri, "Detecting cyber-attacks using a CRPS-based monitoring approach," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Nov. 2018, pp. 618–622.

[35] N. Abouzakhar, A. Gani, G. Manson, M. Abuitbel, and D. King, "Bayesian learning networks approach to cybercrime detection," in *Proc. PostGraduate Netw. Conf. (PGNET)*, Liverpool, U.K., 2003, pp. 1–5.

[36] J. Wang, R. Wen, J. Li, F. Yan, B. Zhao, and F. Yu, "Detecting and mitigating target link-flooding attacks using SDN," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 6, pp. 944–956, Nov./Dec. 2019.

[37] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Mar. 2008.

[38] S. K. Fayaz, Y. Tobioka, V. Sekar, and M. Bailey, "Bohatei: Flexible and elastic ddos defense," in *Proc. 24th USENIX Secur. Symp. (USENIX Secur.)*, 2015, pp. 817–832.

[39] (Apr. 27, 2020). *Software-Defined Networking*. [Online]. Available: https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html

[40] P. Phaal, S. Panchen, and N. McKee, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*, document RFC 3176, Network Working Group, 2001, pp. 1–31.

[41] C. Birkinshaw, E. Rouka, and V. G. Vassilakis, "Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks," *J. Netw. Comput. Appl.*, vol. 136, pp. 71–85, Jun. 2019.

[42] (May 11, 2020). *Rate Limiting*. [Online]. Available: https://en.wikipedia.org/wiki/Rate_limiting

[43] S. A. Mehdi, J. Khalid, and S. A. Khayam, "Revisiting traffic anomaly detection using software defined networking," in *Proc. Int. Workshop Recent Adv. Intrusion Detection*. Berlin, Germany: Springer, 2011, pp. 161–180.

[44] S. Shalev-Shwartz and S. Ben-David, *Understanding Machine Learning: From Theory to Algorithms*. Cambridge, U.K.: Cambridge Univ. Press, 2014.

[45] H. Daumé, III, *A Course in Machine Learning*, vol. 5. Ciml.info, 2012, p. 69. Accessed: Jun. 23, 2020. [Online]. Available: http://ciml.info/dl/v0_9/ciml-v0_9-ch03.pdf

[46] B. S. Nandhini and J. I. Sheeba, "Cyberbullying detection and classification using information retrieval algorithm," in *Proc. Int. Conf. Adv. Res. Comput. Sci. Eng. Technol. (ICARCSET) ICARCSET*, 2015, p. 20.

[47] K. Reynolds, A. Kontostathis, and L. Edwards, "Using machine learning to detect cyberbullying," in *Proc. 10th Int. Conf. Mach. Learn. Appl. Workshops*, Dec. 2011, pp. 241–244.

[48] K. Dinakar, R. Reichart, and H. Lieberman, "Modeling the detection of textual cyberbullying," in *Proc. 5th Int. AAAI Conf. Weblogs Social Media*, Jul. 2011, pp. 11–17.

[49] M. A. Al-garadi, K. D. Varathan, and S. D. Ravana, "Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network," *Comput. Hum. Behav.*, vol. 63, pp. 433–443, Oct. 2016.

[50] V. N. Uzel, E. S. Essiz, and S. A. Ozel, "Using fuzzy sets for detecting cyber terrorism and extremism in the text," in *Proc. Innov. Intell. Syst. Appl. Conf. (ASYU)*, Oct. 2018, pp. 1–4.

[51] B. Haidar, M. Chamoun, and A. Serhrouchni, "Multilingual cyberbullying detection system: Detecting cyberbullying in arabic content," in *Proc. 1st Cyber Secur. Netw. Conf. (CSNet)*, Oct. 2017, pp. 1–8.

[52] S. Benferhat, T. Kenaza, and A. Mokhtari, "A naive bayes approach for detecting coordinated attacks," in *Proc. 32nd Annu. IEEE Int. Comput. Softw. Appl. Conf.*, Jul. 2008, pp. 704–709.

[53] (2019). *The 10 Best Machine Learning Algorithms for Data Science Beginners*. Accessed: Nov. 8, 2019. [Online]. Available: https://www.dataquest.io/blog/top-10-machine-learning-algorithms-for-beginners/

[54] C. Van Hee, G. Jacobs, C. Emmery, B. Desmet, E. Lefever, B. Verhoeven, G. De Pauw, W. Daelemans, and V. Hoste, "Automatic detection of cyberbullying in social media text," *PLoS ONE*, vol. 13, no. 10, Oct. 2018, Art. no. e0203794.

[55] R. Vijayanand, D. Devaraj, and B. Kannapiran, "Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection," *Comput. Secur.*, vol. 77, pp. 304–314, Aug. 2018.

[56] L. Ma, B. Ofoghi, P. Watters, and S. Brown, "Detecting phishing emails using hybrid features," in *Proc. Symposia Workshops Ubiquitous, Autonomic Trusted Comput.*, Jul. 2009, pp. 493–497.

[57] Z. Zulkefli, M. M. Singh, A. R. Mohd Shariff, and A. Samsudin, "Typosquat cyber crime attack detection via smartphone," *Procedia Comput. Sci.*, vol. 124, pp. 664–671, Jan. 2017.

[58] S.-H. Ahn, N.-U. Kim, and T.-M. Chung, "Big data analysis system concept for detecting unknown attacks," in *Proc. 16th Int. Conf. Adv. Commun. Technol.*, Feb. 2014, pp. 269–272.

[59] F. M. Darus, N. A. A. Salleh, and A. F. M. Ariffin, "Android malware detection using machine learning on image patterns," in *Proc. Cyber Resilience Conf. (CRC)*, Nov. 2018, pp. 1–2.

[60] M. Oujaoura, B. Minaoui, M. Fakir, R. El Ayachi, and O. Bencharef, "Recognition of isolated printed tifinagh characters," *Int. J. Comput. Appl.*, vol. 85, no. 1, pp. 1–13, Jan. 2014.

[61] T. P. Vuong, G. Loukas, and D. Gan, "Performance evaluation of cyber-physical intrusion detection on a robotic vehicle," in *Proc. IEEE Int. Conf. Comput. Inf. Technology; Ubiquitous Comput. Commun.; Dependable, Autonomic Secure Comput.; Pervasive Intell. Comput.*, Oct. 2015, pp. 2106–2113.

[62] M. Al-diabat, "Detection and prediction of phishing websites using classification mining techniques," *Int. J. Comput. Appl.*, vol. 147, no. 5, pp. 5–11, Aug. 2016.

[63] S. V. Nath, "Crime pattern detection using data mining," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. Intell. Agent Technol. Workshops*, Dec. 2006, pp. 41–44.

[64] D. Kriesel. (2007). *A Brief Introduction to Neural Networks*. Accessed: Jun. 23, 2020. [Online]. Available: http://www.dkriesel.com/en/science/neural_networks

[65] J. Raiyn, "A survey of cyber attack detection strategies," *Int. J. Secur. Appl.*, vol. 8, no. 1, pp. 247–256, Jan. 2014.

[66] G. Jiang and G. Cybenko, "Temporal and spatial distributed event correlation for network security," in *Proc. Amer. Control Conf.*, Jun. 2004, pp. 996–1001.

[67] N. Zhang and Y. Yuan, "Phishing detection using neural network," Stanford Univ., Stanford, CA, USA, CS229 Lecture Notes, 2012, pp. 1–5. Accessed: Jun. 23, 2020. [Online]. Available: http://cs229.stanford.edu/proj2012/ZhangYuan-PhishingDetectionUsingNeuralNetwork.pdf

[68] Akashdeep, I. Manzoor, and N. Kumar, "A feature reduced intrusion detection system using ANN classifier," *Expert Syst. Appl.*, vol. 88, pp. 249–257, Dec. 2017.

[69] D. Hassan, "Cost-sensitive access control for detecting remote to local (R2L) and user to root (U2R) attacks," *Int. J. Comput. Trends Technol.*, vol. 43, no. 2, pp. 124–129, 2017.

[70] A. Shenfield, D. Day, and A. Ayesh, "Intelligent intrusion detection systems using artificial neural networks," *ICT Exp.*, vol. 4, no. 2, pp. 95–99, Jun. 2018.

[71] J. Liang, J. Chen, Y. Zhu, and R. Yu, "A novel intrusion detection system for vehicular ad hoc networks (VANETs) based on differences of traffic flow and position," *Appl. Soft Comput.*, vol. 75, pp. 712–727, Feb. 2019.

[72] B. Haidar, M. Chamoun, and A. Serhrouchni, "Arabic cyberbullying detection: Using deep learning," in *Proc. 7th Int. Conf. Comput. Commun. Eng. (ICCCE)*, Sep. 2018, pp. 284–289.

[73] M. Dadvar and K. Eckert, "Cyberbullying detection in social networks using deep learning based models; A reproducibility study," 2018, *arXiv:1812.08046*. [Online]. Available: https://arxiv.org/abs/1812.08046

[74] R. Alshammari, "Arabic text categorization using machine learning approaches," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 226–230, 2018.

[75] L. Cheng, J. Li, Y. N. Silva, D. L. Hall, and H. Liu, "XBully: Cyberbullying detection within a multi-modal context," in *Proc. 12th ACM Int. Conf. Web Search Data Mining*, Jan. 2019, pp. 339–347.

[76] D. Aksu and M. A. Aydin, "Detecting port scan attempts with comparative analysis of deep learning and support vector machine algorithms," in *Proc. Int. Congr. Big Data, Deep Learn. Fighting Cyber Terrorism (IBIGDELFT)*, Dec. 2018, pp. 77–80.

[77] N. M. Karie, V. R. Kebande, and H. S. Venter, "Diverging deep learning cognitive computing techniques into cyber forensics," *Forensic Sci. Int., Synergy*, vol. 1, pp. 61–67, Jan. 2019.

[78] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simul. Model. Pract. Theory*, vol. 101, May 2019, Art. no. 102031.

[79] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[80] S. M. Kasongo and Y. Sun, "A deep long short-term memory based classifier for wireless intrusion detection system," *ICT Express*, vol. 6, no. 2, pp. 98–103, 2020.

[81] M. Lim, A. Abdullah, N. Z. Jhanjhi, M. Khurram Khan, and M. Supramaniam, "Link prediction in time-evolving criminal network with deep reinforcement learning technique," *IEEE Access*, vol. 7, pp. 184797–184807, 2019.

[82] M. Lim, A. Abdullah, N. Jhanjhi, and M. K. Khan, "Situation-aware deep reinforcement learning link prediction model for evolving criminal networks," *IEEE Access*, vol. 8, pp. 16550–16559, 2019.

[83] M. Rouse. (2016). *Fuzzy Logic*. Accessed: Nov. 26, 2019. [Online]. Available: https://searchenterpriseai.techtarget.com/definition/fuzzy-logic

[84] H. Fatima, G. N. Dash, and S. K. Pradhan, "Soft computing applications in cyber crimes," in *Proc. 2nd Int. Conf. Anti-Cyber Crimes (ICACC)*, Mar. 2017, pp. 66–69.

[85] A. A. Ahmed and M. F. Mohammed, "SAIRF: A similarity approach for attack intention recognition using fuzzy min-max neural network," *J. Comput. Sci.*, vol. 25, pp. 467–473, Mar. 2018.

[86] A. Chandrashekhar and J. V. Kumar, "Fuzzy min-max neural network-based intrusion detection system," in *Proc. Int. Conf. Nano-Electron., Circuits Commun. Syst.* Singapore: Springer, 2017, pp. 191–202.

[87] A. F. Aldubai, V. H. Humbe, S. S. Chowhan, and Y. F. Aldubai, "Intruder detection using fuzzy min-max neural network and a principal component analysis (PCA) in network data," *Int. J. Comput. Sci. Eng.*, vol. 5, no. 12, pp. 777–780, 2017.

[88] C. Azad and V. K. Jha, "A novel fuzzy min-max neural network and genetic algorithm-based intrusion detection system," in *Proc. 2nd Int. Conf. Comput. Commun. Technol.* Hyderabad, India: Springer, 2016, pp. 429–439.

[89] C. Azad and V. K. Jha, "Fuzzy min-max neural network and particle swarm optimization based intrusion detection system," *Microsyst. Technol.*, vol. 23, no. 4, pp. 907–918, Apr. 2017.

[90] A. Shalaginov, J. W. Johnsen, and K. Franke, "Cyber crime investigations in the era of big data," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 3672–3676.

[91] P. A. Barraclough, M. A. Hossain, M. A. Tahir, G. Sexton, and N. Aslam, "Intelligent phishing detection and protection scheme for online transactions," *Expert Syst. Appl.*, vol. 40, no. 11, pp. 4697–4706, Sep. 2013.

[92] F. Saidi, Z. Trabelsi, and H. B. Ghazela, "A novel approach for terrorist sub-communities detection based on constrained evidential clustering," in *Proc. 12th Int. Conf. Res. Challenges Inf. Sci. (RCIS)*, May 2018, pp. 1–8.

[93] K. K. Sindhu and B. B. Meshram, "Digital forensics and cyber crime datamining," *J. Inf. Secur.*, vol. 3, no. 3, pp. 196–201, 2012, doi: 10.4236/jis.2012.33024.

[94] A. Shahrestani, M. Feily, R. Ahmad, and S. Ramadass, "Architecture for applying data mining and visualization on network flow for botnet traffic detection," in *Proc. Int. Conf. Comput. Technol. Develop.*, Nov. 2009, pp. 33–37.

[95] H. Chen, W. Chung, J. J. Xu, G. Wang, Y. Qin, and M. Chau, "Crime data mining: A general framework and some examples," *Computer*, vol. 37, no. 4, pp. 50–56, Apr. 2004.

[96] M. A. Khan, S. K. Pradhan, and H. Fatima, "Applying data mining techniques in cyber crimes," in *Proc. 2nd Int. Conf. Anti-Cyber Crimes (ICACC)*, Mar. 2017, pp. 213–216.

[97] K. C. Lekha and S. Prakasam, "Data mining techniques in detecting and predicting cyber crimes in banking sector," in *Proc. Int. Conf. Energy, Commun., Data Analytics Soft Comput. (ICECDS)*, Aug. 2017, pp. 1639–1643.

[98] S. Smadi, N. Aslam, L. Zhang, R. Alasem, and M. A. Hossain, "Detection of phishing emails using data mining algorithms," in *Proc. 9th Int. Conf. Softw., Knowl., Inf. Manage. Appl. (SKIMA)*, Dec. 2015, pp. 1–8.

[99] H. Kwon, A. Mohaisen, J. Woo, Y. Kim, E. Lee, and H. K. Kim, "Crime scene reconstruction: Online gold farming network analysis," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 544–556, Mar. 2016.

[100] H. Fatima, S. Satpathy, S. Mahapatra, G. Dash, and S. K. Pradhan, "Data fusion & visualization application for network forensic investigation-a case study," in *Proc. 2nd Int. Conf. Anti–Cyber Crimes (ICACC)*, Mar. 2017, pp. 252–256.

[101] J. F. Peters, *Foundations of Computer Vision: Computational Geometry, Visual Image Structures and Object Shape Detection*. Berlin, Germany: Springer, 2017.

[102] R. S. Rao and S. T. Ali, "A computer vision technique to detect phishing attacks," in *Proc. 5th Int. Conf. Commun. Syst. Netw. Technol.*, Apr. 2015, pp. 596–601.

[103] A. S. Ahmed, S. Deb, A.-Z.-S. B. Habib, M. N. Mollah, and A. S. Ahmad, "Simplistic approach to detect cybercrimes and deter cyber criminals," in *Proc. Int. Conf. Comput., Commun., Chem., Mater. Electron. Eng. (IC4ME2)*, Feb. 2018, pp. 1–4.

[104] A. Derhab, A. Bouras, F. B. Muhaya, M. K. Khan, and Y. Xiang, "Spam trapping system: Novel security framework to fight against spam botnets," in *Proc. 21st Int. Conf. Telecommun. (ICT)*, May 2014, pp. 467–471.

[105] V. Meera, M. M. Isaac, and C. Balan, "Forensic acquisition and analysis of VMware virtual machine artifacts," in *Proc. Int. Mutli-Conf. Autom., Comput., Commun., Control Compressed Sens. (iMac4s)*, Mar. 2013, pp. 255–259.

[106] A. I. Abubakar, H. Chiroma, S. A. Muaz, and L. B. Ila, "A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems," *Procedia Comput. Sci.*, vol. 62, pp. 221–227, Jan. 2015.

[107] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Cost-based modeling for fraud and intrusion detection: Results from the JAM project," in *Proc. DARPA Inf. Survivability Conf. Expo. DISCEX*, Jan. 2000, pp. 130–144.

[108] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, Jul. 2009, pp. 1–6.

[109] C. Isaksson and M. H. Dunham, "A comparative study of outlier detection algorithms," in *Proc. Int. Workshop Mach. Learn. Data Mining Pattern Recognit.* Leipzig, Germany: Springer, 2009, pp. 440–453.

[110] C. S. Department. (2012). *University of New Mexico Intrusion Detection Dataset*. [Online]. Available: https://www.cs.unm.edu/

[111] G. Creech and J. Hu, "Generation of a new IDS test dataset: Time to retire the KDD collection," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2013, pp. 4487–4492.

[112] B. Borisaniya and D. Patel, "Evaluation of modified vector space representation using ADFA-LD and ADFA-WD datasets," *J. Inf. Secur.*, vol. 6, no. 3, p. 250, 2015.

[113] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2015, pp. 1–6.

[114] N. Moustafa and J. Slay, "The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *Inf. Secur. J., A Global Perspective*, vol. 25, nos. 1–3, pp. 18–31, Apr. 2016.

[115] R. Panigrahi and S. Borah, "A detailed analysis of CICIDS2017 dataset for designing intrusion detection systems," *Int. J. Eng. Technol.*, vol. 7, pp. 479–482, Dec. 2018.

WADHA ABDULLAH AL-KHATER (Graduate Student Member, IEEE) received the master's degree in computer science from King Saud University, Saudi Arabia. She is currently pursuing the Ph.D. degree with Qatar University. She is also a Lecturer in information technology with the Community College of Qatar. Her current research interests include cybercrime investigation, digital forensics, and radio frequency identification (RFID).

SOMAYA AL-MAADEED (Senior Member, IEEE) received the Ph.D. degree in computer science from Nottingham, U.K., in 2004. She is currently the Head of the Computer Science Department, Qatar University, where she is also the Coordinator of the Computer Vision and AI Research Group. She enjoys excellent collaboration with national and international institutions and industry. She is a Principal Investigator of several funded research projects generating approximately five million. She has published extensively pattern recognition and delivered workshops on teaching programming for undergraduate students. She attended workshops related to higher education strategy, assessment methods, and interactive teaching. In 2015, she was elected as the IEEE Chair for the Qatar Section.

ABDULGHANI ALI AHMED (Senior Member, IEEE) received the B.Sc. degree in computer science, in 2002, the M.Sc. degree in cybersecurity, in 2006, and the Ph.D. degree in cybercrimes and forensic investigation, in 2014. Prior to get his Ph.D. degree, he was a Lecturer in the fields of cybersecurity, computer networks, information system and management, object-oriented programming, and network administration. He has served as a Senior Lecturer with the Department of Computer Systems and Networking Department, Faculty of Computer Systems and Software Engineering, University Malaysia Pahang, Malaysia. He is currently a Senior Lecturer with the School of Computer Science and Informatics, De Montfort University, U.K. He is also the Founder and the Leader of Safecyber Systems Corporation for security solutions development. The current focus of Safecyber Corporation is developing several systems, including Safecyber, Safeware, and SafeApp. He has excellent achievements in the track of invention and innovation. In terms of inventions, his record of Intellectual Properties achievements shows two patents and several copyrights. He has managed to obtain several local and international grants to fund cybersecurity studies and research. He has published several studies and scientific articles in well-known international journals and conferences. He has a long experience in working with a higher education as a Lecturer and a Senior Lecturer, since 2004. He is currently teaching security courses, such as information security, network security, ethical hacking, computer forensic and investigation, malware analysis, and cybercrime. He currently serves as a Main Supervisor for many postgraduate (master's and Ph.D.) students who are studying and conducting studies in the area of cybersecurity, big data privacy, cloud computing security, and cybercrime investigation. His current research interests include cybersecurity, network security, cloud computing security, big data privacy, ethical hacking, malware analysis, incident response, digital forensic, and cybercrime investigation. He is a member of the International Association of Engineers (IAENG). In terms of innovation, he received many Gold, Silver, and Bronze medals from local, national, and international exhibitions. He acts as a Volunteer Reviewer for well-reputed journals, such as the IEEE SYSTEMS JOURNAL, the *Journal of Network and Computer Applications* (JNCA), IEEE ACCESS, *Wireless Networks*, *Neural Computing and Applications*, IETE Technical Review, KIIS, and JDCTA.

ALI SAFAA SADIQ (Senior Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in computer science, in 2004, 2011, and 2014, respectively. He has served as a Lecturer with the School of Information Technology, Monash University, Malaysia. He has also served as a Senior Lecturer at the Department of Computer Systems and Networking Department, Faculty of Computer Systems and Software Engineering, University Malaysia Pahang, Malaysia. He is currently a Faculty Member at the Faculty of Science and Engineering, School of Mathematics and Computer Science, University of Wolverhampton, U.K. He is also an Adjunct Staff at Monash University and the Centre for Artificial Intelligence Research and Optimisation, Torrens University, Australia. He has published several scientific/research articles in well-known international journals and conferences. He was involved in conducting five research grants projects, whereby three of them are in the area of network and security and the others in analyzing and forecasting floods in Malaysia. He has supervised three Ph.D. students and three master's students as well as some other undergraduate final year projects. His current research interests include wireless communications, network security, and AI applications in networking. He received the Pro-Chancellor Academic Award as the best student in his batch for both master's and Ph.D. degrees. He also received the UTM International Doctoral Fellowship (IDF).

MUHAMMAD KHURRAM KHAN (Senior Member, IEEE) is currently a Professor of cybersecurity at the Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia. He is one of the founding members of CoEIA and has served as the Research and Development Manager, from 2009 to 2012. He, along with his team, developed and successfully managed Cybersecurity Research Program of CoEIA, which turned the center as one of the best centers of excellence in the region. He is the Founder and the CEO of the Global Foundation for Cyber Studies and Research, an independent, non-profit, and nonpartisan cybersecurity think-tank in Washington, DC, USA, which explores and addresses global cyberspace challenges from the intersecting dimensions of policy and technology. He has published more than 350 research articles in the journals and conferences of international repute. In addition, he is an inventor of ten U.S./PCT patents. He has edited seven books/proceedings published by Springer-Verlag and IEEE. He has secured several national and international competitive research grants in the domain of cybersecurity. He has played a leading role in developing the BS Cybersecurity Degree Program and Higher Diploma in Cybersecurity at King Saud University. His research interests include cybersecurity, digital authentication, the IoT security, cyber policy, and technological innovation management. He is a Fellow of the IET, U.K., BCS, U.K., FTRA, South Korea, a Senior Member of the IACSIT, Singapore, and a member of the IEEE Consumer Electronics Society, the IEEE Communications Society, the IEEE Technical Committee on Security & Privacy, the IEEE IoT Community, the IEEE Smart Cities Community, and the IEEE Cybersecurity Community. He was a recipient of the King Saud University Award for Scientific Excellence (Research Productivity), in May 2015. He was also a recipient of the King Saud University Award for Scientific Excellence (Inventions, Innovations, and Technology Licensing), in May 2016. He received the Outstanding Leadership Award at the IEEE International Conference on Networks and Systems Security 2009, Australia. Besides, he has received the certificate of appreciation for outstanding contributions in Biometrics and Information Security Research at the AIT International Conference, in June 2010, at Japan. He received the Gold Medal for the Best Invention & Innovation Award at the 10th Malaysian Technology Expo 2011, Malaysia. Moreover, in April 2013, his invention received the Bronze Medal at the 41st International Exhibition of Inventions at Geneva, Switzerland. In addition, he received the Best Paper Award from the *Journal of Network and Computer Applications* (Elsevier), in December 2015. He is also the Vice Chair of the IEEE Communications Society Saudi Chapter. Moreover, he is one of the organizing chairs of more than five dozen international conferences and a member of the technical committees of more than ten dozen international conferences. In addition, he is an active reviewer of many international journals as well as research foundations of Switzerland, Italy, Saudi Arabia, and Czech Republic. He is the Editor-in-Chief of a well-reputed international journal *Telecommunication Systems* published by Springer for over 26 years with its recent impact factor of 1.707 (JCR 2019). Furthermore, he is on the Editorial Board of several international journals, including, the IEEE COMMUNICATIONS SURVEYS & TUTORIALS, the *IEEE Communications Magazine*, the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, the *Journal of Network & Computer Applications* (Elsevier), IEEE ACCESS, the *IEEE Consumer Electronics Magazine*, *PLOS ONE*, *Electronic Commerce Research*, *IET Wireless Sensor Systems*, the *Journal of Information Hiding and Multimedia Signal Processing*, and the *International Journal of Biometrics*. He has also played the role of guest editor for several international journals of IEEE, Springer, Wiley, and Elsevier Science. He is a Distinguished Lecturer of the IEEE. His detailed profile can be visited at http://www.professorkhurram.com.