Survey of Cybercrime and its Detection Techniques

Navyashree. R[1]
III MTech, Dept of CSE
SSIT, Tumkur

Dr. Guruprakash.C.D[2]
Professor, Dept of CSE
SSIT, Tumkur

Dr. M.Siddappa[3]
Professor & Head Dept of CSE
SSIT, Tumkur

Abstract: Cybercrimes are examples for illicit violations and misdemeanours using machines or networking mechanisms as goals and commissioning devices. Prevalent cybercrime include child pornography, cyber stalking, identity stealing, cyber-laundering, cyber terrorism, drug sales, phishing, etc. Typically, these crimes result in privacy violations, security breaches, business losses, financial misconduct, or damage to public and government property. As a result, this report is intensively analyzing cybercrime monitoring and mitigation strategies. First it explores the various forms regarding cybercrimes as well as addresses the challenges regarding confidentiality along with protection through computer networks. It also outlines the methods which cyber criminals may use to commit these crimes against people, enterprises including communities. It also analyzes the current cyber crime monitoring and prevention strategies.

Keywords: Security, cybercrime detection techniques, neural network, fuzzy logic, machine learning, data mining.

I. Introduction

Cybercrime can be described as crime carried out to inflict fear and distress to persons or injure, harm, and damage property using computers or other communication tools. Cybercrimes can be classified as computer-assisted as well as computer-focused cybercrimes. Few examples for computer-assisted crimes include child pornography, theft, and money laundering besides cyber stalking. Hacking, phishing scams, and website defacement are forms of computer-focused cybercrimes. [1].

In the 1960s, the first cybercrime event took place, in which programming codes were replicated[2]. Many incidents of theft and forgery were reported after 1970, when over $1.5 million was embezzled from consumer accounts by a bank analyst at Union Dime Savings Bank in New York. Bob Thomas created a creeper virus which infected the Advanced Research Project Agency Network (ARPANET) networks in 1971, that became the earliest packet switching infrastructure network and TCP/IP protocol[2],[3]. A worker at Imperial Chemical Indus managed to rob large number of computers as well as copies from the company in early 1977 and demanded 275,000 sterling pounds as a payment [2]. The first electronic worm was created by Robert T. Morris at Massachusetts Institute of Technology in 1988[4]. In 1994, Russian hackers in Russia, Finland, Israel, Germany, United States, Netherlands, and Switzerland moved large amounts of currency to bank accounts from the city bank [2].

In 1995, the first phishing attempt was made[2]. Created in 1997, the Electronic Disruption Theater was in charge for designing electronic version for site-in tools that are utilized in demonstrations. A mechanism called FloodNet was used by demonstrators in 1998 to conduct a denial of service.

This paper includes a thorough analysis of cybercrime detection strategies, which are classified using various detection approaches. The first study presents the different kinds of cybercrime. The second is a overall study of known cybercrime detection techniques. Remainder of the article is structured as following. Section 2 describes as well as identifies several kinds of cybercrime. Section 3 addresses recent cybercrime detection research techniques. Section 4 lays out the conclusion.

II. Types Of Cybercrime

The following subdivision list and describe few of cybercrimes in brief.

A. *Cyber Warfare*

It is a form of war which doesn't use weapons, rather cyber attacks. This could be carried out without government permission by organizations or group of hackers, which can lead to political conflicts between nations.. For the past 20 years many warfares have taken place. For instance, Russia and Georgia were occupied with a cyber warfare during 2008.

B. *Cyber Terrorism*

It is an illegal act involving violence against individuals and assets. It often serves as a political, ethnic or ideological intent. This form of cybercrime can spread panic, paranoia, and aggression among people. Terrorists use the Internet to spread propaganda, exploit individuals, manipulate public sentiment, and shut down national Infrastructure. An instance of this is the December 2015 Ukrainian assault on a power grid, it began with a scam e-mail.

C. Child Pornography

It pertains to photographs, audio and videos recordings of minors wearing indecent clothing with little to no clothes, who might also be in indecent positions. Any creation, distribution or possession of any form of digital child pornography content is considered to be a criminal crime under the laws.

D. Cyber Espionage

It alludes to activities involving spies and stealing of valuable and confidential information for the convenience and benefits of opposing businesses or external overseas authorities. It utilizes computers to carry out operations. Around 300 English businesses distressed due to cyber espionage incidents by Chinese enterprises during December 2007. [35].

E. Cyber Bullying

Cyber bullying is the use of electronic media to bully a person usually by delivering messages of an aggressive or threatening nature. Bullying may cause physical and mental harm and it may affect the character of a person. Victims might receive malicious and rude texts, tweets, or posts implying violence, harassing victims, or threatening their lives.

F. Phishing

The attacker is trying to trick the consumer into delivering confidential details. Phishing comprises a mixture of social engineering and spoofing tactics. The user gets an email informing and asking them to provide sensitive information, alerting them about an intrusion, and trying to convince them to setup latest antivirus which might potentially could be a malware. Likewise phishing emails might also include links which might lead to malicious websites. Amongst the most successful defense policies is never to open a link in a dubious email. Visiting reputable internet sites which have 'https' with their URLs, and installing antivirus software, implementing firewalls as well as anti-phishing toolbars are just more ways to protect yourself.

G. SQL Injection

It is a method of attack where the attacker uses SQL queries to manipulate databases. Before altering or deleting the files, the intruder will examine at the database and obtain its contents. Setting a high benchmark level of credentials, via the use of user id and password, for all clients is one of the better precautionary plans for this kind of invasion.

H. Denial Of Service(DoS)

DoS attacks are a significant online risk that compromises resource accessibility. With a large amount of queries, like Internet Control Message Protocol (ICMP) and SYN floods, DoS crashes infected computers, forcing the devices to crash and cease the provision of specified service. A different form of DoS issue termed a Distributed Denial-of-Service (DDoS) attack, appears to cause the perpetrator to enter several network channels, and any recipient can become an agent to target another machine.

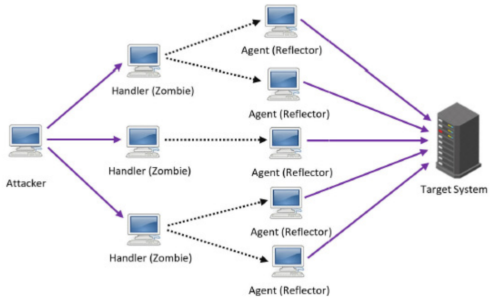

FIGURE 1. An example of a DDoS attack.

III. Technique To Detect Cybercrimes

A wide array of previous studies have been undertaken to establish techniques for identifying cyber crimes. The major categories of these approaches are seen in Figure 2 and defined in the subsequent sections

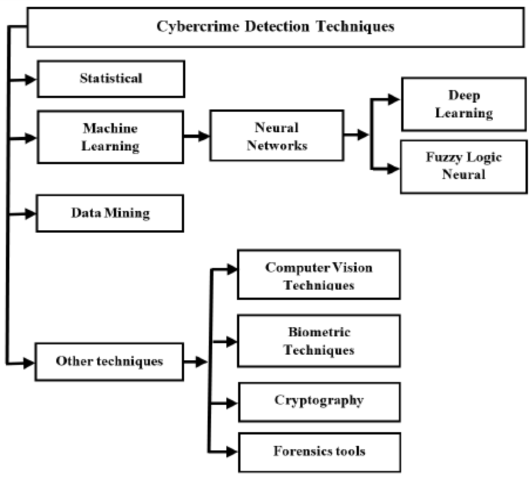

FIGURE 2. Categorization of cybercrime detection techniques.

.

A. Detection Of Cybercrime With Statistical Methods

One of the best identification models for cyber attacks is the Hidden Markov Model. It is indeed a time-consuming process, nevertheless. By reducing the required time needed for data training to identify cyber attacks by using N-gram extraction algorithm, Sultana et al.[6] enhanced hidden Markov Model. Instead of complete trace cases, the proposed model uses repeated recurring patterns in trace files. The N-gram extraction algorithm is being utilized to retrieve typical patterns during data mining.

Liang *et al*. [7] suggested a filter which will be used in an intrusion detection system (IDS) such that it can identify attacks on vehicular ad-hoc network(VANET).Here Hidden Markov Model is used in order to implement the filter.

A methodology proposed for a IDS which is centered upon cosine similarity was developed by Rasmi and Jantan[8] for anticipating intended attacks. This latest algorithm, called the Attack Intent Similarity algorithm. For each attack intension, a similarity matrix of prior and current attack intentions is created which is used to determine the probability ratio.

Harrou et al. [9] developed an anomaly detector method which is based on 1999 DAPRA dataset and it is used to identify TCP SYN flood attacks. In both DoS and as well as DDoS attacks, TCP SYN floods are used. In order to detect the strongest anomaly detection system, they combined CRPA metric Shewhart and Exponentially Weighted Moving Average (EWMA) which are the statistical methods The experiment revealed that superior outcomes were obtained by combining the CPRA along with the Shewhart and EWMA.

A system for identifying network cybercrimes was developed by Abouzakhar et al.[10] .This system uses Bayesian learning network concept. This method is not as viable in practice as deterministic correlation approachs.

A latest form of DDoS attack, named as link-flooding attack (LFA), was detected and resolved by Wang et al[11] .In very critical parts of a network, LFA attacks will break off service through flooding them with legit low-speed flows. The researchers suggested a new protection mechanism called LFADefender. LFADefender is versatile and can adjust its role in real time in the network, whereas a regular IDS is positioned in a fixed network area. Here the network identifies high-flow-density connections and rerouting is initiated in such a manner that the congested links are avoided and the attack is overcome.

Birkinshaw[12] used software-defined networking(SDN) to propose an IDS .Two types of attacks have been targeted by the authors: port scanning and DoS, for which Rate Limiting(RL) and Credit-Based Threshold Random Walk (CBTRW) have been implemented. On a host, worm infection is detected by a CB-TRW algorithm, while to stop DoS attacks an RL algorithm is utilized.

B. Detection Of Cybercrime With Machine Learning

Machine learning is the science of predicting outcomes based on input data, also named training data. This learning mechanism may be supervised or unsupervised. Outputs are not labeled in unsupervised learning approaches whereas in supervised it will be labeled.

In order to classify cybercrimes, researchers have used various algorithms from the supervised learning algorithm classification, such as naive Bayes as well as K-nearest neighbour (KNN) and the unsupervised learning algorithm classification, such as K-means.

To better classify crime patterns, Nath[13] used clustering algorithm along with K-means clustering for data mining. K-means methods can merge the different data easily, but could not ensure that correct solution might be reached when the data converges. In addition, K-means is belongs to one of the unsupervised learning algorithm, and thus right answers are not established.

A cyber bullying identification method using the the naïve Bayes classifier and the Levenshtein algorithm was introduced by Nandhini and Sheeba[14].

In order to detect cyber terrorism, Uzel et al.[15] used text classification. Here the researchers added numerical weights to words. Then they converted the file to a vector. The researchers used the naive Bayes multinomial and SVM as classifiers for identification.

Ofoghi et al.[16] proposed a hybrid feature method that by collecting feature vectors, detects phishing emails.

Since most of the IDSs predict known attacks a new paradigm system was proposed by Ahn *et al.* [36] to predict unknown attacks. It included classification using logistic regression analysis or SVM, prediction using regression analysis.

Darus *et al.* [17] proposed technique to detect malware in android platform.Three types of algorithms for classification were used, such as random forest (RF) algorithms, decision tree, and KNN. The authors observed that RF had greater precision than approaches to decision tree and KNN.

Vuong et al.[18] proposed a system for identifying cyber threats on mobility systems, such as robots. There are four kinds of attacks in the presented system for mobile robotic vehicles: two kinds of malware, DoS and SQL injection.

Al-diabat[19] researched on different types of phishing methods and attacks and threats henceforth to mitigate this he attempted to identify fraudulent sites by evaluating the characteristics that differentiate among legitimate and illegal sites. They made use of the C4.5 algorithm.

C. Detection Of Cybercrime With Neural Network

The neural network is a simulation of how the human brain operates. Neural networks also have significant degree of noise input to data fault tolerance, which is observed to be advantageous relative to machine learning algorithms where it won’t be taken into consideration.

Raiyn [20] discussed the identification of cybercrimes in the cloud and proposed the idea of using IP addresses to assess the geographical location of users.

In order to detect threats from phishing, Zhang and Yuan[21] used neural network. For the detection of phishing threats, they used a multilayer feedforward neural network to achieve 95 percent precision.

The IDS using a feedforward neural network model was suggested by Manzoor and Kumar[22]. For the detection of DoS attacks, 99.93 per cent accuracy was achieved and 96.51 per cent accuracy for the detection of root user (U2R) attacks was achieved. When a regular user has admittance to a privileged super (root) user, U2R attacks occur.

D. Detection Of Cybercrime With Deep Learning

Dadvar and Eckert[23] have tracked cyberbullying on various social media sites. They have used 4 deep neural network based models: bidirectional LSTM (BLSTM), long short-term memory (LSTM), BLSTM with attention and the convolutional neural network (CNN). For text as well as image classification, CNN is helpful, while for text classification, the LSTM neural network is appropriate. BLSTM encodes data in two ways: backwards as well as forwards.CNN model has been shown to perform better than machine-learning methods for cyber bullying determination.

Almiani *et al.* [24] proposed IDS for FOG security and Internet of Things (IoT). On the NSL-KDD data collection, they used a deep recurrent neural network; they calculated the performance of the new method using two matrices: Matthews correlation coefficient as well as Cohen's kappa coefficient.

For a wireless network, Kasongo and Sun[36] suggested an IDS utilizing deep long short-term memory as a classifier. Using NSL-KDD data collection, the proposed IDS was tested and it attained 86.99 percent precision on the tested data sample.

To assess the hidden relationship between criminals in the criminal network Lim et al.[25] used deep reinforcement learning (DRL) techniques. Since only limited criminal histories are usable, standard ML algorithms are not sufficient therefore the performance of DRL algoritms is much better in such cases

E. Detection Of Cybercrime With Fuzzy Logic

Fuzzy logic is nothing but a blend of both fuzzy sets and classic sets. It measures the degree of validity, or the degree to which an entity is part of the set, we may assert. This does not classify objects into 1 and 0, where 0 means that a set does not belong, and 1 indicates that it belongs to a set. Rather, 0 and 1 are severe cases of truth [28], which is fuzzy logic. Due to the ambiguity and concerns regarding the gathering of evidence, this reasoning is needed for the identification of cybercrimes.

Fatima et al.[26] described a soft computer application methodology. This can be utilized, wherever a final solution could not be determined because of insufficient supporting and comprehensive knowledge. The researchers concentrated on following applications supporting soft computing: ANN and neuro-fuzzy logic. They interpreted both applications. The findings revealed that neuro-fuzzy logic is better at identifying cyber crimes.

Ahmed and Mohammed[27] used a fuzzy minmax strategy to determine the intentions of the attackers in live time. Two phases were involved in the process. The pattern of the attack is decided in the first stage. While the purpose of the threat is calculated in the second stage by examining correlations between the features of the pattern and the information obtained from the attack using fuzzy minmax neural network.

Using five different tables in which 288 attributes were held with twofold cross validation, Barraclough et al. [28] used fuzzy logic to locate phishing attacks. They also attained elevated precision.

F. Detection Of Cybercrime With Data Mining

Sindhu and Meshram[29] have suggested a cybercrime detection method that uses the algorithm a priori.

A modern framework named visual threat detector, it incorporates data mining along with visualisation in order to identify behavior of botnet in the network, was introduced by Shahresani et al.[30]. The authors used many visualisation tools to aid network administrator quickly identify botnets, such as scatter plots, histograms, matrix visualisations.

Random Forest (RF) algorithm was used by Smadi et al. [31] to identify phishing mails. Using 32 attributes, the researchers extracted the function metric from the email contents during preprocessing stage. 98.87% accuracy was achieved.

G. Detection Of Cybercrime With Other Techniques

Following section includes additional methods that have been implemented to identify cybercrimes centered on detection methods like biometrics, cryptography, and forensic tools. Some of the techniques rely on the study and interpretation of imagery. Computer vision techniques are often made use to detect cybercrimes, in particular phishing, through examining website URLs so that we can assess what is identified.

Rao and Ali [32] mentioned a method for identifying websites used for phishing by incorporating visual resemblance techniques and whitelist. The researchers used the Accelerated Stable Functionality (SURF) identification technique to strip characters from bogus and illegal websites. White list includes all valid URLs that have been used to search URLs.

Derhab et al. [33] approached the topic of spam botnet detection by proposing a security mechanism called the Spam Trapping Scheme (STS).It is accountable for offering a third line of detection as well as prevention of spam botnet distribution. The Spam Trapping Method uses encrypted email to differentiate among genuine and spam emails. It uses a cryptographic key in valid mail. Users, the e-mail programme, and the STS system are familiar with the cryptographic key. We can differentiate since spam mails does not have encrypted key.

IV. CONCLUSION

The review of this paper addressed a variety of forms of cybercrime and also reviewed a number of studies on their detection techniques available. While technology advances and internet-enabled gadgets become more popular, new possibilities emerge for this technology to be targeted by criminals. Cybercrimes are difficult to detect since appropriate data sets are not available as benchmarks. There are many types of cyber crime and they take place in different platforms and hence involving a different type of datasets. Since it is a very sensitive issue it is best that both the law enforcers and researchers work together to take appropriate measures.

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/de_nition/ARPANET

[4] (2018). *The Morris Worm*. Accessed: Jan. 28, 2020

[5] V. Beal. (Apr. 27, 2020). *SCADA_Supervisory Control and Data Acquisition*.

[6] 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

[7] 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.

[8] M. Rasmi and A. Jantan, ``A new algorithm to estimate the similarity between the intentions of the cyber crimes for network forensics," *Pro- cedia Technol.*, vol. 11, pp. 540_547, Jan. 2013.

[9] 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.

[10] 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.

[11] J. Wang, R. Wen, J. Li, F. Yan, B. Zhao, and F. Yu, ``Detecting and mitigating target link-_ooding attacks using SDN," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 6, pp. 944_956, Nov./Dec. 2019.

[12] 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.

[13] 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.

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

[15] *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.

[16] 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.

[17] F. M. Darus, N. A. A. Salleh, and A. F. M. Arif_n, ``Android malware detection using machine learning on image patterns," in Proc. Cyber Resilience Conf. (CRC), Nov. 2018, pp. 1_2.

[18] T. P. Vuong, G. Loukas, and D. Gan, ``Performance evaluation of cyberphysical 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.

[19] M. Al-diabat, ``Detection and prediction of phishing websites using classi_cation mining techniques," Int. J. Comput. Appl., vol. 147, no. 5, pp. 5_11, Aug. 2016.

[20] J. Raiyn, ``A survey of cyber attack detection strategies," Int. J. Secur. Appl., vol. 8, no. 1, pp. 247_256, Jan. 2014.

[21] 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.

[22] Akashdeep, I. Manzoor, and N. Kumar, ``A feature reduced intrusion detection system using ANN classi_er,'' Expert Syst. Appl., vol. 88, pp. 249_257, Dec. 2017.

[23] M. Dadvar and K. Eckert, ``Cyberbullying detection in social networks using deep learning based models; A reproducibility study,'' 2018, arXiv:1812.08046.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] A. Shahrestani, M. Feily, R. Ahmad, and S. Ramadass, ``Architecture for applying data mining and visualization on network _ow for botnet traffic detection,'' in *Proc. Int. Conf. Comput. Technol. Develop.*, Nov. 2009, pp.33_3.

[31] 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.

[32] 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.

[33] 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.

[35] 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.

[36] 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

[37] 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.