Journal of Theoretical and Applied Information Technology
31st August 2023. Vol.101. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DEEP NEURAL SYSTEM FOR IDENTIFYING CYBERCRIME ACTIVITIES IN NETWORKS

[1]YERININTI VENKATA NARAYANA, [2]Dr. MOORAMREDDY SREEDEVI

[1]Research Scholar, Department of Computer Science, Sri Venkateswara University, Tirupati, Andhra Pradesh,
[2] Associate Professor, Department of Computer Science, Sri Venkateswara University, Andhra Pradesh,
Email: naarayanaa808@gmail.com,, msreedevi_svu2007@yahoo.com

ABSTRACT

Nowadays, the increase in communication networks increases the risk of cybercrime. These crimes affect all individuals, from children to adults. Cybercrime causes serious impacts that many nations were researching various detection frameworks and safeguard approaches such as regulation of internet usage, establishing an organization to deal with cybercrime issues and adaptive forensic techniques. The various limitations regarding the cybercrime detection framework must be eliminated. Hence this current article reviewed different cybercrime detection frameworks based on deep neural models. Here several literature works were discussed with their advantages and their limitations. Furthermore, in the performance analysis section, the results of the few works were compared. Subsequently, common defeats and their reason were explained in the discussion part. Finally, future works have directed the following studies to improve the efficiency of the detection frameworks.

Keywords: *Cybercrime, Intelligence Frameworks, Classification, Features*.

1. INTRODUCTION

Any crimes achieved through the system or other communication tools by creating a bad impact or damage to the people and breaking the properties or system are termed cybercrime [1]. Cybercrimes are classified into two classes, namely, computer-focused and computer-assisted cybercrimes [2]. The crimes like stalking, fake laundering of money etc., have come under computer-assisted crimes, and the assaults like phishing, hacking and spoiling of online sites come under the computer-focused activities of crimes [3]. In 2003, a huge financial loss of about 100 billion USD arose due to the effect of cybercrime. Also, in 2007, there was a rush of about 100 billion USD in cybercrime, and the actionable trades exceeded 21numbers [4]. Every day the storing and processing of data on the computing system are gradually rising with the data of people communicating, sharing, and working using the internet and computers [5]. It erased the language and the country barrier. However, these properties make the system more difficult to detect and monitor cyber problems [6]. Whenever dealing with people on the internet, the concept of cyber-crimes appears. Therefore, cyberspace is not preserved from either cybercrimes or intruders [7]. Gathering accurate information about cybercrimes is quite difficult. Also, the severities of the cyber problems remain unnoticed due to the lack of knowledge about cybercrimes [8]. Law enforcement plays a crucial role in controlling the severity of the reported crimes [48]. The main three research tracks in cybercrime intelligence are given in fig.1.

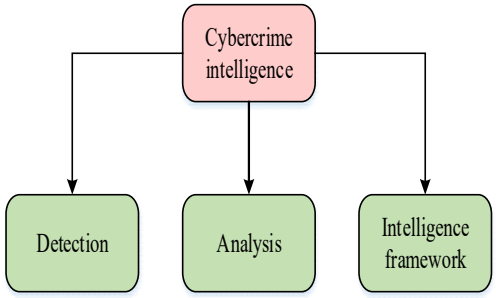

Fig.1. Cybercrime Research Tracks

Nowadays, intruders take numerous ways to accomplish cybercrimes [9]. The distributed and internet computing environment extension makes the system more vulnerable to intrusions and attacks [10]. Furthermore, with the growing network rate, cybercrimes are globally enhanced, becoming a threat to any computing or communication system [46]. It also makes it hard to manage new crimes or threats [11]. A conventional working algorithm prevents combating virtually progressing cyber-attacks [12]. This is an important

reason to develop the most innovative intelligence technology to fight against cybercrimes. Some hardware, like detectors and sensors, is insufficient for cybercrime analysis and monitoring [13]. These are hardware areas not capable of recognizing the behaviours of normal and criminal activities. They must be adaptable, strong, and able to detect wide cyber threats [14]. To increase their capacity, more intelligence technology was adapted to categorize the normal and the abnormal situations and make it reliable for real-time detections [15]. Artificial intelligence offers major ways to detect cybercrimes [16].

The technologies such as neural networks, fuzzy logic, ML, pattern recognition, data mining etc. [17] have played the most crucial character in cybercrime detection and protection [47]. According to various studies, artificial intelligence like DL or ML is mostly used for cybercrime detection [18, 19]. Also, it offers self-management, self-security and tuning [20]. However, some traditional AI approaches focus only on the person's behaviours, knowledge representations and interference methods. So, few kinds of literature are reviewed with their advantages and limitations, and their future scope is discussed.

2. DEEP NEURAL SYSTEM FOR CYBERCRIME DETECTION

The network's crime rate has increased as neither of the conventional frameworks executed by forensic experts has prevented or minimized the cybercrimes [45,49]. This is due to the fact that the targets or victims of cybercrimes vary according to the reason for the crime, and cybercriminals always develop their techniques and make use of new approaches to accomplish crimes and accomplish their objectives. Many studies have been done in the past to provide techniques for identifying cybercrimes. Here is an overview of the many deep neural-based crime detection algorithms.

2.1. Multi-classification-based cybercrime detection

Manyumwa et al. [32] suggested the multiclass classification approach using ensemble boosting algorithms to detect the malicious URL attack in cyberspace. This model aimed at three main attacks: phishing, malware and spam. The CatBoost, AdaBoost, XGBoost and LightGBM are used to design the multiclass classification approach. Here the XGBoost shows increased performance. The network creates a large attack surface for cybercriminals, which produces harmful effects for individuals. So, to detect these attacks, Ullah et al. [38] introduced the CNN framework in 1D, 2D and 3D. Here it validates the 4 available datasets. Additionally, transfer learning is utilized to perform the multiclass and binary classification using CNN. These classifications achieved a higher performance result. The comparisons are given in table.1.

Table.1. Comparison Of Multi-Classification-Based Cybercrime Detection

Author	Method	Advantages	Disadvantages
Manyumwa et al. [32]	CatBoost, AdaBoost, XGBoost and the LightGBM	Better performance	XGBoost outperforms the others
Ullah et al. [38]	CNN	Less time to train and validation	The FNR rate is very high.

2.2. Hybrid architecture for cybercrime detection

Cybercriminals utilize malicious URLs to commit numerous crimes in the network. Therefore Srinivasan et al. [27] designed a DeepURLDetect (DURLD) to detect the malicious website using a hybrid of CNN and LSTM. It gives a better detection rate. However, it can be designed as more robust by incorporating the extra auxiliary modules. Cybercrime analysis-based ML algorithms are time-consuming. So Vinayakumar et al. [28] proposed a novel ScaleMalNet by a hybrid of 3 DL structures such as DNN, CNN and RNN. Here the feature analysis is carried out based on static and dynamic analysis and additional image processing techniques. It can detect a wide range of malware in real-time data. Robertas et al. [41] presented an ensemble that relied upon a classification approach for cybercrime detection. Here the classification is executed by the stacked ensemble network and CNN for improving the recognition of windows PE malware. The performance of the proposed framework exceeds the other ML approaches. In future, this framework will be extended for large dataset processing.

Table.2. Comparison Of Hybrid Architecture For Cybercrime Detection

Author	Method	Advantages	Disadvantages
Srinivasan et al. [27]	DURLD	better detection rate	it can be designed as more robust by incorporating the extra auxiliary modules
Vinayakumar et al. [28]	ScaleMalNet	Detect wide range of real time malwares	The hyper tuning method has not been adopted.
Robertas et al. [41]	stacked ensemble network and CNN	Better than ML techniques	Not suitable for large set of data
Srinivasan et al. [26]	deep spam net	No need of feature engineering phase	Not suitable for real time dataset

The past work on ML-based cybercrime detection relied on the feature engineering phase. It is difficult for the adversarial network. So Srinivasan et al. [26] designed a DL architecture named deep spam net which uses CNN and LSTM and relies on natural language processing to detect the spam in the email. This network leverages the text and directly maps into the email's spam. This model focuses on real-time data for further extension. Omrani et al. [22] investigated the binary classification using ANN and SVM by analyzing the TCP connection traffic as a benign or suspicious for the detection of cybercrimes in the network application and electronic devices' increasing environment. The comparisons of these approaches are given in table.2.

2.3. ML based cybercrime detection

Some of the existing approaches suffer from the inadequate presence of computation methods, and the predictions are failed, especially on the unstructured data. To overcome these problems, Ruba et al. [23] presented a flexible computation tool employing the ML technique to analyze cybercrimes. However, to extend the preventive measures and actions, the extension of features is required. Also, crime detection features can be enhanced by deep learning. Islam et al. [34] introduced an effective online bullying and abusive message through the combination of NLP and ML algorithms. It detects the crime messages based on two unique features Term Frequency-inverse text frequency (TF-ITF) and Bag of Words (BoW). The various ML model involved in this detection process is support vector machine (SVM), Decision Tree (DT), Naïve Bayes (NB) and Random Forest (RF). Here the SVM outperforms the other three algorithms, and the TF-IDF gives better accuracy.

Nowadays, cyber criminals achieve greater benefits from attacking the crypto-currency mining pools. So to detect this abusive crypto-mining activity Pastor et al. [37] introduced network flow features based on ML and deep learning (DL) models. The fully connected neural network (FCNN) is utilized, for the model training and classification is tested with RF, Logistic regression (LR) and Regression Tree (RT) models. However, the FCNN produced the worst result using the network flow features.

The increased popularity of social media platforms has given rise to cyberbullying in online communication and social media. Therefore Garadi et al. [29] derived the special features of Twitter and tested them in the ML techniques. The proposed features result from the feasible detection of cybercrime in the Twitter network. Here the selected features increased the performance results and the discriminative power.

Table.3. Comparison Of ML Techniques

Author	Method	Advantages	Disadvantages
Ruba et al. [23]	NB, k- means clustering.	Increased performance	The extension of features is required
Islam et al. [34]	SVM, DT, NB and RF	Better accuracy	Only SVM outperforms others
Pastor et al. [37]	FCNN, RF, LR and RT	Less time	FCNN produced the worst result using the network

			flow features.
Garadi et al. [29]	NB,SVM,KNN,RF	Selected features increased the performance results	Change in crime behaviour affects the accuracy
Boussi et al. [24]	ML algorithm	It detects crimes regardless of the places	Detect only higher-priority malware
Alam et al. [43]	RF and DT	RF produced high accuracy	The attack is not predicted for logged dataset

To ensure better security in cyberspace, Boussi et al. [24] introduced a new framework that performs the ML classification function. This framework employed the basic process, such as data training on the chip and activation of the classification algorithm. This chip is incorporated into electronic devices. It detects crimes regardless of the place. In future, it will be implemented to show its efficiency. To detect the phishing attack in the system, Alam et al. [43] explained the ML methods such as RF and DT. Additionally, for the feature selection, the model used the feature selection algorithm such as IG, GR, relief-F and REF and also, to classify the parameters in the dataset, PCA is applied to the designed framework. The advantages and disadvantages of the reviewed ML techniques are listed in table.3.

2.4. Optimized network for cybercrime detection

To create a robust cybercrime detection framework, Singh et al. [31] used the cuckoo search (CS) meta-heuristic approach for the learning of preprocessing, feature analysis and classification methodologies. Content-based detection is improved by this introduced technique. Here the SVM and NB are used as the classification methodologies. Here, the cuckoo search is utilized to select a better model and optimize the classification parameters. The suggested approach is tested on the Twitter dataset. Singh et al. [33] introduced a cuckoo-inspired ensemble network for the detection of content-based crimes. This model is tested on four datasets. The proposed framework has attained better detection performance for all four datasets. The comparison is given in the table.4.

Table.4. Comparison Of Optimized Network For Cybercrime Detection

Author	Method	Advantages	Disadvantages
Singh et al. [31]	SVM and NB	Better model selection	Computation time is large
Singh et al. [33]	cuckoo inspired ensemble network	better detection performance	Optimizing is not strong.

2.5. Deep learning frameworks

Advanced Persistent Threat (APT) is the main attack among the exchanging medium such as a smartphone. This attack includes both malware and social engineering. Zulkefli et al. [36] presented a new approach to prevent this attack. Initially, the strategy of the criminal to launch the social engineering attack was learnt, and the attack is categorized as phish or not using the decision tree. The proposed model can make able to hostile the APT through spear phishing in the smartphone. However, the false negative errors are quite maximized. Sometimes the user's trust in well-known websites is destroyed by the phishers. Phishing leverages both web content and a universal resource locator. So, to prevent this, Adebowale et al. [42] described a hybrid classification architecture combining CNN and LSTM for the detection of phishing. Here both network layers are used for the extraction of features. However, the LSTM needs effective knowledge for the formation of features. In recent times, cyber bullying has become a serious issue in computing and communication networks. Therefore Nikhila et al. [21] presented a CNN for the classification of cybercrime in the cross-platform. Here the imbalanced textual dataset was taken for testing. So, to hold the balance of the dataset the generative adversarial network is utilized.

Nowadays, most cybercrimes are committed on social media. Therefore, to check the integrity of twitter, Ullah et al. [25] introduced the deep, dense pyramidal neural network in the tweet's classification. It classifies the tweets by analyzing the linguistic features of crime or breaches in data, and the network is trained to identify the indicators. Here the performance may be degraded due to the imbalanced data. The main indication of cybercrime is network data traffic. To analyze DNS traffic, Berger et al. [30] introduced the system

named DNSMap. It incorporated the graph analysis process, which has the ability to recognize the transition in the network and the malicious nodes. The one disadvantage is that if one node is found to be malicious in the graph component, then all the other nodes are decided as malicious.

Many cybercrime detection frameworks have been introduced in the past few years. However, there are still some drawbacks are existed in all approaches. So Nouh et al. [35] studied most of the state-of-the-art procedures and introduced a novel intelligence framework for cybercrime to fill the gaps identified in the existing approaches. This intelligence framework is designed to sight the crimes in large datasets. Raza et al. [39] introduced 10 layered deep Variational encoder (VAE) networks for cybercrime detection. In this model, the features are analyzed by the hidden layers of the encoder and decoder block of the presented network and reconstruct the data for enhancing the detection performance. Here the credit card transaction details are utilized for the intrusion identification, and the results are related to the few ML classifiers. The comparison is given in the table.5.

Table.5. Comparison Of Deep Learning Frameworks

Author	Method	Advantages	Disadvantages
Zulkefli et al. [36]	decision tree classifier	hostile the APT through spear phishing in smartphone	false negative errors are quite maximized
Adebowale et al. [42]	CNN and LSTM	Highly effective in fake website identification	the LSTM needs effective knowledge for the formation of features
Nikhila et al. [21]	CNN	Overcome imbalance problems	The model can be improved by tuning
Ullah et al. [25]	deep, dense pyramidal neural network	It classifies the tweets by analyzing the linguistics	performance may be degraded due to the imbalanced data
Berger et al. [30]	DNSMap	recognize the transition in the network	In the graph component, if one node is found to be malicious, then all the other nodes are decided as malicious
Raza et al. [39]	VAE	Enhanced detection performance	Due to high false positives have shown lower precision and f1 score
Karie et al. [40]	DLCF	help in forensic investigations	The DL algorithm utilized in this framework should not be changed or alter the PDE.
Bendiab et al. [44]	ResNet 50	effective classification	Need an extension for a larger dataset

In cyber forensics, the presence of big data makes the process more complex, difficult and time-consuming. Big data contains data from multiple sources in a distinct format. Therefore, to help in the execution of cyber forensics for big data, Karie et al. [40] introduced a deep learning framework for cyber forensics named DLCF.

Cybercriminals easily abuse sensitive information and data in networks. To address this challenge, Bendiab et al. [44] designed a unique traffic analysis framework to recognize malware quickly in networks. For traffic analysis, the framework comprises the residual network (ResNet50) for precisely detecting malware and benign traffic. This network proved the effective classification. Cybercriminals utilize domain generation algorithms to safeguard their system from being shut down or blacklisted. Therefore, to detect these generated domain names, Ravi et al. [50] created a deep-learning architecture using CNN and RNN.

3. PERFORMANCE ANALYSIS

In the cybercrime detection framework, the features are the key parameter for efficient detection. Based on the selected features, the value of classification is recorded. Also, the size and the structure of the data must be a concern. The overall performance results of the reviewed work are described in the table. 6.

Table.6. Comparison Of State-Of-The-Art Approaches

Author	Method	Dataset	Results
Ruba et al. [23]	Naïve Bayes, k means clustering	Cybercrime dataset from Kaggle and CERT-In	Recall-99% Accuracy-99% f-score-99% Precision-99%
Islam et al. [34]	SVM, DT, NB and RF	Facebook and Twitter comment dataset	Accuracy-97.8% Recall-97.2% f-measure-97.9% precision-98.8%
Pastor et al. [37]	FCNN, RF, LR and RT	Tsat dataset	Accuracy-100% Recall-100% f-score-100% Precision-100%
Garadi et al. [29]	NB,SVM,KNN,RF	Twitter dataset	Accuracy-95% Precision-94% Recall-93.9% f-score-93.6% Area under curve (AUC) -94.3
Alam et al. [43]	RF and DT	Phishing dataset from Kaggle	Accuracy-91.9% Precision-93.84% Recall-88% f-score-90.84%
Srinivasan et al. [27]	DURLD	Dataset Alexa.com, DMOZ directory, MalwareDomainlist.com and MalwareDomains.com	Accuracy-95.4% Precision-96.8% Recall-93% f-score-94.9% TPR-87.9% FPR-0.121% AUC-99.09%
Vinayakumar et al. [28]	ScaleMalNet	Ember	Accuracy-96.3% Recall-96.2% f-score-96.2% Precision-96.3%
Robertas et al. [41]	stacked ensemble network and CNN	ClaMP dataset	Accuracy-99.9% Recall-99.8% Precision-99.9% TPR-100% FPR-0
Srinivasan et al. [26]	deep spam net	Lingspam, Enron , PU, and Spam Assassin	Accuracy-95.9% Precision-93.6% Recall-100% f-score-96.7%
Manyumwa et al. [32]	CatBoost, AdaBoost, XGBoost and the LightGBM	DMOZ, PhishTank, URLhaus, WEBSPAM	Accuracy-95%
Ullah et al. [38]	CNN	BoT-IoT, , MQTT-IoT-IDS2020,IoT Network Intrusion and IoT-23	Recall-99.95% Precision-99.95% Accuracy-99.97% f-score-99.95%

Singh et al. [31]	SVM and NB	Twitter, ASKfm, Formspring	Precision-89.7% Recall-97% f-score-93.24% accuracy-98.7%-
Singh et al. [33]	cuckoo inspired ensemble network (CEN)	Formspring, ASKfm, and Twitter	Precision-94.2% Recall-97.24% f-score-96% Accuracy-99%
Zulkefli et al. [36]	decision tree classifier	URL dataset	Accuracy-90%
Adebowale et al. [42]	CNN and LSTM	Legitimate and phishing URLs	Accuracy-93.28% f-score-93.29% Recall-93.30% Precision-93.27%
Nikhila et al. [21]	CNN	Imbalanced textual dataset	Precision-89% Recall-85% f-score-81%
Ullah et al. [25]	deep, dense pyramidal neural network	Cybercrime datasetsfrom e Irish and New York regions from financial organization	Accuracy-65.75% Precision-48.25 Recall-83.24%
Berger et al. [30]	DNSMap	ISP dataset	Accuracy 99% Recall-98% Precision-99% f-score 98%
Raza et al. [39]	VAE	Credit Card Fraud Detection"	Accuracy-96% Precision-81.5% Recall-74.2% f-score-77.6%
Bendib et al.[44]	Resnet50	Created dataset	Accuracy-94.50% Precision-95.78% Recall-94.02% f-score-94.90%

Many prior studies have been conducted for cybercrime identification. Most studies have adopted the content, and textual-based view and hybrid structure were utilized for handling the imbalanced data structure and for further crime identification.

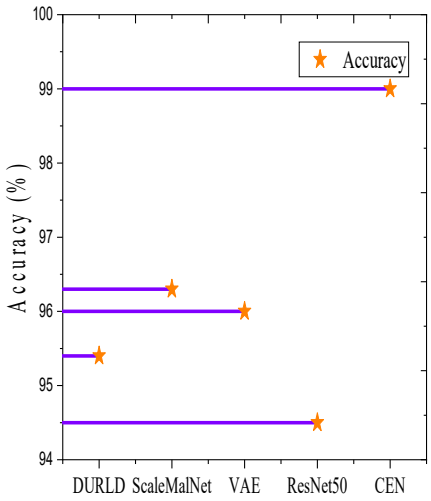

Fig.2. Comparison Of Accuracy

In crime detection, the working efficiency of the detecting framework is computed by the

value of accuracy. The comparison of the existing detection techniques is described in fig.2. Here, the optimized ensemble network (CEN) gains better accuracy when compared to the other models, such as DURLD, ScaleMalNet, VAE and ResNet50.

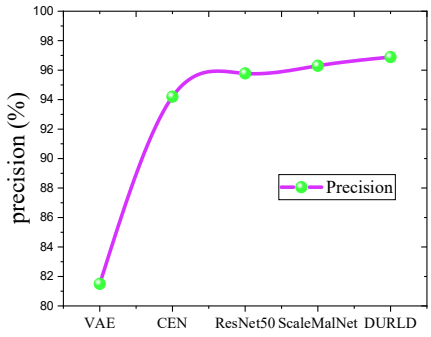

Fig.3. Comparison Of Precision Rate

The comparison for the precision rate is described in fig.3. Here, the model DURLD attained the finest precision rate compared to the other models.

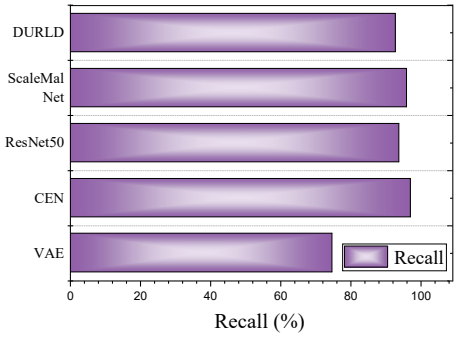

Fig.5. Comparison Of Recall

The comparison of the recall rate is explained in fig.5. Here the CEN has attained the good recall rate comparing to the other models.

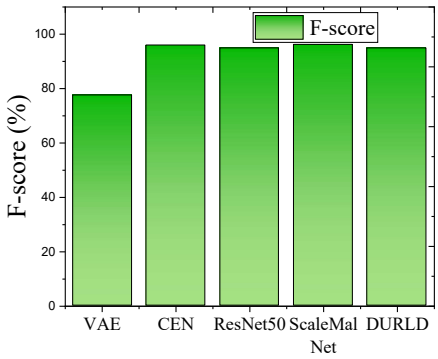

Fig.6. Comparison Of F-Score

The comparison of F-score for a few detection frameworks is described in fig.6. Here also, and the optimized ensemble network gained the highest rate of F-score when compared to the other models.

3. DISCUSSION

The life of individuals, national security and business organization were greatly affected by cybercrime and criminals. In the 21st century, it is the major increasing type of crime. Several frameworks and processes are derived for cybercrime detection. Also, some of the frameworks were processed with a large dataset. However, it takes a large computation time, and accuracy gets reduced. Another reason for these disadvantages is the processing of imbalanced data. Also, some of the advantages are carried by the intelligence frameworks. However, selecting feature engineering phases may degrade the framework's performance.

4. CONCLUSION

In today's rapid increase in information technology, the network environment brought advanced and convenient features to human life. However, it provided a way for emerging cybercrime which is difficult to control, manage and avoid. During the implementation of the detection framework, some problems may arise due to unstructured data and insufficient features. Designing the optimization approach in the detection framework will help to enhance the detection and accuracy rate. Also, before designing the framework, the need of the application should be identified to find a suitable network. Available kinds of literature described that identification frameworks already have various applications to take action against cybercrimes. Hence, to schedule the application requirements, one of the neural frameworks will be structured.

5. FUTURE WORK

In the future, the optimized neural network can afford the finest results compared to the present techniques with the following objectives: detection of attack patterns to prevent the cyber-crime activities based on the temporal features and detection of unknown cyber-attacks.

REFERENCES

[1]. Al-Khater WA, Al-Maadeed S, Ahmed AA, Sadiq AS, Khan MK. Comprehensive review of cybercrime detection techniques. IEEE Access. 2020 Jul 22;8:137293-311.

[2]. Dilek S, Çakır H, Aydın M. Applications of artificial intelligence techniques to combating cyber crimes: A review. arXiv preprint arXiv:1502.03552. 2015 Feb 12.

[3]. Veena K, Meena K, Teekaraman Y, Kuppusamy R, Radhakrishnan A. C SVM classification and KNN techniques for cyber crime detection. Wireless Communications and Mobile Computing. 2022 Jan 17;2022:1-9.

[4]. Koto, Ismail. "Cyber Crime According to the ITE Law." *International Journal Reglement& Society (IJRS)* 2.2 (2021): 103-110.

[5]. Ngafeeson M. Cybercrime classification: a motivational model. College of Business Administration, The University of Texas-Pan American. 2010 Mar 3;1201.

[6]. Devi A. Cyber Crime and Cyber Security: A Quick Glance. InDetecting and Mitigating Robotic Cyber Security Risks 2017 (pp. 160-171). IGI Global.

[7]. Jyothi KK, Kalyani G, Rao TV. Approaches and Scenarios to Combat Cyber Crime. International Journal of Science, Engineering and Computer Technology. 2014 Dec 1;4(12):376.

[8]. AKPAN EE. A Strategic Assessment of Cyber Security Strategies and Mitigation of Cybercrime in Nigeria.

[9]. Lee EA. Cyber physical systems: Design challenges. In2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC) 2008 May 5 (pp. 363-369). IEEE.

[10]. Lee EA. Cyber-physical systems-are computing foundations adequate. InPosition paper for NSF workshop on cyber-physical systems: research motivation, techniques and roadmap 2006 Oct 16 (Vol. 2, pp. 1-9).

[11]. Bass T. Intrusion detection systems and multisensor data fusion. Communications of the ACM. 2000 Apr 1;43(4):99-105.

[12]. Yan Q, Yu FR. Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communications Magazine. 2015 Apr 8;53(4):52-9.

[13]. Adat V, Gupta BB. A DDoS attack mitigation framework for internet of things. In2017 international conference on communication and signal processing (ICCSP) 2017 Apr 6 (pp. 2036-2041). IEEE.

[14]. Tabassum A, Mustafa MS, Al Maadeed SA. The need for a global response against cybercrime: Qatar as a case study. In2018 6th International Symposium on Digital Forensic and Security (ISDFS) 2018 Mar 22 (pp. 1-6). IEEE.

[15]. Yeboah-Ofori A, Abdulai J, Katsriku F. Cybercrime and risks for cyber physical systems. International Journal of Cyber-Security and Digital Forensics (IJCSDF). 2019;8(1):43-57.

[16]. Petrolo R, Loscri V, Mitton N. Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms. Transactions on emerging telecommunications technologies. 2017 Jan;28(1):e2931.

[17]. Rani S, Kataria A, Sharma V, Ghosh S, Karar V, Lee K, Choi C. Threats and corrective measures for IoT security with observance of cybercrime: A survey. Wireless Communications and Mobile Computing. 2021 Apr 26;2021:1-30.

[18]. Hemdan EE, Manjaiah DH. Cybercrimes investigation and intrusion detection in internet of things based on data science methods. Cognitive Computing for Big Data Systems OverIoT: Frameworks, Tools and Applications. 2018:39-62.

[19]. Khraisat A, Gondal I, Vamplew P, Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity. 2019 Dec;2(1):1-22.

[20]. Nsude I, Elem SN, Uwaomaan. Combating cybercrime through artificial intelligence for sustainable development in nigeria. Artificial Intelligence and the Media.:63.

[21]. Nikhila MS, Bhalla A, Singh P. Text imbalance handling and classification for cross-platform cyber-crime detection using deep learning. In2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) 2020 Jul 1 (pp. 1-7). IEEE.

[22]. Omrani T, Dallali A, Rhaimi BC, Fattahi J. Fusion of ANN and SVM classifiers for network attack detection. In2017 18th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA) 2017 Dec 21 (pp. 374-377). IEEE.

[23]. Ch R, Gadekallu TR, Abidi MH, Al-Ahmari A. Computational system to classify cyber crime offenses using machine learning. Sustainability. 2020 May 16;12(10):4087.

[24]. Boussi GO, Gupta H. A proposed framework for controlling cyber-crime. In2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) 2020 Jun 4 (pp. 1060-1063). IEEE.

[25]. Ullah I, Lane C, Buda TS, Drury B, Mellotte M, Assem H, Madden MG. Classification of cybercrime indicators in open social data. InInformation Management and Big Data: 7th Annual International Conference, SIMBig 2020, Lima, Peru, October 1–3, 2020, Proceedings 2021 May 12 (pp. 317-332). Cham: Springer International Publishing.

[26]. Srinivasan S, Ravi V, Alazab M, Ketha S, Al-Zoubi AM, KottiPadannayil S. Spam emails detection based on distributed word embedding with deep learning. Machine intelligence and big data analytics for cybersecurity applications. 2021:161-89.

[27]. Srinivasan S, Vinayakumar R, Arunachalam A, Alazab M, Soman KP. DURLD: Malicious URL detection using deep learning-based character level representations. Malware analysis using artificial intelligence and deep learning. 2021:535-54.

[28]. Vinayakumar R, Alazab M, Soman KP, Poornachandran P, Venkatraman S. Robust intelligent malware detection using deep learning. IEEE Access. 2019 Apr 3;7:46717-38.

[29]. Al-Garadi MA, Varathan KD, Ravana SD. Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network. Computers in Human Behavior. 2016 Oct 1;63:433-43.

[30]. Berger A, D'Alconzo A, Gansterer WN, Pescapé A. Mining agile DNS traffic using graph analysis for cybercrime detection. Computer Networks. 2016 May 8;100:28-44.

[31]. Singh A, Kaur M. Detection framework for content-based cybercrime in online social networks using metaheuristic approach. Arabian Journal for Science and Engineering. 2020 Apr;45(4):2705-19.

[32]. Manyumwa T, Chapita PF, Wu H, Ji S. Towards fighting cybercrime: Malicious url attack type detection using multiclass classification. In2020 IEEE International Conference on Big Data (Big Data) 2020 Dec 10 (pp. 1813-1822). IEEE.

[33]. Singh A, Kaur M. Cuckoo inspired stacking ensemble framework for content-based cybercrime detection in online social networks. Transactions on Emerging Telecommunications Technologies. 2021 Jun;32(6):e4074.

[34]. Islam MM, Uddin MA, Islam L, Akter A, Sharmin S, Acharjee UK. Cyberbullying detection on social networks using machine learning approaches. In2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE) 2020 Dec 16 (pp. 1-6). IEEE.

[35]. Nouh M, Nurse JR, Goldsmith M. Towards designing a multipurpose cybercrime intelligence framework. In2016 European Intelligence and Security Informatics Conference (EISIC) 2016 Aug 17 (pp. 60-67). IEEE.

[36]. Zulkefli Z, Singh MM, Shariff AR, Samsudin A. Typosquatcyber crime attack detection via smartphone. Procedia Computer Science. 2017 Jan 1;124:664-71.

[37]. Pastor A, Mozo A, Vakaruk S, Canavese D, López DR, Regano L, Gómez-Canaval S, Lioy A. Detection of encrypted cryptomining malware connections with machine and deep learning. IEEE Access. 2020 Aug 26;8:158036-55.

[38]. Ullah I, Mahmoud QH. Design and development of a deep learning-based model for anomaly detection in IoT networks. IEEE Access. 2021 Jul 1;9:103906-26.

[39]. Raza M, Qayyum U. Classical and deep learning classifiers for anomaly detection. In2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST) 2019 Jan 8 (pp. 614-618). IEEE.

[40]. Karie NM, Kebande VR, Venter HS. Diverging deep learning cognitive computing techniques into cyber forensics. Forensic Science International: Synergy. 2019 Jan 1;1:61-7.

[41]. Damaševičius R, Venčkauskas A, Toldinas J, Grigaliūnas Š. Ensemble-based classification using neural networks and machine learning models for windows pe malware detection. Electronics. 2021 Feb 18;10(4):485.

[42]. Adebowale MA, Lwin KT, Hossain MA. Deep learning with convolutional neural network and long short-term memory for phishing detection. In2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA) 2019 Aug 26 (pp. 1-8). IEEE.

[43]. Alam MN, Sarma D, Lima FF, Saha I, Hossain S. Phishing attacks detection using machine learning approach. In2020 third international conference on smart systems and inventive technology (ICSSIT) 2020 Aug 20 (pp. 1173-1179). IEEE.

[44]. Bendiab G, Shiaeles S, Alruban A, Kolokotronis N. IoT malware network traffic classification using visual representation and deep learning. In2020 6th IEEE Conference on Network Softwarization (NetSoft) 2020 Jun 29 (pp. 444-449). IEEE.

[45]. Islam M, Mahmood AN, Watters P, Alazab M. Forensic detection of child exploitation material using deep learning. Deep learning applications for cyber security. 2019:211-9.

[46]. Khan F, Ncube C, Ramasamy LK, Kadry S, Nam Y. A digital DNA sequencing engine for ransomware detection using machine learning. IEEE Access. 2020 Jun 19;8:119710-9.

[47]. Bhalerao R, Aliapoulios M, Shumailov I, Afroz S, McCoy D. Mapping the underground: Supervised discovery of cybercrime supply chains. In2019 APWG Symposium on Electronic Crime Research (eCrime) 2019 Nov 13 (pp. 1-16). IEEE.

[48]. Usman N, Usman S, Khan F, Jan MA, Sajid A, Alazab M, Watters P. Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics. Future Generation Computer Systems. 2021 May 1;118:124-41.

[49]. Khan SA, Khan W, Hussain A. Phishing attacks and websites classification using machine learning and multiple datasets (a comparative analysis). InIntelligent Computing Methodologies: 16th International Conference, ICIC 2020, Bari, Italy, October 2–5, 2020, Proceedings, Part III 16 2020 (pp. 301-313). Springer International Publishing.

[50]. Ravi V, Alazab M, Srinivasan S, Arunachalam A, Soman KP. Adversarial defense: DGA-based botnets and DNS homographs detection through integrated deep learning. IEEE transactions on engineering management. 2021 Mar 12;70(1):249-66.