Review on Deep Learning based Network Security Tools in Detecting Real-Time Vulnerabilities

E. Baraneetharan

Associate Professor and Head, Department of EEE, Surya Engineering College, Erode, India

E-mail: hodeee@surya.ac.in

Abstract

Network connected hardware and software systems are always open to vulnerabilities when they are connected with an outdated firewall or an unknown Wi-Fi access. Therefore network based anti-virus software and intrusion detection systems are widely installed in every network connected hardwares. However, the pre-installed security softwares are not quite capable in identifying the attacks when evolved. Similarly, the traditional network security tools that are available in the current market are not efficient in handling the attacks when the system is connected with a cloud environment or IoT network. Hence, recent algorithms of security tools are incorporated with the deep learning network for improving its intrusion detection rate. The adaptability of deep learning network is comparatively high over the traditional software tools when it is employed with a feedback network. The feedback connections included in the deep learning networks produce a response signal to their own network connections as a training signal for improving their work performances. This improves the performances of deep learning-based security tools while it is in real-time operation. The motive of the work is to review and present the attainments of the deep learning-based vulnerability detection models along with their limitations.

Keywords: Intrusion detection, network security monitoring, wireless security network, cyber security, neural network security

1. Introduction

1.1 Overview of Network Security

Network security is a primary requirement for a computer network to enable restriction of unauthorized access to the data saved in the system. The network security system also

DOI: https://doi.org/10.36548/jucct.2021.4.005
Received: 15.12.2021, received in revised form: 10.01.2022, accepted: 21.01.2022, published: 31.01.2022

improves the operational performances of the network by regulating the traffic flow. Figure 1 explores an overview of the network security tools. The hardware components represent the servers and the computer systems that are connected over the network line. The security system enabled in the hardware components recognizes the entry of flagged data packets as threats and restricts them. These type of security tools are represented as in-line security tools, whereas the out-line security tools are employed to detect the traffic changes in the network connection just by monitoring it without a direct connection. The software components of the network security indicate the usual antivirus setup that can be applied over the network nodes and systems for an added protection. The cloud component security tools provide an offloading environment just by monitoring the changes in the network traffic. Such tools do not block or scan the threats entering the network.

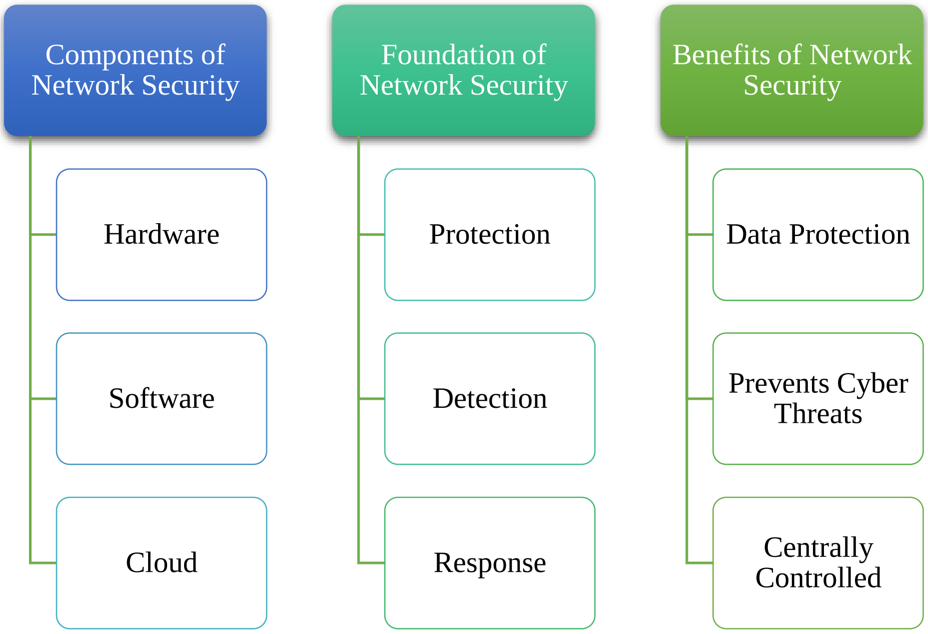

Figure 1. Overview of a Network Security model

Network is the place where all kind of information are stored by a common person or a big firm. The data stored in the network may contain the personal information of a person or customer that has to be secured in a right way. The hackers are always connected to the network for sending continuous intrusions to access such precious data. In some cases the hackers try to change or manipulate the data stored in the network rather than stealing them. The network security tools are centrally placed contrary to the domestic antivirus tool and administrate the operation of the networks from a remote place.

2. Related Work

2.1 Types of Network Security tools and techniques

Access control security tool restricts the entry of unauthorized access to the network environment. This makes the network reliable to the accessible people. However, the access control tools are not efficient in preventing the intrusions created by the accessible users. The access control tool also hinders the entry of new and genuine users into the server and that limits the revenue of a business. Anti-malware tools protect the network by restricting the virus and malware spread over the networks. Therefore it reduces the damage caused by the Trojans and spyware into the network connected systems. Anomaly Detection Engines (ADE) are developed in recent days to provide security over the breaches generated by the hackers. The anomalies can be tacked by the ADE only when the breach type is known and understandable by the tool. The application security system is an efficient tool in protecting certain temporary stored data in a particular application. It protects the applications from loss of information when there occurs a sudden system shutdown due to hardware malfunction or hacking. The data loss prevention system restricts the network accessible user from sharing the information to an unauthorized user. An email security model is also incorporated in such applications that scans the data that are transferred among the users. Moreover such security algorithms are efficient in blocking the attacks spread over the email messages. Figure 2 explores the types of network security techniques and tools available so far.

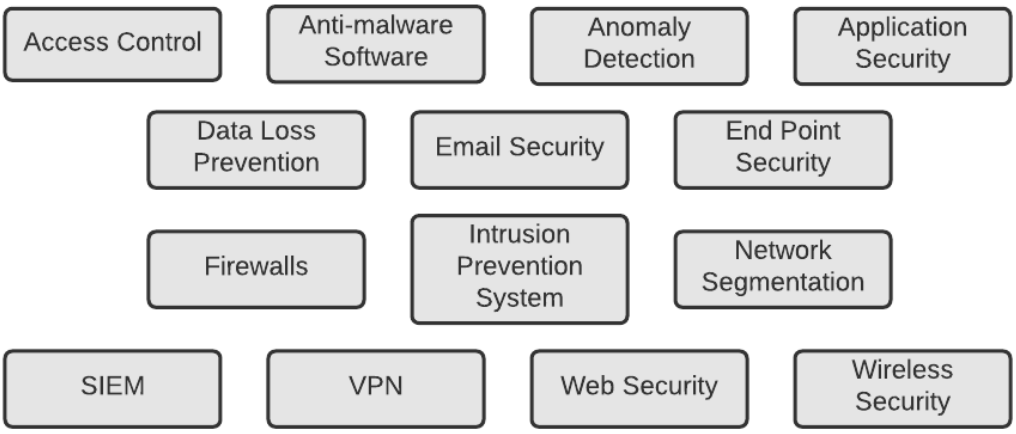

Figure 2. Types of Network Security tools

The endpoint security system creates a block between the personal user system and business user system when both are connected to the same business network. This allows the business user to access just the required information from the network storage. However, this setup protects only the business user system when there is an attack in the network. The firewall model also works in the same principle where the user network is restricted to enter over the general internet service. This improves the authorized traffic inside the network and in turn enables the business networks to run in a better way. The intrusion detection algorithms are developed to scan and monitor each and every packets rolling over the network and thus the system is very effective in observing the known intrusions.

The network segmentation protocol restricts the traffic enabled by the hackers into the network system by categorizing their nature of access. This reduces the presence of overloading effect in the network systems. Security Information and Event Management (SIEM) allows the user to extract the right information from the network in a secure and reduced accessing time. The Virtual Private Network (VPN) creates an encrypted block between the actual network device and the user device during a communication. It analyses the secure socket layer and IP addresses of the remote device for verification. The web security system protects the networks while surfing into the internet services through browsers. It reduces the threat accessibility over a device by making the browser as their access point. Similarly the wireless security system is employed in the place where the network authentications are available to the user through WiFi and other wireless modes. The following section analyzes the network security tools and methods available so far in the digital medium.

3. Literature Survey

3.1 Multifactor Authentication

The multifactor authentication systems on accessing IoT and cloud data are widely employed in recent days for additional security. A light weighted authentication setup was developed to access the large-scale information available online [16]. A bitwise XOR model was utilized with one-way cryptographic hash function that enables better performance while verifying its proof of correctness. An elliptic curve crypto model was designed to create a secure communication in the internet of multimedia things [17]. The design was efficient in addressing the stolen verifier and masquerading attack. However, the multifactor authentication systems are corrupted through temporary information leak attack implemented by an untrue authentication [18].

3.2 Network Behavioral Analysis

Intrusions are generated in recent days by asking the user to download a malicious file in the system. The NBA model reacts to such malicious files by analyzing their deviations on behavior. To address such issue, a botnet detection algorithm was framed by extracting the efficient features from the regular network flow. This classifies the botnet entry to the network flow by understanding their change in operation [19]. The extracted features are also very effective in detecting the encrypted network traffic. An unsupervised machine learning algorithm was developed to classify the network behaviors by making an assessment on malware capability. The network packet natures were verified for understanding the temporary changes [20]. An operating system behavior change detection approach was proposed by analyzing the changes in session and host ports of a virtual network. The experimental work performed with such approach produced a better accuracy in detecting the changes at PCAP dataset [21].

3.3 Threat Intelligence Automation

An automated threat defense algorithm was designed by training it with the data collected from a regular attacker model. The extracted network functions were chained in the model as a service function model for attaining a proactive network structure [22]. A deep learning based threat intelligence scheme was designed to observe threat attacks in space and ground networks. A deep pattern extractor model was placed for observing the hidden patterns from the threatened network. The observed hidden patterns were considered in the work to classify the type of attack. The experimental work performed with TONIoT and NBAIoT datasets showed an acceptable false alarm rate [23]. The automated intelligence techniques failed the system when it was affected with an unknown or a new threat. Therefore, a convolution neural network based algorithm was designed to extract the features of an unknown threat at their first arrival [24].

3.4 Real-time Protection

The distributed denial of service attacks occur in every IoT system when it is placed without a security model. This happens due to continuous transmission of data packets from the sensors to the cloud servers. An experimental work was made using a CNN algorithm in

CIC-DDOS 2019 dataset to prove its efficiency that indicated a noticeable performance when compared to the MLP, DNN and dense MLP algorithms [25]. A Support Vector Machine (SVM) based approach was developed to address the cyber threats on smart meters. The SVM algorithm was merged with temporal failure propagation graph for identifying the threat movement in the network space. The recognition algorithm employed in the work analysed the similarity score among the present event data over the pre-calculated attack data for detecting the changes [26].

3.5 Sandboxing

Sandboxes are a pre-layer protecting system created to project like an end user system in the network layer for observing the malwares without harming the actual user system. In most systems, the sandboxes are operated manually that improves the error rate on estimating the vulnerabilities. Therefore, the artificial user layer is automated with computational algorithms for the parallel execution of data. This improves the performances of data flow along with the data regulation in the blockchain environments [27]. The sandbox models were incorporated to the Linux operating system with pattern matching algorithm for segregating the malware movements over the connected system. The experimental analysis showed a better improvement in detecting the IoT malware samples [28]. The sandbox system was implemented to the hadoop file system for ensuring the data security against the generation of malicious jar file by a legitimate user. The sandbox system analyzed the nature of the jars to avoid spreading it over the data files stored in the hadoop setup [29].

3.6 Forensics

Network forensic is a kind of digital forensic employed to collect legal information and evidence gathering in the network traffic at the presence of intrusions. It helps the users to find out their weakness on network security. The system is very helpful in creating a new network tool with a greater updation. A binary ensemble classifier system was developed to observe the nature of the attacks in botnet systems. The experimental work showed a better accuracy rate with KNN algorithm while using a single classifier system and produced better accuracy value on AdaBoost with decision tree in ensemble model [30]. A methodology called particle deep framework was structured to perform forensic on internet of things network. The network flow information were extracted in the model which were moved further to a particle swarm optimizer for extracting the useful data for deep learning analysis. A deep neural network approach was added up in the line for classifying the abnormalities present in the IoT network.

The work showed a better performance rate while experimenting with UNSWNB15 and Bot-IoT dataset [31].

3.7 Web Application Firewalls

The web application firewalls are efficient in collecting the HTTP network traffic for detecting the cross-site scripting and forgery attacks. It is achieved by creating a wall between in the installed application and the internet, whereas in the regular firewalls a protecting shield or wall is placed at the edge of the network system [32].

4. Discussion

A lot of network security methods are generated every day to improve the performances of the data movement over the internet. Each method have their own merits and limitations. Table 1 explores the attainments and demerits of few network securing methods based on the literature study carried out. The research goes on all day to reduce the specified limitations.

Table 1. Performances of the network security tools

Methodology	Attainments	Limitations
Multifactor Authentication	• Improves convenience • Manageable without network • Updatable Model • Same application can be used for multiple accounts	• Expensive on large scale implementation • Risk of misuse • Irrecoverable when stolen • False positive presence
Network Behavioral Analysis	• Minimization of response time to the attacks • Possibility of 24/7 analysis • Protects from unknown threats • End point intelligence	• Expensive • Requires manual expert interface • Chances for observing false positive and false negative • Specific pattern operation
Threat Intelligence Automation	• Automated • More consistent • Detects own vulnerabilities • High speed response	• Loss of control • Distrust in new implementation • Maintenance required

Real-time Protection	• Spyware protection • Malware rejection • Cost effective • Payment protection	• Limited detection • Loop holes presence • Minimum protection • Slowdowns the system
Sandboxing	• Protects hardware • Prevent unauthorized data access • Absence of conflicts between OS and softwares	• Complex environment • Human interruption required • Costly • Requires technical knowledge • Additional hardware resource
Forensics	• Ensures integrity • Evidence collection • Tracking attacks • Future attack prevention	• Requires internet access • Needs hacking tools • Large storage space needed • Frequent upgrade required
Web Application Firewalls	• Minimal cost • Reacts to internal and external attacks • Prevents DDOS attack • Avoids cookie poisoning	• Requires pre-framed policies • Resource consumption • Frequent re-configuration required • Limited security

Table 2. Role of deep learning in network security

Methodology	**Attainments with deep learning models**
Multifactor Authentication	– Face and hand gesture authentication using Deep CNN [33] – CNN based finger, palm and face print authentication [34]
Network Behavioral Analysis	– Cyber threat detection in IoT using deep neural network [35] – Deep transfer learning on unknown network threats [36]
Threat Intelligence Automation	– Deep learning based threat intelligence system on IoT transportation system [37] – Generative Adversarial Learning for Cyber Threat Intelligence [38]

Real-time Protection	– Multi-layer deep learning network for IoT attack detection [39] – Software defined network based hybrid deep learning threat detection system in Fog-to-Things [40]
Sandboxing	– CNN based malicious code detection on Sandbox environment [41] – Dynamic analysis of IoT botnet using Sandbox [42]
Forensics	– Face sketch synthesis in Internet of Things (IoT) with CNN [43] – Email data forensic using gated RNN [44]
Web Application Firewalls	– Auto threshold deep support vector data description for anomaly detection [45] – Code injection detection using CNN [46]

The arrival of deep learning algorithms move the performances network security tools to a certain extent. Table 2 indicates the role of deep learning models on different network security methods. However, the performance of deep learning algorithms is not satisfied in a few cases due to the advancements of intrusion and malwares. The system lags when there is a new intrusion arrival in the cyber network models. Deep learning algorithm has a limitation where it requires a huge amount of data for its training process. However, such limitations are addressed in recent days with the help of a feedback gained neural network setups.

5. Conclusion

Almost all the sectors in operations are equipped with an internet connection for their control and data storage process. The healthcare sector is a primary application that utilizes the cloud environment to the maximum for saving the personal information of the patients. In the same way, the hotel and trip assisting applications are also store the travel activities of the users. Certain advertising applications developed, collect the history of the users to create a relevant display on their gadgets. In most cases, the users are interested in sharing their own data to an unknown software. Therefore, the critical app developers create some minor malwares for stealing such personal information. The network security tools are developed to identify and block such malwares and intrusions received from unknown sources. The accuracy performances of such intrusion detection systems are improved in recent days through deep learning algorithms. The paper reviewed the role of deep learning algorithms in several network security tools and obtained a research gap that the neural network models does not gain an acceptable accuracy while encountering a new intrusion or vulnerability in the system.

References

[1] Sathesh, A. "Enhanced soft computing approaches for intrusion detection schemes in social media networks." Journal of Soft Computing Paradigm (JSCP) 1, no. 02 (2019): 69-79

[2] Raj, Jennifer S. "Secure Data Sharing Platform for Portable Social Networks with Power Saving Operation." Journal of IoT in Social, Mobile, Analytics, and Cloud 3, no. 3 (2021): 250-262.

[3] Koleshwar, Ankita S., S. S. Sherekar, V. M. Thakare, and Aniruddha Kanhe. "Analytical Classification of Sybil Attack Detection Techniques." In *Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2020*, pp. 89-98. Springer Singapore, 2021.

[4] Joe, C. Vijesh, and Jennifer S. Raj. "Deniable Authentication Encryption for Privacy Protection using Blockchain." Journal of Artificial Intelligence and Capsule Networks 3, no. 3 (2021): 259-271.

[5] Manoharan, J. Samuel. "A Novel User Layer Cloud Security Model based on Chaotic Arnold Transformation using Fingerprint Biometric Traits." Journal of Innovative Image Processing (JIIP) 3, no. 01 (2021): 36-51.

[6] Shanmugapriya, T., K. Kousalya, J. Rajeshkumar, and M. Nandhini. "Wireless Sensor Networks Security Issues, Attacks and Challenges: A Survey." In *International conference on Computer Networks, Big data and IoT*, pp. 1-12. Springer, Cham, 2019.

[7] Mugunthan, S. R. "Soft computing based autonomous low rate DDOS attack detection and security for cloud computing." J. Soft Comput. Paradig.(JSCP) 1, no. 02 (2019): 80-90.

[8] Sable, Saurabh, and Prashant Adakane. "Sensitive Data Security over Network Through a Combination of Visual Cryptography and Data Hiding Mechanism." In *International Conference on Mobile Computing and Sustainable Informatics*, pp. 415-420. Springer, Cham, 2020.

[9] Shakya, Subarana. "An efficient security framework for data migration in a cloud computing environment." Journal of Artificial Intelligence 1, no. 01 (2019): 45-53.

[10] Sivaganesan, D. "Performance Estimation of Sustainable Smart Farming with Blockchain Technology." IRO Journal on Sustainable Wireless Systems 3, no. 2 (2021): 97-106.

[11] Smilarubavathy, G., R. Nidhya, N. V. Abiramy, and A. Dinesh Kumar. "Paillier Homomorphic Encryption with K-Means Clustering Algorithm (PHEKC) for Data Mining Security in Cloud." In *Inventive Communication and Computational Technologies*, pp. 941-948. Springer, Singapore, 2021.

[12] Smys, S., and Haoxiang Wang. "Security Enhancement in Smart Vehicle Using Blockchain-based Architectural Framework." Journal of Artificial Intelligence 3, no. 02 (2021): 90-100.

[13] Bhalaji, N. "Cloud Load Estimation with Deep Logarithmic Network for Workload and Time Series Optimization." Journal of Soft Computing Paradigm 3, no. 3 (2021): 234-248.

[14] Siyad, C. Ismayil, and S. Tamilselvan. "Deep learning enabled physical layer security to combat eavesdropping in massive MIMO networks." In *International Conference on Computer Networks and Inventive Communication Technologies*, pp. 643-650. Springer, Cham, 2019.

[15] Kirubakaran, S. Stewart. "Study of Security Mechanisms to Create a Secure Cloud in a Virtual Environment with the Support of Cloud Service Providers." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 03 (2020): 148-154.

[16] Alsahlani, Ahmed Yaser Fahad, and Alexandru Popa. "LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment." *Journal of Network and Computer Applications* 192 (2021): 103177.

[17] Mahmood, Khalid, Waseem Akram, Akasha Shafiq, Izwa Altaf, Muhammad Ali Lodhi, and SK Hafizul Islam. "An enhanced and provably secure multi-factor authentication scheme for Internet-of-Multimedia-Things environments." *Computers & Electrical Engineering* 88 (2020): 106888.

[18] Wang, Ding, Xizhe Zhang, Zijian Zhang, and Ping Wang. "Understanding security failures of multi-factor authentication schemes for multi-server environments." *Computers & Security* 88 (2020): 101619.

[19] Feizi, Sanaz, and Hamidreza Ghaffari. "Detecting botnet using traffic behaviour analysis and extraction of effective flow features." *International Journal of Internet Technology and Secured Transactions* 12, no. 1 (2022): 49-60.

[20] de Heer, Hugo. "MalPaCA: Malware behaviour analysis using unsupervised machine learning: Comparative analysis of various clustering algorithms on determining the best performance in terms of network behaviour discovery." (2021).

[21] Khan, Abdullah Ayub, and Syed Asif Ali. "Network forensics investigation: behaviour analysis of distinct operating systems to detect and identify the host in IPv6 network." *International Journal of Electronic Security and Digital Forensics* 13, no. 6 (2021): 600-611.

[22] Yurekten, Ozgur, and Mehmet Demirci. "Citadel: Cyber threat intelligence assisted defense system for software-defined networks." *Computer Networks* 191 (2021): 108013.

[23] Al-Hawawreh, Muna, Nour Moustafa, Sahil Garg, and M. Shamim Hossain. "Deep Learning-enabled Threat Intelligence Scheme in the Internet of Things Networks." *IEEE Transactions on Network Science and Engineering* (2020).

[24] Zhao, Jun, Qiben Yan, Jianxin Li, Minglai Shao, Zuti He, and Bo Li. "TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data." *Computers & Security* 95 (2020): 101867.

[25] de Assis, Marcos VO, Luiz F. Carvalho, Joel JPC Rodrigues, Jaime Lloret, and Mario L. Proença Jr. "Near real-time security system applied to SDN environments in IoT networks using convolutional neural network." *Computers & Electrical Engineering* 86 (2020): 106738.

[26] Sun, Chih-Che, D. Jonathan Sebastian Cardenas, Adam Hahn, and Chen-Ching Liu. "Intrusion detection for cybersecurity of smart meters." *IEEE Transactions on Smart Grid* 12, no. 1 (2020): 612-622.

[27] Wang, Shuai, Xiaojun Tu, Hongfeng Chai, Quan Sun, Jie Wu, Hua Cai, and Fei-Yue Wang. "Blockchain-Powered Parallel FinTech Regulatory Sandbox Based on the ACP Approach." *IFAC-PapersOnLine* 53, no. 5 (2020): 863-867.

[28] Uhrıcek, Daniel. "LiSa–Multiplatform Linux Sandbox for Analyzing IoT Malware." (2020).

[29] Begum, Gousiya, S. Zahoor Ul Huq, and AP Siva Kumar. "Sandbox security model for Hadoop file system." *Journal of Big Data* 7, no. 1 (2020): 1-10.

[30] Bijalwan, Anchit. "Botnet forensic analysis using machine learning." *Security and Communication Networks* 2020 (2020).

[31] Koroniotis, Nickolaos, Nour Moustafa, and Elena Sitnikova. "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework." *Future Generation Computer Systems* 110 (2020): 91-106.

[32] Applebaum, Simon, Tarek Gaber, and Ali Ahmed. "Signature-based and Machine-Learning-based Web Application Firewalls: A Short Survey." *Procedia Computer Science* 189 (2021): 359-367.

[33] Aleluya, Earl Ryan M., and Celesamae T. Vicente. "Faceture ID: face and hand gesture multi-factor authentication using deep learning." *Procedia Computer Science* 135 (2018): 147-154.

[34] Sajjad, Muhammad, Salman Khan, Tanveer Hussain, Khan Muhammad, Arun Kumar Sangaiah, Aniello Castiglione, Christian Esposito, and Sung Wook Baik. "CNN-based anti-spoofing two-tier multi-factor authentication system." *Pattern Recognition Letters* 126 (2019): 123-131.

[35] Ullah, Farhan, Hamad Naeem, Sohail Jabbar, Shehzad Khalid, Muhammad Ahsan Latif, Fadi Al-Turjman, and Leonardo Mostarda. "Cyber security threats detection in internet of things using deep learning approach." *IEEE Access* 7 (2019): 124379-124389.

[36] Zhao, Juan, Sachin Shetty, Jan Wei Pan, Charles Kamhoua, and Kevin Kwiat. "Transfer learning for detecting unknown network attacks." *EURASIP Journal on Information Security* 2019, no. 1 (2019): 1-13.

[37] Kumar, Prabhat, Govind P. Gupta, Rakesh Tripathi, Sahil Garg, and Mohammad Mehedi Hassan. "DLTIF: Deep Learning-Driven Cyber Threat Intelligence Modeling and Identification Framework in IoT-Enabled Maritime Transportation Systems." *IEEE Transactions on Intelligent Transportation Systems* (2021).

[38] Zhang, Ning, Mohammadreza Ebrahimi, Weifeng Li, and Hsinchun Chen. "Counteracting Dark Web Text-Based CAPTCHA with Generative Adversarial Learning for Proactive Cyber Threat Intelligence." *arXiv preprint arXiv:2201.02799* (2022).

[39] Diro, Abebe Abeshu, and Naveen Chilamkurti. "Distributed attack detection scheme using deep learning approach for Internet of Things." *Future Generation Computer Systems* 82 (2018): 761-768.

[40] Ullah, Ihtisham, Basit Raza, Sikandar Ali, Irshad Ahmed Abbasi, Samad Baseer, and Azeem Irshad. "Software Defined Network Enabled Fog-to-Things Hybrid Deep Learning Driven Cyber Threat Detection System." *Security and Communication Networks* 2021 (2021).

[41] Xing, Jianhua, Hong Sheng, Yuning Zheng, and Wei Li. "Research on a Malicious Code Detection Method Based on Convolutional Neural Network in a Domestic Sandbox Environment." In *International Symposium on Cyberspace Safety and Security*, pp. 290-298. Springer, Cham, 2020.

[42] Le, Hai-Viet, and Quoc-Dung Ngo. "V-Sandbox for Dynamic Analysis IoT Botnet." *IEEE Access* 8 (2020): 145768-145786.

[43] Elhoseny, Mohamed, Mahmoud Mohamed Selim, and K. Shankar. "Optimal deep learning based convolution neural network for digital forensics face sketch synthesis in internet of things (IoT)." *International Journal of Machine Learning and Cybernetics* 12, no. 11 (2021): 3249-3260.

[44] Hina, Maryam, Mohsin Ali, Abdul Rehman Javed, Fahad Ghabban, Liaqat Ali Khan, and Zunera Jalil. "Sefaced: Semantic-based forensic analysis and classification of e-mail data using deep learning." *IEEE Access* 9 (2021): 98398-98411.

[45] Moradi Vartouni, Ali, Matin Shokri, and Mohammad Teshnehlab. "Auto-Threshold Deep SVDD for Anomaly-based Web Application Firewall." (2021).

[46] Abaimov, Stanislav, and Giuseppe Bianchi. "CODDLE: Code-injection detection with deep learning." *IEEE Access* 7 (2019): 128617-128627.

Author's biography

Dr. E. Baraneetharan received the B.E. degree in Electrical and Electronics Engineering and M.E. degree in Power Electronics and Drives, both from Anna University, Chennai, India, in 2005 and 2009 respectively. He received a Ph.D degree in the field of Electrical Engineering from Anna University, Chennai in 2019. Since 2009, he has held a teaching professorship with special interests in Power electronics, Digital control signals and electromagnetic interference (EMI) for the development in high speed switching circuits. In 2004 itself, he was involved in design and management responsibilities for research and development projects in the Power electronics field for industry and scientific applications. His research interest includes high-efficiency switching circuits with recent digital techniques where he has experience in applications like 75HP/ 460 V industrial motor side, 750 kVA generators in industrial applications. He had published his research papers in several international journals and published two books in the field of electrical and electronics engineering. Presently he is working as an Associate Professor of the concerned department Surya Engineering College, Erode, Tamilnadu, India.