WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Network Security through Deep Learning: A Survey of Attack Detection Techniques

M.P.Venkat Vijay[a], P.Yuvaraj[b] ,B.Nilesh[c] , L.Sivabarathi[d] S.Priyadharsan[e]

[abcde]Student, ComputerScience & Engineering, Paavai College of Engineering, Namakkal

ABSTRACT

The emergence of artificial intelligence and fifth-generation networks has led to new dangers and challenges for wireless communication systems, particularly in cybersecurity. We provide a review of attack detection strategies employing deep learning approach strength in this study. To be more precise, we first provide an overview of the core issues with network security and threat detection and then present a number of well-received deep learning solutions. We focus specifically on attack detection techniques developed on several types of architectures, including auto encoders, generative adversarial networks, recurrent neural networks, and convolutional neural networks, based on categorization using deep learning approaches. Next, in order to demonstrate the current status of attack detection techniques with deep learning structures, we give a few benchmark datasets along with descriptions and contrast how well representing approaches perform. In conclusion, we provide a summary of this work and talk about potential methods to enhance attack detection performance while considering the use of deep learning structures.

Keywords:

Introduction

The ongoing evolution and widespread application of the Internet confer several advantages to a multitude of network users. In the meantime, as networks are used more frequently, network security becomes increasingly crucial. Preventing unwanted access and alteration is the goal of defense when it comes to computers, networks, programs, different types of data, and other relevant topics, all of which are directly tied to network security [1]. However, as more and more systems in the financial, e-commerce, and military become internet-connected, they become targets for network attacks, which increases risk and damage. Essentially, in order to protect network security and identify and stop assaults, effective solutions must be provided. Moreover, distinct attack types typically necessitate distinct approaches to processing. In recent years, scientists have employed diverse machine learning techniques to categorize network intrusions, even in the absence of prior knowledge about their intricate features. However, because of their limits in terms of model complexity, existing machine learning techniques are unable to provide unique feature descriptors to represent the attack detection problem. By using neural networks to mimic the structure of the human brain, machine learning has recently achieved a significant breakthrough. These methods, known as deep learning techniques because of their general architecture of deep layers to handle complex problems, are called deep learning. One of the most notable experiments for the game of "go," leveraging the power of a common type of deep learning structure—convolutional neural networks—among these fruitful apps is Google's AlphaGo.

This paper explains deep learning, which is difficult in its original structures and domain-oriented applications, for individuals who want to study network security using deep learning techniques. In essence, a significant body of prior research has been done on attack detection with deep learning methods. Among these, a number of literature studies [2–8] have been done to obtain inspiration for our paper's central idea—applying deep learning to challenge detection. For instance, Berman et al. [5] offer a wealth of reading materials outlining the fundamental concepts and evolution of deep learning techniques, as well as the applications that go along with them in attack detection. In the meantime, they provide a thorough analysis of the relevant literature using the terms "deep learning," "invasion," and "attack" selection. This gives the researchers access to a wealth of background resources. 35 well-known network datasets are described and categorized into seven groups by Ferrag et al. [6], who view the dataset as significantly useful to intrusion detection. In order to assess and analyze the efficiency using accuracy and false alarm rate based on real traffic datasets, namely CSE-CIC-IDS2018 and Bot-IoT, they develop seven presentative models for each category.

In the meantime, they provide a thorough analysis of the relevant literature using the terms "deep learning," "invasion," and "attack" selection. This gives the researchers access to a wealth of background resources. 35 well-known network datasets are described and categorized into seven groups by Ferrag et al. [6], who view the dataset as significantly useful to intrusion detection. In order to assess and analyze the efficiency using accuracy and false alarm rate based on real traffic datasets, namely CSE-CIC-IDS2018 and Bot-IoT, they develop seven presentative models for

each category. As a matter of fact, each of the aforementioned review papers focuses on a different aspect of security, be it databases, types of attacks, or datasets. As opposed to other approaches, we want to base our article on deep learning models, giving particular consideration to attack detection techniques built on various deep learning architectures. Additionally, we provide a fair comparison and our own detailed study of how well representation techniques work when compared to benchmark datasets. We hope that our study will provide readers interested in learning more about how various deep learning architectures impact attack detection with a more readable resource.

The remainder of our work is arranged as follows. Through an overview of the research background, Section 2 focuses on notions of attack detection and cyber applications. Overviews of several supervised and unsupervised deep learning techniques for attack detection are provided in Section 3. The techniques are structured differently. In Section 4, a number of deep learning techniques are compared in terms of performance, and datasets are presented. In Section 5, many suggestions for further research are presented along with a discussion and conclusion based on the existing foundations.

Attack Detection

Attacks can be defined as efforts to get beyond the system's security controls, which makes it easier for attackers to access, change, or even take down the system. As wireless communication systems technologies advance, more frequent network attack activities have been suggested as major concerns to network security, particularly security of wireless communication systems, because of the openness characteristics of wireless channels. As we currently live in the era of big data and machine learning [9], users must prioritize cybersecurity in wireless communication systems to safeguard their computers, networks, and data from intrusions. Cyber systems are vulnerable to a variety of attacks, including spoofing, anomalous packet attacks, distributed denial of service, and flooding. Numerous strategies have been offered by researchers to address attack threads in cybersecurity [10]. Attack detection is one of the best methods available for monitoring, preventing, and resisting attacks. It provides a comprehensive and dynamic security mechanism. Attack detection, in particular, would gather data by keeping an eye on the network, system state, behavior, and system usage. This would enable it to automatically identify instances of system users using the system without authorization and external attackers attacking the system.

Machine learning has advanced at an astonishing rate in the last several years. Deep learning structures create artificial neural networks to mimic the interconnecting neurons of human brains, which gives them a unique ability to handle complex issues among other machine learning techniques. As a result, researchers use a variety of deep learning techniques to detect attacks, producing noteworthy results. However, because deep learning techniques have limitations, there are still a lot of unanswered questions. It is crucial to summarize the ways in which earlier techniques used deep learning techniques to identify threats, as this could provide fresh insights for advancements in the future.

2.1 Intrusion Detection

By gathering and examining network activity, security logs, and other data on the network and among connected computers, intrusion detection systems can identify hostile activity [16]. In essence, an intrusion detection system, which can provide real-time system protection, looks for anomalous activity against the system security policy and indications that the system is under attack. In conventional system configurations, intrusion detection systems serve as a sensible, effective, and active addition to firewalls, which serve as a kind of passive attack defences. The fundamental foundation of a traditional intrusion detection system is the misuse of intrusion detection technology, which primarily extracts traits or guidelines of intrusion behavior. Following the introduction of conventional machine learning models for the identification of abnormal behavior, intrusion detection systems have evolved to perform probability statistical modeling for normal behavior, which enables the analysis and alarming of aberrant behavior with a significant divergence. However, because of its limited capacity to define issue spaces and its complexity in modeling harmful activities, such a system may produce disappointing results.

Deep learning technology is used to examine network packets in order to further overcome the drawbacks of classic machine learning techniques. This gradually shifts the popular conception of intrusion detection from a blacklist to a white model. Shone et al. [17] have suggested a new deep learning model for NIDS that is useful for analyzing network traffic when using symmetrical deep autoencoder technology. Vinayakumar et al. [18] construct a system call modeling methodology with integration method for anomalous intrusion detection system based on LSTM algorithm.

2.2 Malware Detection

Malware is intended to lower a computer, server, or computer network's vulnerability and performance. Malware has the potential to completely destroy the system in extreme cases. First, malware must be installed on the intended machine. After then, it could run scripts, code, active content, and other programs automatically or in response to commands from people. It should be mentioned that these programs or codes may fall under the categories of malware, worms, Trojan horses, spyware, advertising software, and computer viruses.

We categorize malware detection techniques into two groups: anomaly-based detection and signature-based detection. The first group includes traditional antivirus software, which uses file signatures to identify harmful files. On the other hand, a lot of false positives could result from harmful codes that are only slightly distorted. Subsequently, sandbox and virtual machine technologies began to identify the dynamic behaviors of viruses; this can be considered a significant advancement from static detection to dynamic analysis, significantly enhancing the capacity to identify undiscovered dangerous code.

Saxe, for instance, talks on the deep learning of a four-layer network application in [19]. PE Metadata Features can be employed to obtain suitable computational feature text extraction technology. In order to categorize using character-level embeddings, the author suggests using the eXpose neural network, which uses the original short strings as input and extracts features. The express method outperforms the baseline method based on manual feature extraction due to the self-extraction feature design.

Deep Learning Methods for Attack Detection

We also loosely classify the existing deep learning techniques for attack detection [23] into three categories, taking into account the classification of earlier studies [24, 25]. These categories include unsupervised techniques (autoencoder (AE), deep belief network (DBN), and generative adversarial network (GAN)), supervised techniques (deep neural network (DNN), convolutional neural network (CNN), and recurrent neural network (RNN)), and other hybrid approaches. The specifics of this classification are displayed in Figure 1. In essence, more classification criteria are present. Berman et al. [5], for instance, examine related deep learning techniques based on the nature of assaults and highlight the diverse applications of deep learning. Additionally, Al-Garadi et al. [2] provide a thorough overview of deep learning techniques centered on cybersecurity applications.

Using various deep learning algorithms may provide distinct benefits for attack detection techniques. Because manually labeled samples contain a large amount of information, supervised learning based algorithms frequently produce excellent accuracy. The typical performance of unsupervised learning based approaches is poor if there is insufficient knowledge from labeled data. Manual labeling, however, takes a lot of time, particularly for sophisticated attacks. Because real-world network attacks are inherently complicated, there are even certain examples that defy easy categorization. This means that systems based on unsupervised learning could function effectively even in the absence of prior awareness of threats, which is a clear benefit.

Hybrid approaches reduce the quantity of training samples while retaining a reasonable level of performance, making them appropriate for handling scenarios including variant attacks. However, its widespread use is hindered by its often complex structure and high computation time.

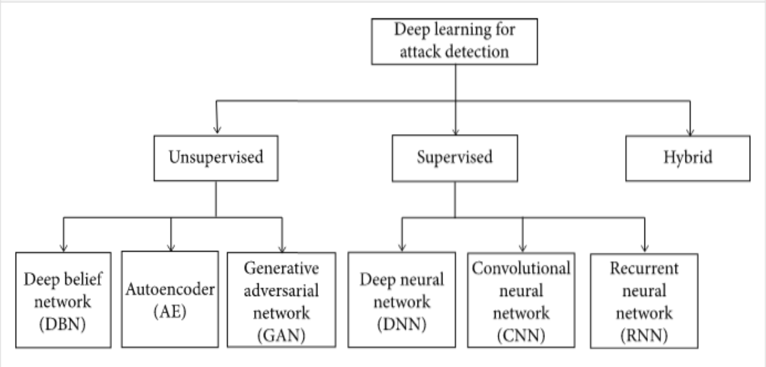

Deep learning for attack detection
Unsupervised
Supervised
Hybrid
Deep belief network (DBN)
Autoencoder (AE)
Generative adversarial network (GAN)
Deep neural network (DNN)
Convolutional neural network (CNN)
Recurrent neural network (RNN)

Figure 1: Classification of DL Algorithms for attack Detection

3.1 Based Methods for Attack Detection Autoencoder

Let's start by introducing the AE architecture, which is essentially a neural network-structured data compression technique. It can, in fact, reassemble the representation into the output after first compressing the input into a feature space representation. As an example of a standard representation learning algorithm, AE is frequently utilized for outlier detection and dimension reduction. Cybersecurity researchers also use AE to represent aberrant behaviors in its compressed feature space, which offers dynamic representation for threats that are not yet known to exist. Hybrid approaches reduce the quantity of training samples while retaining a reasonable level of performance, making them appropriate for handling scenarios including variant attacks. However, its widespread use is hindered by its often complex structure and high computation time.

Zhang et al. [26] propose to detect network intrusion by stacking dilated convolutional AE (DCAEs), which is a successful combination of representation learning and self-taught, in order to extract useful feature descriptors from original network traffic data. More specifically, the preprocessing stage converts the initial network traffic data into a vector. DCAEs use a vast number of unlabeled samples to learn the hierarchical structure of feature representation during unsupervised training. The feature description ability discovered from the unlabeled cases can then be improved and fine-tuned using the backpropagation technique with a few tagged instances. Using unsupervised pretraining and real network traffic actually improves the adaptability and flexibility of their model, enabling it to handle complex raw data.

Javaid et al. [29] use self-taught learning (STL) for training and sparse AE and softmax-regression layer for building in order to create a customizable system for detecting intrusion threats. In particular, their suggested STL may be broken down into two stages: first, sparse AE is utilized for unsupervised feature learning, and then, following feature extraction, softmax-regression is applied for classification. In fact, the use of STL might significantly enhance a created network's capacity to learn in the face of unknown threats, as new attack categories could be examined gradually during runtime without the need for extensive training.

3.2 Generative Adversarial Network Based Methods for Attack Detection

One of the most promising unsupervised learning techniques to be introduced in recent years is the generative adversarial network (GAN), which finds inherent patterns in data to produce new examples. The zero-sum game concept serves as the primary source of inspiration for GAN. It continues to play games between the generator and discriminator when applied to a deep neural network, and eventually it learns the distribution representation of real data. is to mimic, model, and acquire as much knowledge as possible about the distribution properties of real data, whereas the purpose of is to determine if an input data is an output of or real data. The creation and discrimination abilities of both can be significantly enhanced by the ongoing rivalry between these internal models.

Although GAN is still in its infancy and requires a lot of training, researchers have built several successful attack detection apps by treating it as a building block. To identify jamming assaults on wireless communications, for example, Erpek et al. [38] offer a GAN-based technique and defend it using gathered attack data. Their model specifically comprises of a jammer, a receiver, and a transmitter. While the jammer gathers channel state and ACKs to build a classifier that could successfully anticipate the next transmission and block it, the transmitter uses a pretrained classifier to forecast the current channel state and determine whether to send based on the most recent sensing findings. Under the average power constraint, the jammer controls the power using the classification score.

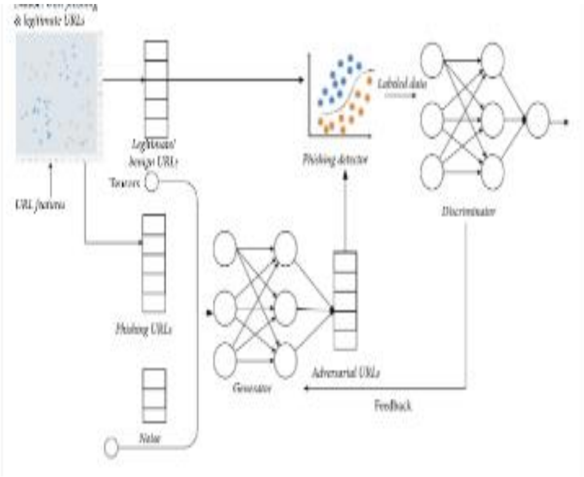


Figure 2: Structure of GAN Model

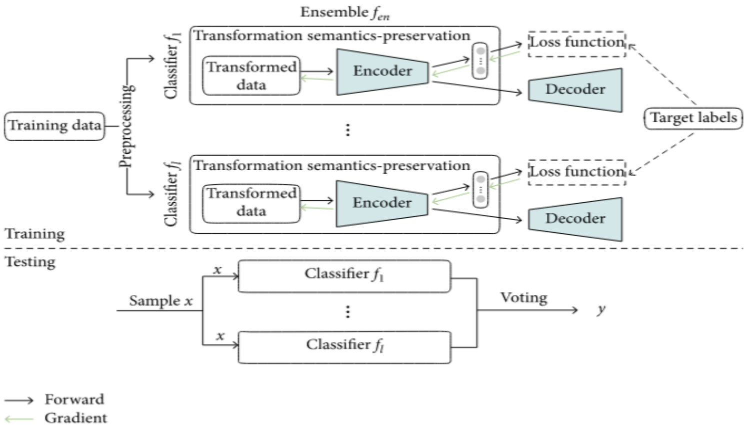
Because machine learning technology can detect phishing URLs—that is, phony web addresses—and respond to them quickly, it is a popular method of phishing detection. By altering components, an opponent might circumvent the URL classification system, nevertheless. AlEroud and Karabatis [39] suggest employing a GAN generator to produce URL-based phishing instances, which are subsequently sent to a discriminator, or black-box phishing detector, in order to address this issue. The generator network in their proposed GAN model, whose structure is depicted in Figure 4, has the ability to produce perturbed versions of actual phishing samples and turn them into adversary examples. Working as a phishing detector, the discriminator network learns to identify both artificial and real cases, updating the generator parameters and weights based on information gleaned from the discriminator.

The field of assault detection does not frequently use GAN. In actuality, the structures and algorithms of GAN are rapidly evolving. As of right now, GANs have demonstrated encouraging outcomes in a variety of fields, which makes us think that this new method for synthesizing attempts will play a big role in developing a defensive mechanism. Such an innovative defensive technique can also do a great deal of work, including opinion spamming, stopping zero-day phishing efforts, and identifying intrusion threats. As a result, we believe there is a large body of research between GAN structure and attack detection field.

4. Other Deep Learning Methods for Attack Detection

Li et al. [57] used a hybrid deep learning approach based on AE and DNN to detect malicious code early in 2015. To be more precise, they use AE to minimize the dimensionality of the original data and concentrate on the key elements. After that, they employ a DBN-based learning model, which comprises of a layer of BPNN and multilayer RBM, to detect malicious code. By characterizing BP as supervised trained and each layer of RBM as unsupervised trained, their ideal hybrid model is ultimately achieved by fine-tuning the entire network. Their hybrid network has a greater detection accuracy than other DBN-based networks, according to experiments.

Ludwig [58] uses an ensemble network later in 2017 to categorize different kinds of attacks. Actually, many classifiers are used by neural network learning to classify targets, and the combined results create reliable outputs. For improved performance, their suggested approach combines AE, BNN, DNN, and extreme learning machine to discern between typical and anomalous behaviors. Promising results are obtained when using their suggested ensemble technique for detection tasks, outperforming single classifiers in terms of accuracy.



Ludwig [58] uses an ensemble network later in 2017 to categorize different kinds of attacks. Actually, many classifiers are used by neural network learning to classify targets, and the combined results create reliable outputs. For improved performance, their suggested approach combines AE, BNN, DNN, and extreme learning machine to discern between typical and anomalous behaviors. Promising results are obtained when using their suggested ensemble technique for detection tasks, outperforming single classifiers in terms of accuracy. Liu et al. [60] offer an end-to-end detection technique in 2019 to efficiently detect network assaults. The author suggests two payload classification methods, PL-CNN and PL-RNN, based on the deep learning model. Without using feature engineering or end-to-end detection, the model picks up feature representation from the original payload. Simultaneously, they develop a data preparation technique that maintains efficiency while retaining sufficient information. Using the DARPA 1998 dataset, the accuracy of the suggested approaches is 99.36% and 99.98%, respectively. In order to address the practical issue, the suggested approaches encourage the utilization of network data flow for efficient end-to-end attack detection.

Zhang et al. [61] most recently in 2019 take the original data information for analysis directly instead of designing the flow's features. Deep network, a new network intrusion detection model that combines the enhanced leNet-5 and LSTM neural network structure, is proposed concurrently with learning the temporal and spatial properties of flow. The CTU and CICIDS2017 datasets are used to assess the network's performance. Both the volume of traffic and the kind of the attack are high. The experimental findings demonstrate that the network model can obtain the highest detection accuracy and performs better than existing network intrusion detection models.

Conclusion

Deep learning achieves notable outcomes in the areas of unsupervised feature learning and pattern recognition by processing data using cascaded layers in a hierarchical structure. Motivated by the effectiveness of deep learning techniques, we think deep learning is critical to the field of network security, leading us to examine the state-of-the-art deep learning techniques for attack detection. We examine current approaches, categorize them based on various deep learning methodologies, and condense the effectiveness of the most exemplary approaches.The study of using deep learning techniques to attack detection has advanced significantly in the last several years. However, there are still a lot of issues. First of all, deep learning techniques are difficult to adapt and use as real-time classifiers for attack detection. The majority of earlier studies just reduced feature dimensions in order to minimize computing costs during the feature extraction phase. Second, image analysis and pattern recognition are suitable applications for the majority of deep learning approaches. Therefore, it will be interesting to see how to use deep learning techniques to classify network traffic in a reasonable manner. Thirdly, the outcomes of the categorization will be improved with further data from the experiments [68]. Nonetheless, the majority of attack detection issues lack adequate data. As a result, numerous experiments have demonstrated that integrating supervised and unsupervised learning may result in improved performance. Furthermore, it is still unclear how to use the advancements in IoT [69], fog, cloud [70], and big data technologies to enhance the efficacy of deep learning-based threat detection techniques. Based on the aforementioned study, we believe that this overview will be helpful to people who have suggestions for enhancing the accuracy of attack detection; our review will offer direction and dictionaries for future research in this area.

REFERENCES

1. S. Aftergood, "Cybersecurity: the cold war online," Nature, vol. 547, no. 7661, pp. 30-31, 2017.
2. M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," 2018, http://arxiv.org/abs/ 11023.

3. G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," in Proceedings of 2018 10th International Conference on Cyber Conflict (CyCon), pp. 371–390, IEEE, Tallinn, Estonia, June 2018.
4. D. Berman, A. Buczak, J. Chavis, and C. Corbett, "A survey of deep learning methods for cyber security," Information, vol. 10, no. 4, p. 122, 2019.
5. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, p. 102419, 2020.
6. C. S. Wickramasinghe, D. L. Marino, K. Amarasinghe, and M. Manic, "Generalization of deep learning for cyber-physical system security: a survey," in Proceedings of IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, pp. 745–751, IEEE, Washington, DC, USA, October 2018.
7. Y. Xin, L. Kong, Z. Liu et al., "Machine learning and deep learning methods for cybersecurity," IEEE Access, vol. 6, pp. 35365–35381, 2018.
8. X. Xu, C. He, Z. Xu, L. Qi, S. Wan, and M. Z. A. Bhuiyan, "Joint optimization of offloading utility and privacy for edge computing enabled iot," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 2622–2629, 2020.
9. X. Xu, Q. Liu, X. Zhang, J. Zhang, L. Qi, and W. Dou, "A blockchain-powered crowdsourcing method with privacy preservation in mobile environment," IEEE Transactions on Computational Social Systems, vol. 6, no. 6, pp. 1407–1419, 2019.
10. X. Xu, X. Liu, Z. Xu, F. Dai, X. Zhang, and L. Qi, "Trust-oriented iot service placement for smart cities in edge computing," IEEE Internet of Things Journal, vol. 7, 2019.
11. X. Xu, Y. Chen, X. Zhang, Q. Liu, X. Liu, and L. Qi, A Blockchain-Based Computation Offloading Method for Edge Computing in 5g Networks, John and Wiley, Hoboken, NJ, USA, 2019.
12. C. Wang, Z. Chen, K. Shang, and H. Wu, "Label-removed generative adversarial networks incorporating with k-means," Neurocomputing, vol. 361, pp. 126–136, 2019.
13. T. Meng, K. Wolter, H. Wu, and Q. Wang, "A secure and cost-efficient offloading policy for mobile cloud computing against timing attacks," Pervasive and Mobile Computing, vol. 45, pp. 4–18, 2018.
14. X. Li and H. Wu, "Spatio-temporal representation with deep neural recurrent network in MIMO CSI feedback," , 2019, CoRR abs/1908.07934.
15. R. Vinayakumar, K. Soman, and P. Poornachandran, "Evaluating effectiveness of shallow and deep networks to intrusion detection system," in Proceedings of 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1282–1289, IEEE, Udupi, India, September 2017.
16. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.
17. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," IEEE Access, vol. 7, pp. 41525–41550, 2019.
18. J. Saxe and K. Berlin, "expose: a character-level convolutional neural network with embeddings for detecting malicious urls, file paths and registry keys," 2017, http://arxiv.org/abs/ 1702.08568.
19. R. Pascanu, J. W. Stokes, H. Sanossian, M. Marinescu, and A. Thomas, "Malware classification with recurrent networks," in Proceedings of 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1916–1920, Queensland, Australia, April 2015.
20. Z. Feng, C. Shuo, and W. Xiaochuan, "Classification for dga-based malicious domain names with deep learning architectures," in Proceedings of 2017 Second International Conference on Applied Mathematics and Information Technology, London, UK, January 2017.
21. J. Woodbridge, H. S. Anderson, A. Ahuja, and D. Grant, "Predicting domain generation algorithms with long short-term memory networks," 2016, http://arxiv.org/abs/ 1611.00791.
22. M. Z. Alom, T. M. Taha, C. Yakopcic et al., "The history began from alexnet: a comprehensive survey on deep learning approaches," 2018 pages, CoRR abs/1803.01164.
23. E. Aminanto and K. Kim, "Deep learning in intrusion detection system: an overview," in Proceedings of 2016 International Research Conference on Engineering and Technology (2016 IRCET), Higher Education Forum, Seoul, South Korea, January 2016.
24. L. Deng, "A tutorial survey of architectures, algorithms, and applications for deep learning," APSIPA Transactions on Signal and Information Processing, vol. 3, 2014.
25. Y. Yu, J. Long, and Z. Cai, "Network intrusion detection through stacking dilated convolutional autoencoders," Security and Communication Networks, vol. 2017, Article ID 4184196, 10 pages, 2017.
26. M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, "Autoencoder-based feature learning for cyber security applications," in Proceedings of 2017 International Joint Conference on Neural Networks (IJCNN), pp. 3854–3861, IEEE, San Diego, CA, USA, June 2017.

27. F. Farahnakian and J. Heikkonen, “A deep auto-encoder based approach for intrusion detection system,” in Proceedings of 2018 20th International Conference on Advanced Communication Technology (ICACT), pp. 178–183, IEEE, Chuncheon, South Korea, July 2018.
28. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A deep learning approach for network intrusion detection system,” in Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies (formerly BIONETICS), pp. 21–26, New York, NY, USA, December 2016.
29. D. Papamartzivanos, F. Gomez Marmol, and G. Kambourakis, Introducing Deep Learning Self-Adaptive Misuse Network Intrusion Detection Systems, IEEE Access, Piscataway, NJ, USA, 2019.