ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 8, August 2022

A Survey of Network Intrusion Detection Techniques Using Deep Learning

[1] Auwal Sani Iliyasu, [2] Ibrahim Abba, [3] Badariyya Sani Iliyasu, [4] Munzali Surajo

[1] Department of Computer Engineering Technology, Kano State Polytechnic, Kano, Nigeria.
[2] Department of Electrical Engineering, Kano State Polytechnic, Kano, Nigeria.
[3] Department of Computer Science, Federal College of Education (Technical), Bichi, Kano, Nigeria.
[4] Department of Electrical Engineering, Kano State Polytechnic, Kano, Nigeria.
Corresponding Author Email: [1] engrausan@gmail.com, [2] ibrahimaba12950@yahoo.com, [3] ausan84@yahoo.co.uk, [4] munzalisurajo@gmail.com

***Abstract*— Network intrusion detection has been studied for long time, with many techniques such as signature-based methods and classical machine learning methods currently available. Recently, DL techniques have received considerable attention for use in intrusion detection systems, due to their inherent advantages such as automatic feature learning. This paper gives an overview about DL techniques employed in intrusion detection to enable new researchers who wish to begin research in the field to be conversant with the state-of-the-art methods as well as unexplored areas.**

***Index Terms*—Intrusion detection, network security, deep learning, machine learnings.**

I. INTRODUCTION

The proliferation of marketplace for hacking skills and illegal hacking forum has simplified cyber-attacks to the extent that, even a low-skilled hacker can inflict a substantial damage by merely purchasing vulnerabilities, user-friendly hacking scripts, software, and tools [1]. As systems and applications become increasingly more complex, they are likely to suffer from more bugs and vulnerabilities that might be exploited by malicious users. Hence, there is need for a continuous upgrade of existing security infrastructures such as Intrusion detection systems (IDS) [2]. An IDS aims to protect the network systems against malicious activities, attacks, violations of security policies etc.

Therefore, An IDS can be deployed as either Host-based or a network Network-based. However, in this work, we are particularly interested in IDS that monitors network systems [3].

Network intrusion detection techniques can be broadly categorized in to two: Signature-based methods and Anomaly-based or machine learning-based [3]. In Signature-based methods, an incoming network traffic is matched against commonly known attacks signatures, which are identified by domain experts. Thus, signature-based methods effectively detect known attacks, however they perform poorly against novel attacks[4]. On the other hand, Anomaly-based/machine learning-based methods try to establish a model of benign traffic, and then flag any network traffic that deviates from the model as an attack[5].

However, recently, the emergence of technologies such as cloud computing, Internet of things (IoT), has resulted in increase in volume and complexity of network traffic. On the other hand, deep learning (DL) techniques are efficient in handling large and complex datasets. As an end-to-end learning model, DL offers advantages such as automatic feature learning which eliminate the need of a domain expert for feature selection [6]. Hence, there is growing interest in applying DL techniques for network intrusion detection [7].

Therefore, in this paper, we provide an overview on research works that apply Deep learning models for Network Intrusion detection. Our purpose is to provide more depth in the area, to enable new researchers who wish to begin research in the field to be conversant with the state-of -the art methods as well as unexplored areas. Therefore, other works such as those that employ classical machine learning techniques are out of the scope of the review. The paper is organized as follows: Section 2 discusses the commonly used DL architectures; Section 3 presents our Taxonomy of works that apply DL techniques for intrusion detection. Section 4 concludes the paper.

II. DL ARCHITECTURES

DL composed of multiple layers of artificial neurons capable of learning representation/pattern using multiple levels of abstraction [8]. DL has seen considerable adoption in many fields such as computer vision, Natural Language processing etc. This subsection explains some state-of-the-art Deep Learning architectures commonly employed for intrusion detection.

A. Multi-layer Perceptron (MLP)

The Multi-layer Perceptron MLP, also known as feed-forward networks are neural networks architectures with at least one hidden layer beside the conventional input and output layers. Layers in MLP are made up of nodes referred to as neurons, each neuron is fully connected to all neurons in the previous layer. Neurons present in each given layer functions independently without sharing any connection. These layers are connected to provide only unidirectional flow of information. Hence the name feed-forward networks. The primary task of MLP is to approximate any given function by making a neuron takes a sum of dot product of its weights with its inputs, and then pass it through a non-linear activation function to produces an output. The output serves as input to another neuron in the subsequent layer. The last fully connected layer is referred to as the output layer and represents the classes score in the classification context [9].

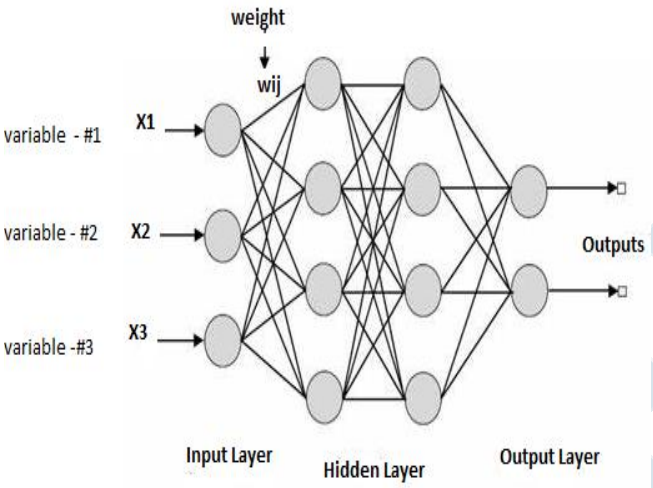

Fig.1. Feed-forward Network Architecture

B. Convolutional Neural Network (CNN)

Convolutional Neural Networks are designed to overcome the drawbacks of overfitting and scaling with high dimensional data associated with regular neural network like MLP, whereby, each neuron in one layer is connected to all other neurons in the next layer. CNN architecture models connectivity pattern of Neurons in mammalian visual cortex, in which individual neurons respond to stimuli only in a limited region of a receptive field. It is made up of a sequence of layers called convolutions. A collection of these fields overlaps to cover the visual area. Each neuron in a convolution layer is connected to a small region of the preceding layer using what is termed as a kernel or filter. This highly reduces the parameter space, and enables it to scales well with data of high dimension. Each layer of a CNN transforms multi-dimensional input volume to another multi-dimensional output volume of neuron activation. However, there exists a layer called pooling which is often sandwiched between one or two convolution layers to enable down sampling of the output. Finally, the last hidden layers of CNN architecture usually employ fully connected layers [10].

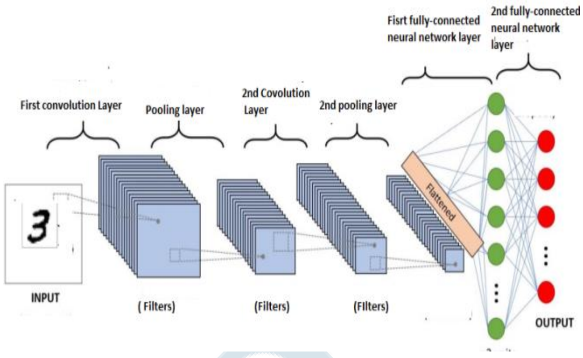

Fig. 2 CNN Architecture

C. Recurrent Neural Network (RNN)

A neural network which has a self-recurrent connection in addition to forward flow of information is referred to as Recurrent neural network. It is a form of artificial neural networks in which the self-recurrent connection acts as some kind of memory that allows it to store temporal information. In this architecture, the output of a recurrent neuron at time step t is a function of all the inputs from previous time steps. This feature of the RNN makes it more suited for sequential data such as time series prediction and speech recognition in which good performance has been recorded in a number of literatures. The long-short term memory (LSTM) was introduced to tackle the gradient problem associated with Conventional RNN when training long sequences. LSTM are capable of detecting long-term dependencies in a data and also converge faster. Thus, making them more preferable than the traditional RNN [11].

D. Autoencoder

Another form of artificial neural network is the Autoencoder. This ANN learns to reproduces a given input as its output. The network is composed of Encoder function $h = f(x)$, a feature extraction function which is a hidden layer and a decoder function $r = g(h)$. The internal representation of the input data is learnt by the Encoder function while the decoder function reconstructs the input from the output of the encoder function.

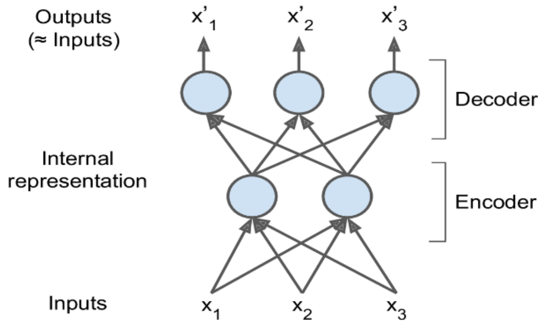

Fig. 3 Autoencoder

It is worth noting that the output is not an exact replica of the input but an approximate value even though the Autoencoder constructs a copy its input as its output. The model is constrained such that it prioritizes which aspect of the input data to learn. As an analogy, noise could be added to the input the network will be trained to recover the original input. The presence of the constraints forces the Autoencoder to learn efficient representation of the input data instead of copying the input directly to the output. This feature makes the Autoencoder suitable for dimensionality reduction as the learned representation which are referred to as codings have much lower dimensionality than the original input data. Autoencoders find suitable application in model where new data that resembles the training data is randomly generated [12].

E. Generative Adversarial Network (GAN)

A new class of artificial neural network is the GAN is a recently developed by Goodfellow et al [citation]. The model comprises of a combination of two neural networks which are trained in adversarial setting. The first network composes of A generator which takes in a random noise and generates new data instances, while the second neural network, receives input from both the generator and the original training data and is termed as discriminator. Each data instances are then reviewed by the discriminator and a decision is made on whether the data is from actual training dataset (real) or from the generator. Theoretically, there exist a point where the generator captures the whole training data distribution and which the discriminator becomes unable to ascertain whether the inputs are from the generator or not. Hence, the GAN is said to be fully trained at this point [13]..

III. TAXONOMY OF DEEP LEARNING-BASED NETWORK INTRUSION DETECTION TECHNIQUES

This work will employ the following criteria to categorize research works in literature that apply deep learning techniques for network intrusion detection problem

- Features
- Model type
- Learning mode

a. Features

The feature refers to the traffic attribute, which is used as the input to the deep learning model. It mainly comprises the following:

- Packet-based features: this mainly consist of layer 3 and layer 4 header fields such as port numbers, protocols, flags etc. Since, there are several combinations of these fields, the useful ones are carefully selected by domain expert to serve as features to deep learning techniques. However, in a situation where the approach is an and end-to-end, the whole packets can be used as input to the deep learning model [5].
- Flow based features: network flow is described as comprising packets sharing the following five tuples: source IP address, destination IP address, port numbers and protocols. Flow based features comprises mainly of Flow statistics such as minimum packet length, average packet length, volume of packet exchange in forward directions etc. These attributes are obtained after completion or termination of a flow. There exist many combinations of these attributes to be used as features [14].
- Time-series properties: these are similar to flow-based features; however, time-series features are derived when an arbitrary number of consecutive packets in a given flow are observed instead of an entire flow. The packets can be sampled in any part of a flow not necessarily at the beginning. The features derived may comprises properties such as inter-arrival time between consecutive packets, direction of consecutive packets, packets length etc. One advantage of time-series features over flow-based features is that, they could be used for real-time classification, since features can be generated before completion or termination of a flow. In recent studies [citation] where time-series features were employed, as few as 20 packets in a flow were used to achieve a reasonable accuracy [15].

b. Model type

This refers to the actual deep learning algorithm used in the traffic classification task. Several models and architectures such as MLP, CNN, RNN, LSTM, AEs, GAN and DBN have been employed. One can refer to section 3 for a detailed explanation about these models.

c. Learning Mode

The learning mode refers to the way in which the deep learning algorithm is trained. The most popular deep learning mode used in network traffic classification is the supervised learning. However, unsupervised learning, semi-supervised learning and one shot or few shot learning methods are also significantly employed.

Table 1 present our taxonomy of research works that employ DL techniques for intrusion detection

Table 1 Taxonomy of recent representative studies of DL techniques in NIDS

Ref.	Features	Model Type	Learning method
Javaid et al. [16]	Flow-based	MLP	Supervised
Roy et al. [17]	Flow-based	MLP	Supervised
Sydney et al. [18]	Packet-based	MLP	Supervised
Yin et al. [19]	Packet-based	RNN	Supervised
Wang et al. [20]	Packet-based	LSTM+CNN	Supervised
Vinaya et al. [21]	Flow-based	CNN	Supervised
Kitsune [22]	Flow-based	AE	Unsupervised
Iliyasu As et al	Flow-based	GAN	Semi-supervised
Kim et al. [23]	Flow-based	RNN	Supervised
Tang et al. [24]	Packet-based	RNN	Supervised
Milad et al. [25]	Time-series	CNN	Supervised
Yong et al. [26]	Packet-based	CNN+LSTM	Supervised
Alqatf et al. [27]	Flow-based	Hybrid (AE+SVM)	supervised
Shone et al. [28]	Flow-based	AE	Unsupervised
Aldwairi et al. [29]	Packet-based	RBM	Unsupervised
Khan et al. **[30]**	Packet-based	Stacked AE	Unsupervised

IV. CONCLUSION

Network intrusion detection is an important task for cybersecurity. Recently, the Internet has seen great transformation with the emergence of technologies such as cloud computing and IoT, which increase the complexity of cyber-threat landscape. On the other hand, DL techniques perform effectively on complex dataset, hence the reason for their recent widespread adoption in intrusion detection system. Therefore, this paper surveys research works that employ DL methods for intrusion detection.

These paper gives an overview about DL techniques employed in intrusion detection to enable new researchers who wish to begin research in the field to be conversant with the state-of-the-art methods as well as unexplored areas.

REFERENCES

[1] J. Abbate, "the internet: global evolution and challenges," THE INTERNET, p. 9.

[2] A. Ku. Saxena, S. Sinha, and P. Shukla, "General study of intrusion detection system and survey of agent based intrusion detection system," in 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, May 2017, pp. 471–421. doi: 10.1109/CCAA.2017.8229866.

[3] K. A. Scarfone and P. M. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-94, 2007. doi: 10.6028/NIST.SP.800-94.

[4] K. Goeschel, "Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis," in SoutheastCon 2016, Norfolk, VA, USA, Mar. 2016, pp. 1–6. doi: 10.1109/SECON.2016.7506774.

[5] L. Dhanabal and D. S. P. Shantharajah, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms," vol. 4, no. 6, p. 7, 2015.

[6] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, May 2015, doi: 10.1038/nature14539.

[7] B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in 2016 8th IEEE International Conference on Communication Software and Networks (ICCSN), Beijing, China, Jun. 2016, pp. 581–585. doi: 10.1109/ICCSN.2016.7586590.

[8] I. Goodfellow, Y. Bengio, and A. Courville, Deep learning. Cambridge, Massachusetts: The MIT Press, 2016.

[9] A. B. Dieng, "Deep Probabilistic Graphical Modeling," p. 142.

[10] S. Albawi, T. A. Mohammed, and S. Al-Zawi, "Understanding of a convolutional neural network," in 2017 International Conference on Engineering and Technology (ICET), Antalya, Aug. 2017, pp. 1–6. doi: 10.1109/ ICEngTechnol.2017.8308186.

[11] A. Graves, "Generating Sequences With Recurrent Neural Networks," arXiv:1308.0850 [cs], Jun. 2014, Accessed: Apr. 09, 2022. [Online]. Available: http://arxiv.org/abs/1308.0850

[12] J. Hochst, L. Baumgartner, M. Hollick, and B. Freisleben, "Unsupervised Traffic Flow Classification Using a Neural Autoencoder," in 2017 IEEE 42nd Conference on Local

Computer Networks (LCN), Singapore, Oct. 2017, pp. 523–526. doi: 10.1109/LCN.2017.57.

[13] I. Goodfellow et al., "Generative Adversarial Nets," p. 9.

[14] Arash Habibi Lashkari, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," Sharafaldin, I., Lashkari, A.H. and Ghorbani, A.A., 2018, January. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In ICISSp (pp. 108-116)..

[15] A. S. Iliyasu and H. Deng, "Semi-Supervised Encrypted Traffic Classification With Deep Convolutional Generative Adversarial Networks," IEEE Access, vol. 8, pp. 118–126, 2020, doi: 10.1109/ACCESS.2019.2962106.

[16] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," presented at the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), New York City, United States, 2016. doi: 10.4108/eai.3-12-2015.2262516.

[17] S. S. Roy, A. Mallik, R. Gulati, M. S. Obaidat, and P. V. Krishna, "A Deep Learning Based Artificial Neural Network Approach for Intrusion Detection," in Mathematics and Computing, vol. 655, D. Giri, R. N. Mohapatra, H. Begehr, and M. S. Obaidat, Eds. Singapore: Springer Singapore, 2017, pp. 44–53. doi: 10.1007/978-981-10-4642-1_5.

[18] S. M. Kasongo and Y. Sun, "A Deep Learning Method With Filter Based Feature Engineering for Wireless Intrusion Detection System," IEEE Access, vol. 7, pp. 38597–38607, 2019, doi: 10.1109/ACCESS.2019.2905633.

[19] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," IEEE Access, vol. 5, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[20] W. Wang et al., "HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection," vol. 6, p. 15, 2018.

[21] R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Applying convolutional neural network for network intrusion detection," in 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, Sep. 2017, pp. 1222–1228. doi: 10.1109/ICACCI.2017.8126009.

[22] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," arXiv:1802.09089 [cs], May 2018, Accessed: Apr. 10, 2022. [Online]. Available: http://arxiv.org/abs/1802.09089

[23] J. Kim, J. Kim, H. L. Thi Thu, and H. Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection," in 2016 International Conference on Platform Technology and Service (PlatCon), Jeju, Feb. 2016, pp. 1–5. doi: 10.1109/PlatCon.2016.7456805.

[24] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks," in 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), Montreal, QC, Jun. 2018, pp. 202–206. doi: 10.1109/NETSOFT.2018.8460090.

[25] M. Nasr, A. Bahramali, and A. Houmansadr, "DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto Canada, Oct. 2018, pp. 1962–1976. doi: 10.1145/3243734.3243824.

[26] Y. Zhang, X. Chen, L. Jin, X. Wang, and D. Guo, "Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data," IEEE Access, vol. 7, pp. 37004–37016, 2019, doi: 10.1109/ACCESS.2019.2905041.

[27] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection," IEEE Access, vol. 6, pp. 52843–52856, 2018, doi: 10.1109/ACCESS. 2018.2869577.

[28] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," IEEE Trans. Emerg. Top. Comput. Intell., vol. 2, no. 1, pp. 41–50, Feb. 2018, doi: 10.1109/TETCI.2017.2772792.

[29] T. Aldwairi, D. Perera, and M. A. Novotny, "An evaluation of the performance of Restricted Boltzmann Machines as a model for anomaly network intrusion detection," Computer Networks, vol. 144, pp. 111–119, Oct. 2018, doi: 10.1016/j.comnet.2018.07.025.

[30] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "TSDL: A Two-Stage Deep Learning Model for Efficient Network Intrusion Detection," IEEE Access, vol. 7, pp. 30373–30385, 2019, doi: 10.1109/ACCESS.2019.2899721.