A Review of Mitigation of Attacks in IoT using Deep Learning Models

Adnan Ghumro[1,*], Aisha Kanwal Memon[1], Irfana Memon[1], Insaf Ali Simming[2]

[1]Department of Computer systems Engineering, QUEST, Nawabsah
[2]Department of Basic Sciences & Related Studies, QUEST, Nawabshah
[*]Corresponding author: adnanrasoolghumro12@gmail.com

Abstract

In current era, the proliferation of IoT devices has transformed our daily life to a new level and made our life easier. IoT devices have interconnected with each other for communing and sharing information to gateways or Access Points (APs) for further processing of data. However, this provides growth to cybersecurity and zero-day attacks in IoT networks. In this paper, we have reviewed the deep learning models and datasets which are used to detect malicious data in an IoT ecosystem. We have observed that the combination of Long Short-Term Memory (LSTM) and Convolution Neural Network (CNN), LSTM, and stacked auto-encoders have better accuracy and precision for detecting malicious packets in the IoT environment. Moreover, a detailed theoretical analysis of deep learning models and datasets is also performed. This review provides a pathway for the new researchers to conduct research in IoT security and privacy issues by making these findings as references.

Keywords—Deep learning, Datasets, Internet of Things, Intrusion Detection System, Security Attacks.

1 Introduction

The field of Internet of Things (IoT) has been progressing since a decade to revolutionize the world in a new technological paradigm. It has the ability to change the life of every human being in this world. IoT devices have capabilities to interconnect with each other and extract information from the environment to send data to gateways, sensors, or any other internet-enabled device [1]. Nowadays, IoT is used in a plethora of applications such as smart homes, smart vehicles, smart agriculture, smart cities, smart grids, healthcare, surveillance, and supply chain management [2][3]. It is predicted that by the end of 2020 more than 50 billion IoT devices will be connected through internet [4][5].

The miniaturization of sensors has increased the influx of internet-connected devices, but it has also given rise to security and privacy concerns in IoT and has made them vulnerable to plenty of security attacks [1][6]. IoT devices are fabricated with little resource and without having sufficient security measures [7][8]. Due to innate resources and computation limitations, traditional security mechanisms will not be suitable to fix security flaws. For efficient detection of security threats and zero-day attacks, Intrusion Detection System (IDS) along with anomaly-based detection methods play a vital role in developing secure IoT ecosystem [4][9].

In an IoT environment, devices generate huge amount of data continuously. The rapid growth of deep learning algorithms has made it possible to efficiently perform automated data analysis and create patterns from data to successfully predict the output of the system accordingly. After training on a large amount of data, a deep learning model can successfully detect known as well as unknown attacks with a good accuracy in real-time scenarios and send the acknowledgement to authorities. In this paper, we have reviewed the deep learning techniques which are used by the researchers to locate an anomaly in an IoT environment. The remaining paper is organized as follows. Section 2 delivers a detailed literature review. Section 3 provides a brief discussion of deep learning and its models used for attack detection. Section 4 presents the discussion and analysis of the techniques based on different datasets and parameters. section 5 mentions the research challenges for deep learning in an IoT ecosystem. In the last section, conclusion and future research direction for deep learning techniques in the context of IoT security are described.

ISSN: 2523-0379 (Online), ISSN: 1605-8607 (Print)

2 Literature Review

In IoT, there is a huge number of sensors used for sensing temperature, light, noise, speed, images, etc. All these sensors which are connected to other core networks of organizations, homes, cities, etc. pave the path for attackers to launch attacks in a network to steal the data, corrupt data and/or misuse it for several personal reasons. These attacks lead to the malfunctioning of the network. Therefore, the researchers have proposed several techniques using deep learning to mitigate suspicious activities in the network.

In [10], authors proposed network-based detection of IoT botnet attacks using deep auto-encoder. The dataset is developed by capturing real-time data from nine IoT devices to train a deep network to predict the anomaly in the network. Deep auto-encoder has obtained satisfactory results as compared to Support Vector Machine (SVM), Local Outlier Factor (LOF), and Isolation Forest. Nearly 100% True Positive Rate (TPR) and a False Positive Rate (FPR) between 0.007 to 0.01 has been reported. An attack is detectable within 174 to 212 ms. Mirai, Bashlite and their variants are detected in this proposed scheme. Therefore, the TPR slightly declines on devices which have multiple functionalities to perform and generate more data as compared to normal IoT device.

In [11], authors proposed a deep learning technique using stacked auto-encoders for attack detection in Fog-to-Things. This deep learning model achieved satisfactory results using the NSL-KDD dataset as compared to the shallow learning algorithm. The accuracy, detection rate, and False Alarm Rate (FAR) are reported to be 99.20, 99.27, and 0.85%, respectively. The NSL-KDD dataset is an improved version of KDD'99, but it still consists of several deficiencies and may not be a better representation of real networks [12].

In [13], authors proposed a dense random neural network mechanism to detect an attack in IoT domain based on binary classification. The model is trained using real-time captured traffic over a week from IoT devices such as a smoke sensor, PIR motion detector, magnetic door opening detector, blood pressure meter, etc. Moreover, attacks are generated in the network using a python written script to train the model on both malicious and benign data to detect the anomaly in the network. Deep Recurrent Neural Network (RNN) extract the features from data and successfully predict attacks from a series of new observations. The results can be compared with a simple threshold detector as well.

In this study [14], authors have proposed a LSTM based attack detection method by using two datasets which are constructed using network traces known as ISCX and public devices like mobile phone, smart TV, etc. using WIFI APs known as AWID dataset. The performance of both datasets under LSTM superseded the traditional Logistic Regression (LR) algorithm and the accuracy of LSTM was nearly 99%, but LR failed to get past 90%.

In another research [15], authors used the UNSW-NB15 dataset having 45 features to train LSTM to predict the attacks in the network. The performance of the dataset is satisfactory as it provides 95% accuracy and has 2.19 ms detection time.

In [16], authors proposed a BI-LSTM deep learning model to detect botnet attacks in IoT. A word Embedding is used for text recognition and conversion of attack packets into a tokenized integer format. The dataset for models was built from the data traffic of Siri camera for 2 hours under a secure sandbox environment to ensure normal conditions. Moreover, BI-LSTM is compared with LSTM in terms of accuracy and loss for several attacks. The performance of both models is good with high accuracy and low loss in Mirai, UDP, and DNS. Nevertheless, the performance of both models declines while detecting *ack* attacks.

In [17], the authors proposed an IDS for mitigation of attacks using Restricted Boltzmann Machine (RBM), Deep Belief Network (DBN), and a combination of DBN and LR using KDDCUP99 dataset to train the model for predicting malicious activity in the network. The validation accuracy of models was 92%, 95% and 97.9% for RBM, DBN2, and DBN4+RBM, respectively. Moreover, KDDCUP99 lacks in performance due to the duplicate data and a lack of emerging attacks.

In [18], the Deep Neural Network (DNN) based scheme is proposed for attack classification in the IoT domain. The model performance is examined using three datasets, i.e., UNSW-NB15, CIDDS-001, and GPRS by accessing three validation methods such as sub-sampling, cross-validation, and repeated cross-validation. The model depicts almost the same performance under CIDDS-001 and UNSW-NB-15 dataset with approximately 96% accuracy, recall, and precision. However, the performance of the model under GPRS dataset is around 80% which, as compared to the other two da-tasets, is not satisfactory.

In [19], the proposed scheme is used to mitigate malicious activity in the Industrial Internet of Things (IIoT). The authors have used a deep auto-encoder and a Deep Feed-forward Neural Network (DFNN) to detect the attacks using two novel datasets NSL-KDD and UNSW-NB15. The models show better performance using NSL-KDD with 99% of malicious

detection rate, and 1.8% of False Positive Rate (FPR). UNSW-NB15 obtained a detection rate of 93% with 8.2% FPR. Moreover, the proposed model performance was compared with eight machine learning algorithms and was demonstrated to have superior performance. In [20], RNN, LSTM, CNN, and CNN+LSTM models were trained on CICIDS2017 dataset to measure the effectiveness of these models. In addition, these models were also compared with the known machine learning algorithms which are used for anomaly detection. It was shown that CNN+LSTM obtained the highest accuracy of 97.16%. However, the model did not have a satisfactory performance for unbalanced dataset.

In [21], the authors proposed a scheme based on Deep Neural Networks (DNNs) to detect several attacks in IoT networks. However, the results of the scheme were observed using simulation as well as a DL testbed to ensure the efficacy of the proposed scheme. In addition, the performance of the model was compared with an Inverse Weight Clustering (IWC) technique. It was shown that the results of DL techniques outperformed the IWC with 95% precision and 97% recall for various attacks.

In [22], the proposed scheme used a distributed deep model with the NSL-KDD dataset to examine the performance of the model for malicious networks. The distributed model had better results with 99.20% accuracy and 0.85% FAR as compared to the centralized shallow model.

In [23], the proposed scheme is capable of detecting attacks in IoT and 5G networks. The autoen-coder Deep Neural Network (DNN) model is used to classify benign and malicious traffic in the network domain. The AWID dataset is used for training the model to detect several attacks. It was shown that the model can efficiently detect malicious traffic with 99.9% accuracy.

In this section, we have discussed promising deep learning techniques used for detecting several security attacks in real-time using supervised learning and unsupervised learning. Moreover, the dynamic range of security datasets are used to examine the performance of models under vulnerable conditions to check the effectiveness in terms of accuracy, precision, detection rate, and recall. Table 1 summarizes the information about deep learning techniques, datasets, attacks that are detected, development level of the model, feature selection, performance metrics, and comparison with other techniques of each deep learning method studied in the literature.

3 Deep Learning Models for Attack Detection

Deep learning based on multi-layered neural networks is a statistical approach for modeling, classifying, and recognizing complex data such as speech, text, and image patterns [24][25]. Each layer in a deep learning model contains some neurons with activation functions that can be operated to produce non-linear outputs as shown in Figure 1. This methodology is said to be inspired by the neuron structure of the human brain [26]. Due to automatic feature engineering, pre-training, and compression capabilities, deep learning has enhanced its recognition. These features make the usability of deep learning feasible in network with limited resources. Moreover, Deep learning has been broadly implemented because of its self-learning capability, potential to produce highly accurate results, and faster processing time. Also, deep learning has been proven effective in security attack detection [27]. Three learning models are used: supervised learning, unsupervised learning, and semi-supervised learning. Some supervised and unsupervised learning techniques which have been used by researchers to detect abnormalities in an IoT network are mentioned in Figure 2.

3.1 Supervised Learning

Supervised learning is a type of deep learning model which is only applicable when the labels of training data are given [28]. Supervised learning tasks can be represented in terms of (X, Y) pairs, where X is a random input variable, and Y is a label which is used to predict the given X [29]. Some common supervised tasks comprise classification and regression [30]. The supervised learning technique is implemented with a number of deep learning models such as CNN, RNN, LSTM, and BI-LSTM, CNN which are suitable for the image and video related data. Whereas, some other models such as RNN, LSTM, and BI-LSTM are widely used with time series or sequential data.

3.2 Unsupervised Learning

Unsupervised learning is used to extract hidden patterns from unlabeled training data [31]. Some common unsupervised tasks include clustering, outlier detection, novelty detection, dimensionality reduction, fraud detection, data compression, trend detection, and network security [28][30]. The unsupervised learning model is concerned with various techniques to include AE, RBM, and DBM.

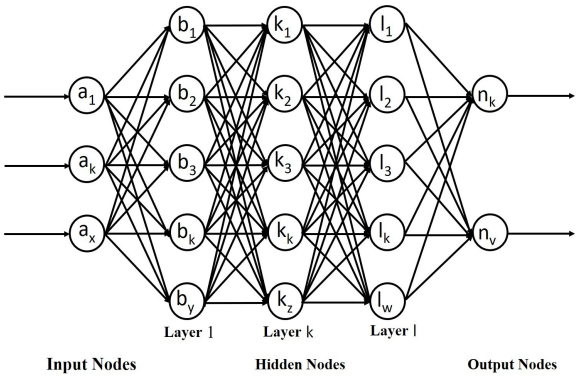

Fig. 1: Deep Neural Network

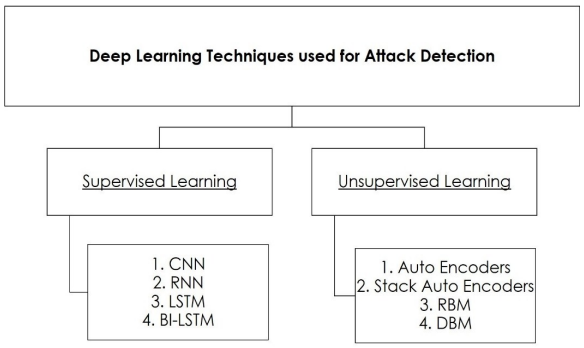

Fig. 2: Classification of deep learning techniques used in the mitigation of attacks

3.3 Semi-Supervised Learning

Semi-supervised learning is concerned with the study of how computers and humans learn in the presence of both labeled and unlabeled data. Conventionally, learning has been studied in the unsupervised paradigm where all the data is unlabeled, or in the supervised paradigm where all the data is labeled. The purpose of semi-supervised learning is to understand how combining labeled and unlabeled data may alter the learning behavior [30]. Nowadays, an astronomical amount of unlabeled data is generated over internet which requires manual analysis and labelling. Therefore, semi-supervised learning improves the performance of a network using labelled and unlabeled data for training [32][33].

4 Discussion & Results

We have performed a rigorous analysis of a variety of attack detection models in the IoT environment for multiple datasets. We also analyzed the performance of the deep learning models used to classify traffic between normal and malicious packets in the IoT ecosystem. According to our analysis, the dataset named NSL-KDD, ISCX, AWID, KDDCUP99, CIDDS-OO1, and GPRS are not complete representation of real-time IoT devices traffic [12][14][23]. Therefore, training deep learning models using these datasets may get high accuracy and detection rate. However, the performance will deteriorate once implemented in real scenarios for the detection of attacks because of the complex nature of traffic as well as the emergence of new attacks in networks. On the other hand, few researchers have constructed their datasets by setting IoT environments to capture and analyze packets using network analyzer software such as Wireshark, Scapy, and Bro IDS [10][14][16][21]. The datasets developed from real-time traffic were collected by only those devices that have fewer features, so that the dataset must be developed from really complex IoT devices as well as with a wide variety of IoT attacks to enhance the detection rate of the models and lower the value of FAR [10][16]. CICIDS2017 and UNBW-NB15 are the two datasets that almost cover the requirement of a real-time IoT environment with 45 and 80 features, respectively with a capability of covering wider range of security attacks [34][35]. Moreover, authors have used a wide range of deep learning models to detect malicious traffic in IoT networks. However, the effective performance of the model completely depends upon the nature of data used to train the Deep Neural Network (DNN) [33]. According to our analysis, the best suitable models for detecting anomalous data in a network with high detection rate and lower FAR are LSTM+CNN, LSTM, and stacked deep auto-encoder respectively by using CICIDS2017 and UNBW-NB15 datasets.

5 Research Challenges for Deep Learning in the IoT Ecosystem

The recent advancements in technology have resulted in the development of various learning approaches such as machine learning and deep learning for detecting security threats and zero-day attacks in the IoT ecosystem. However, several challenges need to be addressed which are explained in the following sections.

5.1 Datasets Related to Security

The major challenge which needs to be coped while using machine learning and deep learning approaches is related to the generation and extraction of high quality and realistic data which contains several possible attacks. A potential direction for the researchers is to create datasets with all possible IoT attacks to enrich the training of a model to set a new benchmark for getting high accuracy and precision. Due to the large

Technique	Dataset	Attacks	Development Level	Feature Selection	Performance Matrics	Comparison
Deep auto-encoder [10]	Real-time (9 IoT Devices)	Bashlite, Mirai	Network	Yes	TPR, FPR, Average Detection Time	Isolation Forest, LOF, SVM
Stacked auto-encoders [11]	NSL-KDD	DOS, R2L, U2R, Probing	___	Yes	Accuracy, DR, FAR	Shallow Model
RNN [13]	Real-time (IoT Devices)	UDP flood, TCP SYN, Sleep Deprivation Attack, Barrage Attack, Broadcast Attack	IoT Gateway	No	Probability of Detection Time	Simple Threshold Detector
LSTM [14]	AWID, ISCX	Authentication, ARP Flooding, Injection, Probe Request, Infiltrating, HTTP DoS, DDoS using IRC Botnet, SSH Brute Force	___	Yes	Accuracy, Recall, Precision	Logistic Regression
Bi-Directional LSTM [15]	UNSW-NB15	Backdoor, DoS, Exploits, Fizzers, Generic, Port Scans, Reconnaissance, Shellcode, Spam, Worms	___	Yes	Accuracy, Miscalculation rate, FPR, Precision, Recall, F1-score	___
Bi-Directional LSTM [16]	A Secure Sandbox Environment (IoT Devices)	Mirai, UDP, ACK, DNS, Multi-vector (with Ack), Multi-vector (without Ack), Multi-vector (with 3 Ack)	___	No	Accuracy, Loss	LSTM
DBN4+LR [17]	KDDCUP'99	DoS, Probe, R2L, U2R	___	Yes	Accuracy, FN	RBM, DBM2
DNN [18]	UNSW-NB15, CIDDS001, GPRS	Backdoor, DoS, Exploits, Fizzers, Generic, Port Scans, Reconnaissance, Shellcode, Spam, Worms, SSH Brute Force	___	___	Accuracy, Precision, Recall, FPR	Comparison of Datasets
Deep auto-encoder, Deep Feed-Forward Neural Network [19]	NSL-KDD, UNSW-NB15	Backdoor, DoS, Exploits, Fizzers, Generic, Port Scans, Reconnaissance, Shellcode, Spam, Worms, Probe, R2, U2R	___	Yes	Accuracy, Detection Rate, FPR	Comparison with ML Algorithm
MLP, LSTM, CNN, LSTM+CNN [20]	CICIDS2017	DDoS	___	___	Accuracy, Precision, Recall	Comparison with ML Algorithm
DNN [21]	Real Network, Simulation	Blackhole, Opportunistic Service, DDoS, Sinkhole, Wormhole	___	Yes	Precision, Recall, F1	IWC
Deep Model [22]	NSL-KDD	DoS, Probe, R2L, U2R	___	___	Accuracy, DR, FAR	Shallow Model
auto-encoder DNN [23]	AWID	Flooding, Injection, Impersonation	___	___	Accuracy	Comaprison ML Algorithm

TABLE 1: Comparison of various deep learning techniques used for attack

technical diversity of various IoT devices, continuously updating a dataset with new attacks is a challenging task.

5.2 Low-Quality Data

IoT devices are deployed in a huge number of applications. the tiny size of IoT devices innated with low memory, power, and computation capabilities affects the quality of data. Consequently, learning to secure the IoT ecosystem requires an algorithm that has capabilities to deal with low quality and noisy data. Therefore, robust machine learning and deep learning algorithms need to be designed which should be capable of dealing with noisy heterogeneous data from several IoT devices.

5.3 Lifelong Learning of IoT Attacks

IoT network is comprised of a dynamic system in which devices are either added or removed thoroughly depending on the application with evolving needs. Because of their dynamic nature, differentiating between benign and malicious data cannot be predefined which emerges as a dedicated challenge. For solving this issue, security model updates are required for understanding and tracking system changes. Consequently, for long-term applications, lifelong learning will be incorporated to construct a model that can perform retaining processes repeatedly for finding new emerging patterns depending on network behavior and adapt to the changes accordingly.

6 Conclusion & Future Directions

In this paper, we have analyzed the performance of various deep learning models trained on different datasets to detect the attacks in IoT network. The performance of deep learning models depends on the training phase, therefore, the better the network is trained, the better the results in terms of accuracy and FAR. The dataset used in the neural network helps the model to learn and find new patterns in the training phase to predict the anomalies in the network. LSTM+CNN, LSTM, and stacked deep autoencoder give high accuracy and low FAR by using CICIDS2017 and UNBW-NB15 datasets because they somehow reflect real traffic and consist of a variety of attacks.

In future, we will construct a robust and diverse set of datasets which contain packets from simple to multi-functional IoT devices to reflect a real IoT environment. Afterwards, the dataset will be used to train several deep learning models to examine their performance under compromised scenarios to set a new benchmark in this domain.

References

[1] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E. and Markakis, E.K. “A Survey on the Internet of Things (IoT) Forensics: Challenges, Approach-es and Open Issues.” IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp.1191-1221,2020.

[2] Lee, I. and Lee, K. “The Internet of Things (IoT): Applications, investments, and challenges for enterprises.” Business Horizons, vol. 58, no. 4, pp.431-440,2015.

[3] Shin, H., Lee, H.K., Cha, H.Y., Heo, S.W. and Kim, H. “IoT security issues and light weight block cipher.” In 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), pp. 381-384,2019.

[4] Al-Garadi, M.A., Mohamed, A., Al-Ali, A., Du, X., Ali, I. and Guizani, M. “A survey of machine and deep learning methods for internet of things (IoT) security.” IEEE Communications Surveys & Tutorials,2020.

[5] Mekki, K., Bajic, E., Chaxel, F. and Meyer, F. “A comparative study of LPWAN technologies for large-scale IoT deployment. ICT Express.” Press. [Google Scholar], vol. 5, no. 1, pp. 1–7, 2019.

[6] Tawalbeh, L.A., Muheidat, F., Tawalbeh, M. and Quwaider, M. “IoT Privacy and Security: Challenges and Solutions.” Applied Sciences, vol. 10, no. 12, p. 4102, 2020.

[7] Atlam, H.F. and Wills, G. “IoT security, privacy, safety and ethics.” In Digital Twin Technologies and Smart Cit-ies, pp. 123-149, 2020.

[8] Abdul-Ghani, H.A., Konstantas, D. and Mahyoub, M. “A comprehensive IoT attacks survey based on a building-blocked reference model.” IJACSA) International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, pp. 355–373, 2018.

[9] Lu, Y. and Da Xu, L. “Internet of things (iot) cybersecurity research: A review of current research topics.” IEEE Internet of Things Journal, vol. 6, no. 2, pp.2103-2115, 2019.

[10] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shab-tai, A., Breitenbacher, D. and Elovici, Y. “N-baiot—network-based detection of iot botnet attacks using deep auto-encoders.” IEEE Pervasive Computing, vol. 17, no.3, pp.12-22, 2018.

[11] Abeshu, A. and Chilamkurti, N.“Deep learning: the frontier for distributed attack detection in fog-to-things computing.” IEEE Communications Magazine, vol. 56, no. 2, pp.169-175, 2018.

[12] Tavallaee, M., Bagheri, E., Lu, W. and Ghorbani, A.A. “A detailed analysis of the KDD CUP 99 data set.” In 2009 IEEE symposium on computational intelligence for security and defense applications, pp. 1-6, 2009.

[13] Brun, O., Yin, Y., Gelenbe, E., Kadioglu, Y.M., Augusto-Gonzalez, J. and Ramos, M. “Deep learning with dense random neural networks for detecting attacks against iot-connected home environments.” In International ISCIS Security Workshop, pp. 79-89, 2018.

[14] Diro, A. and Chilamkurti, N. “Leveraging LSTM networks for attack detection in fog-to-things communications.” IEEE Communications Magazine,vol. 56, no. 9, pp.124-130, 2018.

[15] Roy, B. and Cheung, H. “A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural net-work.” In 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), pp. 1-6, 2019.

[16] McDermott, C.D., Majdani, F. and Petrovski, A.V. “Botnet detection in the internet of things using deep learning

approaches". In 2018 international joint conference on neural networks (IJCNN), pp. 1-8, 2018.

[17] Alrawashdeh, K. and Purdy, C. "Toward an online anomaly intrusion detection system based on deep learning." In 2016 15th IEEE international conference on machine learning and applications (ICMLA), pp. 195-200, 2016.

[18] Tama, B.A. and Rhee, K.H. "Attack classification analy-sis of IoT network via deep learning approach." Res. Briefs Inf. Commun. Technol. Evol.(ReBICTE), vol. 3, pp.1-9, 2017.

[19] Muna, A.H., Moustafa, N. and Sitnikova, E. "Identification of malicious activities in industrial internet of things based on deep learning models." Journal of Information Security and Applications, vol. 41, pp. 1–11, 2018.

[20] Roopak, M., Tian, G.Y. and Chambers, J. "Deep learning models for cyber security in IoT networks." In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 452-457, 2019.

[21] Thamilarasu, G. and Chawla, S. "Towards deep-learning-driven intrusion detection for the internet of things." Sensors, vol. 19, no. 9. p.1977, 2019.

[22] Diro, A.A. and Chilamkurti, N. "Distributed attack detection scheme using deep learning approach for Internet of Things." Future Generation Computer Systems, vol. 82, pp.761-768, 2018.

[23] Rezvy, S., Luo, Y., Petridis, M., Lasebae, A. and Zebin, T. "An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks." In 2019 53rd Annual Conference on Information Sciences and Systems (CISS), pp. 1-6, 2019.

[24] Qingchen, Z., Laurence, T.Y., Zhikui, C. and Peng, L. "A survey on deep learning for big data." Information Fusion, vol. 42, pp.146-157,2018.

[25] Marcus, G. "Deep learning: A critical appraisal". arXiv preprint arXiv:1801.00631,2018.

[26] Zhou, Y., Han, M., Liu, L., He, J.S. and Wang, Y. "Deep learning approach for cyberattack detection." In IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 262-267,2018.

[27] Amanullah, M.A., Habeeb, R.A.A., Nasaruddin, F.H., Gani, A., Ahmed, E., Nainar, A.S.M., Akim, N.M. and Imran, M. "Deep learning and big data technologies for IoT security." Computer Communications, vol. 151, pp.495-517,2020.

[28] Gupta, R., Tanwar, S., Tyagi, S. and Kumar, N. "Machine learning models for secure data analytics: A taxonomy and threat model." Computer Communications, vol. 153, pp.406-440,2020.

[29] Bengio, Y. "Deep learning of representations for unsupervised and transfer learning." In Proceedings of ICML workshop on unsupervised and transfer learning, pp. 17-36, 2012.

[30] Zhu, X. and Goldberg, A.B. "Introduction to semi-supervised learning." Synthesis lectures on artificial intelligence and machine learning, vol. 3, no. 1, pp.1-130,2009.

[31] Love, B.C. "Comparing supervised and unsupervised category learning." Psychonomic bulletin & review, vol. 9, no. 4, pp.829-835, 2002.

[32] Oliver, A., Odena, A., Raffel, C., Cubuk, E.D. and Goodfellow, I.J. "Realistic evaluation of semi-supervised learning algorithms.", pp. 3235–3246, 2018.

[33] Siddiqi, A."Adversarial security attacks and perturba-tions on machine learning and deep learning methods." arXiv preprint arXiv:1907.07291,2019.

[34] Moustafa, N. and Slay, J. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." In 2015 military com-munications and information systems conference (MilCIS), pp. 1-6, 2015.

[35] Sharafaldin, I., Lashkari, A.H. and Ghorbani, A.A. "A detailed analysis of the cicids2017 data set." In International Conference on Information Systems Security and Privacy, pp. 172-188, 2018.