Discovery

Moderation of cyber attacks in IoTs using deep learning techniques

Ifeanyi Stanly Nwokoro[1], **Shafi'I M Abdulhamid**[2], **Kwaku Zacciah Adom-Oduro**[3], **Anayo Chukwu Ikegwu**[4], **Augustina Nebechi Nwatu**[5]

To Cite:
Nwokoro IS, Abdulhamid SM, Adom-Oduro KZ, Ikegwu AC, Nwatu AN. Moderation of cyber attacks in IoTs using deep learning techniques. *Discovery* 2025; 61: e7d1519
doi: https://doi.org/10.54905/disssi.v61i337.e7d1519

Author Affiliation:
[1]Department of Computer Science, Rhema University, Nigeria
[2]Department of Cyber Security, National Open University of Nigeria
[3]Department of Computer Science, Technical University, Ghana
[4]Department of Software Engineering, Veritas University, Nigeria
[5]Department of Biotechnology, Alex Ekwueme Federal University (AE-FUNAI), Nigeria

Peer-Review History
Received: 04 October 2024
Reviewed & Revised: 08/October/2024 to 23/January/2025
Accepted: 27 January 2025
Published: 31 January 2025

Peer-Review Model
External peer-review was done through double-blind method.

Discovery
pISSN 2278–5469; eISSN 2278–5450

DISCOVERY
SCIENTIFIC SOCIETY

ABSTRACT

The widespread use of IoT devices in the modern day has simplified our lives and elevated our everyday routines to a new level. IoT devices are connected to communicate and share data with gateways or access points (APs) for additional data processing. On the other hand, this makes cybersecurity and zero-day assaults in IoT networks more prevalent. Deep learning models and datasets used to identify fraudulent data in IoT environments have been reviewed in this research. In the context of the Internet of Things, we found that the Long Short-Term Memory (LSTM), Convolution Neural Network (CNN) and stacking auto-encoders improve the accuracy and precision of malicious packet detection. We undertook a thorough theoretical examination of deep learning datasets and models. Our research finding serves as paradigm to researchers as a technique to investigate IoT security and privacy challenges.

Keywords: Internet of Things (IOTs); Access Points (APs); Long Short-Term Memory (LSTM); Convolution Neural Network (CNN); Deep Learning.

1. INTRODUCTION

Over the past ten years, the Internet of Things (IoT) has advanced to transform the world using a new technology paradigm. It has the power to transform the lives of all people on the planet. IoT devices can communicate with one another and gather data from their surroundings to transmit to gateways, sensors, or any other device with internet access (Stoyanova et al., 2020). Smart homes, smart cars, smart grids, smart cities, smart agriculture, health care, surveillance, and supply chain management are just a few of the many uses for IoT today (Lee and Lee, 2015; Shin et al., 2019). Over 50 billion Internet of Things devices are expected to be online by the end of 2024 (Al-Garadi et al., 2020; Mekki et al., 2019). The proliferation of internet-connected devices has been supported by sensor downsizing, still, it has also raised privacy and security issues with the Internet of Things and left them open to numerous security breaches (Stoyanova et al., 2020; Tawalbeh et al., 2020).

IoT devices lack adequate security safeguards and are manufactured with few resources (Atlam and Wills, 2020; Abdul-Ghani et al., 2018). Traditional security procedures are inappropriate for addressing security issues because of inherent resources and computational limits. Developing a secure IoT ecosystem requires using intrusion detection systems (IDS) in conjunction with anomaly-based detection techniques to effectively identify security risks and zero-day attacks (Al-Garadi et al., 2020; Lu and Da, 2019). Devices in an IoT context continuously produce enormous amounts of data. Deep learning algorithms are used to carry out automated data analysis effectively to identify patterns in data which helps to forecast the output from experimentation accurately. A deep learning model trained on a lot of data may effectively identify known and unknown assaults in real-time scenarios with a high degree of accuracy and notify the appropriate authorities. Deep learning methods that researchers employ to find an anomaly in an IoT context are reviewed in this paper.

2. LITERATURE REVIEW

Numerous sensors are utilized on the Internet of Things to measure temperature, light, noise, speed, and pictures. All these sensors are linked to other central networks in homes, businesses, cities, etc., creating opportunities for hackers to enter a network and steal, alter, or otherwise abuse data for various private purposes. Systems networks malfunction because of these attacks. As a result, researchers have put forth several deep learning-based strategies to reduce questionable network activity. Meidan et al., (2018) suggested employing a deep auto-encoder for network-based IoT botnet attack detection. The dataset is created by gathering real-time data from nine Internet of Things devices to train a deep network to anticipate network anomalies.

Compared to the Isolation Forest, Local Outlier Factor (LOF), and Support Vector Machine (SVM), the Deep auto-encoder has produced satisfactory results. There have been reports of a False Positive Rate (FPR) ranging from 0.007 to 0.01 and a nearly 100% True Positive Rate (TPR). An attack can be identified within 174-212 m/s and can detect Mirai, Bashlite, and their variants. As a result, the TPR slightly decreases on devices with multiple functionalities to perform and generate more data compared to a typical IoT device. In Abeshu and Chilamkurti, (2018), authors proposed a deep learning technique using stacked auto-encoders for attack detection in fog-to-things.

Compared to the shallow learning algorithm, this deep learning model achieved satisfactory results using the NSL-KDD dataset, with accuracy, detection rate, and False Alarm Rate (FAR) reported to be 99.20, 99.27, and 0.85%, respectively. The NSL-KDD dataset is an improved version of the KDD-99 system, but it still has several flaws and might not be a better representation of real-time networks (Tavallaee et al., 2009). A dense random neural network approach based on binary classification is proposed by authors Brun et al., (2018) to identify an attack in the IoT area. Real-time traffic recorded over a week from the Internet of Things devices, including blood pressure meters, smoke sensors, PIR motion detectors, and magnetic door opening detectors, is used to train the model.

Additionally, a Python script is utilized in creating assaults on networks for the training of models on both benign and malicious data to identify network anomalies. Deep Recurrent Neural Networks (RNNs) can correctly forecast attacks and extract features from data. It is also possible to compare the outcomes by using a basic threshold detector. The authors of this article Diro and Chilamkurti, (2018a) have suggested an LSTM-based attack detection technique employing two datasets: The AWID dataset, which is built by the usage of public devices like smartphones, smart TVs, WiFi APs, etc., and the ISCX dataset, that is built by the usage of network traces. Both datasets performed better under LSTM than under the conventional Logistic Regression (LR) technique. The LSTM's accuracy was close to 99% while that of LR's was below 90%.

In a different study Roy and Cheung, (2019), the authors trained LSTM to anticipate network attacks using the UNSW-NB15 dataset, which contains 45 features with a detection time of 2.19 m/s and 95% accuracy, the dataset's performance gives a satisfactory outlook. BI-LSTM deep learning model was used by authors McDermott et al., (2018) to identify botnet assaults on the Internet of Things. Attack packets were converted into a tokenized integer format, and text recognition was accomplished using word embedding. To guarantee normal conditions, the dataset for the models was constructed using the Siri camera's data traffic for two hours in a secure sandbox environment. BI-LSTM and LSTM are compared regarding accuracy and loss for a few attacks. Both models work well in Miria, UDP, and DNS, with great accuracy and minimal loss.

However, both models' performance deteriorates when ACK attacks are detected. Using the KDDCUP-99 dataset to train the model for predicting malicious activity in a network, Alrawashdeh and Purdy, (2016) proposed an intrusion detection system (IDS) for attack mitigation that makes use of Restricted Boltzmann Machines (RBM), Deep Belief Networks (DBN), and a combination of DBN and LR.

The models' respective validation accuracy was 92%, 95%, and 97.9% for RBM, DBN2, and DBN4+RBM. Furthermore, KDDCUP-99 performs poorly because of redundant data and a dearth of new attacks. In Tama and Rhee, (2017), the Deep Neural Network (DNN) based scheme was proposed for attack classification in the IoT domain.

Three datasets, namely UNSW-NB15, CIDDS-001, and GPRSS were used to assess the model's performance using three validation techniques: Subsampling, cross-validation, and repeated cross-validation. The model exhibits nearly identical performance with roughly 96% accuracy, recall, and precision under the CIDDS-001 and UNSW-NB-15 datasets. Nevertheless, the model's performance on the GPRSS dataset is only about 80%, which is subpar compared to the other two datasets. In Muna et al., (2018), the proposed scheme mitigates malicious activity in the Industrial Internet of Things (IIoT). The authors employed a Deep Feed-forward Neural Network (DFNN) and a deep auto-encoder to detect the attacks using two novel datasets, UNSW-KDD and UNSW-NB15.

The models performed better with NSL-KDD, achieving a 99% malicious detection rate and 1.8% FPR, while UNSW-NB15 achieved a 93% detection rate with 8.2% FPR. The performance of the proposed model was compared with eight machine learning algorithms, and it has superior performance. In Roopak et al., (2019), RNN, LSTM, CNN, and CNN+LSTM models were trained on the CICIDS2017 dataset to assess their efficacy, and these models were also compared with the known machine learning algorithms used for anomaly detection and an accuracy of 97.16% was demonstrated by CNN+LSTM. Nevertheless, the model's performance was unsatisfactory for datasets that were not balanced.

Thamilarasu and Chawla, (2019) proposed a Deep Neural Network (DNN)-based method for identifying various IoT network assaults. To guarantee the effectiveness of the suggested plan, however, the outcomes were observed by simulation and a DL testbed. Furthermore, the Inverse Weight Clustering (IWC) method compared the model's performance. For various attacks, the DL methods performed better than the IWC with 95% precision and 97% recall. The proposed method in Diro and Chilamkurti, (2018b) examined the model's performance for harmful networks using a distributed deep model with the NSL-KDD dataset. It is observed that with a 99.20% accuracy rate and a 0.85% FAR, the distributed model outperformed the centralized shallow model during the comparative analysis. The proposed method in Rezvy et al., (2019) can identify assaults in 5G and IoT networks.

In the network domain, benign and malicious traffic is characterized by using the autoencoder Deep Neural Network (DNN) model. The DNN model is trained using the AWID dataset to identify multiple attacks. It was established that the model had a 99.9% accuracy rate in detecting malicious communications. This section has covered promising deep learning methods that utilize supervised and unsupervised learning to detect various security threats in real time. Additionally, the usefulness of models in terms of accuracy, precision, detection rate, and recall is checked by analyzing their performance under susceptible conditions using the dynamic range of security datasets. Table 1 lists the details of each deep learning method examined in the literature, including datasets, attacks detected, model development stage, feature selection, performance metrics, and comparison with other methods.

Deep Learning Models for Identifying Attacks

Statistical method for modeling, categorizing, and identifying complex data, including speech, text, and image patterns, is deep learning based on multi-layered neural network protocols (Qingchen et al., 2018; Marcus, 2018). As seen in Figure 1, each layer of a deep learning model has a few neurons with activation functions that are used to generate non-linear outputs. The structure of neurons in the human brain is cited as the inspiration for this methodology (Zhou et al., 2018). Deep learning has improved recognition because of its autonomous features: engineering, pre-training, and compression capabilities.

These characteristics enable deep learning in networks with constrained resources. Furthermore, deep learning has been widely employed due to its faster processing time, self-learning capability, and potential for highly accurate outputs. Deep learning has also been successful in detecting security attacks (Amanullah et al., 2020). Supervised learning, unsupervised learning, and semi-supervised learning are the three learning models that are employed. Figure 2 lists a few supervised and unsupervised learning strategies researchers have used to find anomalies in an IoT network.

Supervised Learning Technique

A deep learning model known as supervised learning only works when training data labels are provided (Gupta et al., 2020). (X, P) pairs, in which X is a random input variable, and P is a label used to forecast the given X, can be used to describe supervised learning tasks (Bengio, 2012). Regression and classification are two examples of typical supervised tasks (Zhu and Goldberg, 2009). Several deep learning models, including CNN, RNN, LSTM, and BI-LSTM, are used to perform the supervised learning technique and are appropriate for data about images and videos. However, alternative models like RNN, LSTM, and BI-LSTM are frequently used for sequential or time series data.

Unsupervised Learning Technique

Hidden patterns are extracted from unlabeled training data via unsupervised learning (Zhu and Goldberg, 2009). Clustering, outlier detection, novelty discovery, dimensionality reduction, fraud detection, data compression, trend detection, and network security are some everyday unsupervised tasks (Gupta et al., 2020; Zhu and Goldberg, 2009). The unsupervised learning model considers a few methods, such as AE, RBM, and DBM.

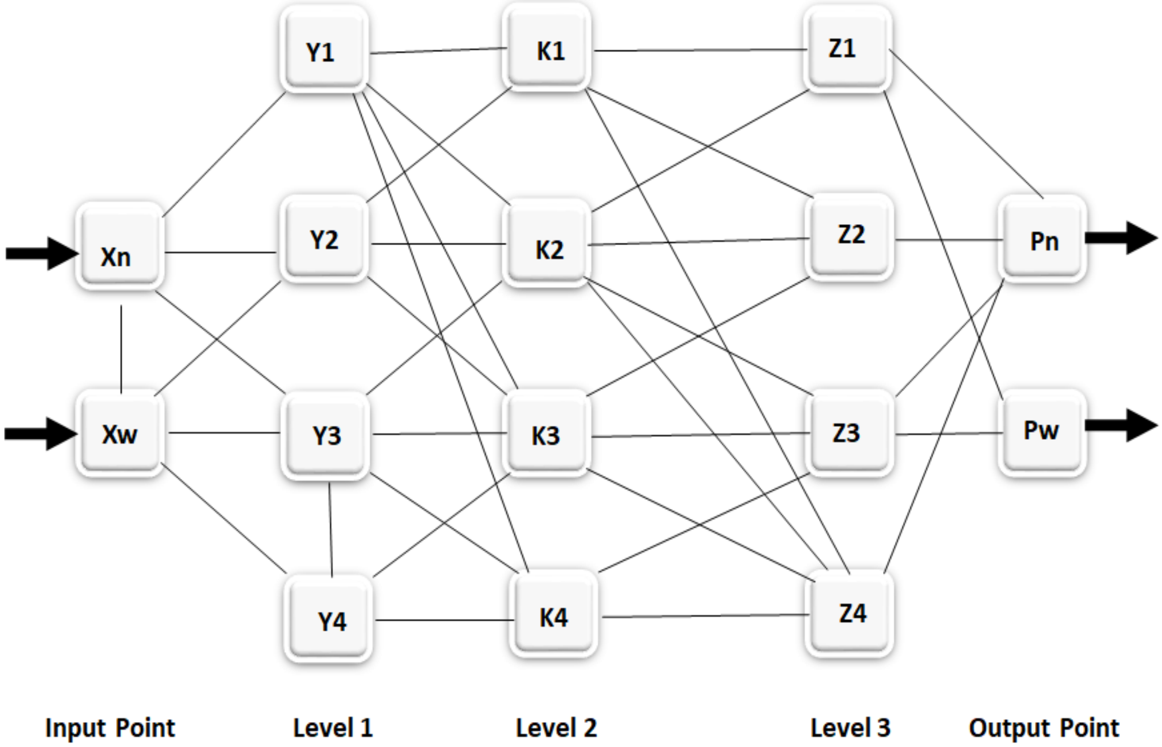

Figure 1 Deep Neural Network

Semi-Supervised Learning Technique

The study of how humans and computers learn when presented with both labeled and unlabeled material is known as semi-supervised learning. Learning has typically been examined in one of two paradigms: Unsupervised, in which all data is unlabeled, or supervised, in which all data is labeled for identification. Understanding how combining labeled and unlabeled input may change learning behavior is the aim of semi-supervised learning (Zhu and Goldberg, 2009). These days, the internet generates an enormous volume of unlabeled data that needs to be manually analyzed and labeled. Thus, employing labeled and unlabeled input for training, and semi-supervised learning enhances the network's performance (Oliver et al., 2018; Siddiqi, 2019).

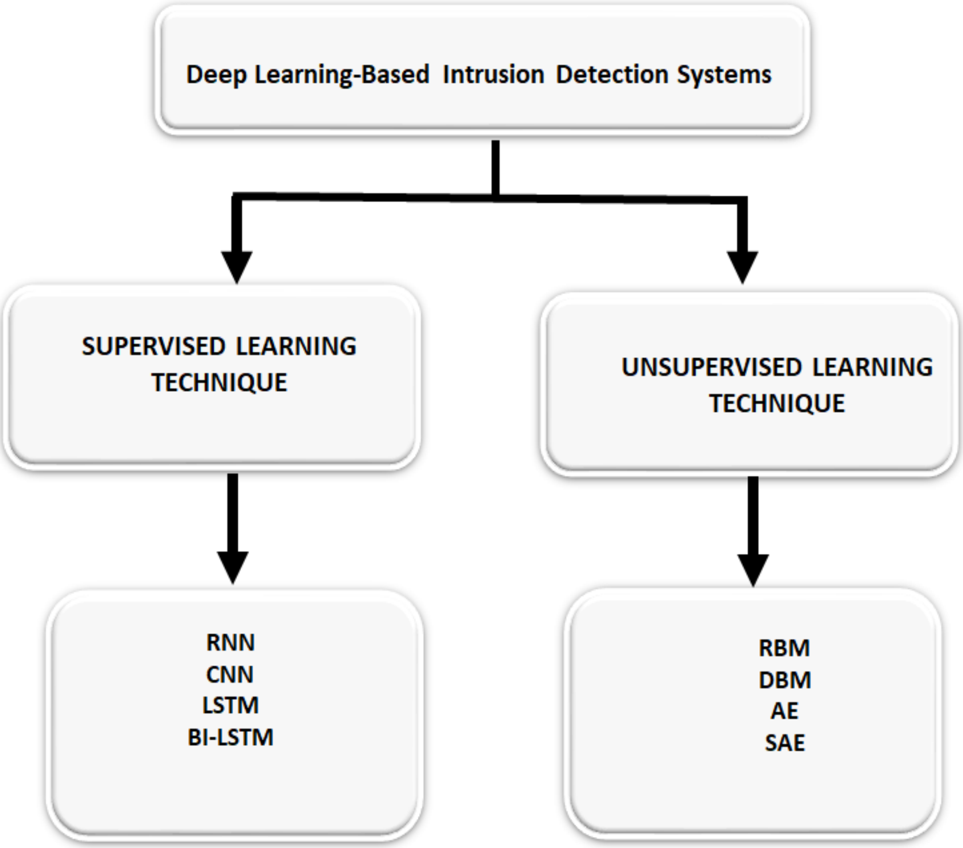
Deep Learning-Based Intrusion Detection Systems
SUPERVISED LEARNING TECHNIQUE
UNSUPERVISED LEARNING TECHNIQUE
RNN
CNN
LSTM
BI-LSTM
RBM
DBM
AE
SAE

Figure 2 Categorization of deep learning approaches for attack mitigation

3. RESULTS

For several datasets, we have conducted a thorough investigation of several attack detection methods in the context of the Internet of Things. Additionally, we examined how well the deep learning models classified traffic in the IoT ecosystem between harmful and legitimate packets. Our research indicates that the datasets NSL-KDD, ISCX, AWID, KDDCUP-99, CIDDS-OO1, and GPRS do not fully capture the traffic of real-time IoT devices (Tavallaee et al., 2009; Diro and Chilamkurti, 2018a; Rezvy et al., 2019). As a result, employing these datasets to train deep learning models may result in high detection rates and accuracy. However, due to the complexity of traffic and the advent of new network attacks, the performance would worsen once deployed in real-world scenarios for attack detection.

However, few researchers have built their datasets by configuring Internet of Things systems to record and examine packets using network analyzer software such as Bro IDS, Scapy, and Wireshark (Meidan et al., 2018; Diro and Chilamkurti, 2018b; McDermott et al., 2018; Thamilarasu and Chawla, 2019). To improve the detection rate and reduce the FAR value, the dataset must be developed from extremely complex IoT devices and a wide range of IoT attacks, as the real-time traffic datasets are assembled by devices with fewer features (Meidan et al., 2018; McDermott et al., 2018). With 45 and 80 features, respectively, CICIDS2017 and UNBW-NB15 are the two datasets that nearly fully address the needs of a real-time IoT environment that can cover a greater variety of security threats (Moustafa and Slay, 2015; Sharafaldin et al., 2018).

A variety of deep learning models have been activated by specialists to identify fraudulent traffic in the Internet of Things networks. However, the type of data used to train the Deep Neural Network (DNN) is the only factor that affects the model's effective performance in network security (Siddiqi, 2019). Based on our investigation, utilizing the CICIDS2017 and UNBW-NB15 datasets the best models for identifying anomalous data in a network with a high detection rate and lower FAR are LSTM+CNN, LSTM, and stacking deep auto-encoder, respectively.

4. DISCUSSION

Technological developments have led to the creation of several learning techniques, including machine learning and deep learning, for identifying security risks and zero-day attacks in the Internet of Things ecosystem. Nonetheless, several issues are to be determined, which are discussed below.

Security-Related Datasets

The creation and extraction of realistic, high-quality data that comprises multiple potential threats is the main obstacle that is essential when using machine learning or deep learning techniques. The researchers may decide to build datasets containing every potential IoT assault to enhance model training and establish a new standard for achieving high accuracy and precision. It can be difficult to regularly update a dataset with new assaults because of the wide technical diversity of different IoT devices.

Poor Data Quality

IoT devices are utilized in a variety of applications as the data quality is impacted by IoT devices' small size and low memory, power, and computation capabilities. Algorithms that can handle noisy and low-quality data are necessary for learning to safeguard the IoT ecosystem. Consequently, it is essential to create robust machine learning and deep learning algorithms to handle noisy, heterogeneous input from several Internet of Things devices.

Learning IoT Attacks

An IoT network consists of a dynamic system where devices are constantly being added or withdrawn based on the changing pattern of the application. It is difficult to distinguish between dangerous and benign data because of their dynamic nature, which presents a unique problem. Updates to the security model are necessary to comprehend and monitor system changes to resolve this problem. Lifelong learning procedures are unified for long-term applications to build models that can repeatedly carry out some retaining procedures for discovering new developing patterns based on network behavior and adjusting to changes aptly.

Table 1 Comparison of various deep learning techniques used for attack

System	Dataset	Attacks	Efficiency	Evaluation
Deep Model (22)	NSL-KDD	DoS, U2R, Probe, R2L	Accuracy, DR, FAR	Shallow Technique
RNN (13)	Real-Time IoT Devices	UDP flood, TCP, SYN, Sleep Deprivation Attack, Barrage Attack, Broadcast Attack	Probability of Detection Time	Simple Threshold Detector
Deep Auto-Encoder (10)	Real-Time IoT Devices	Bashlite, Mirai	TPR, FPR, Average Detection Time	Isolation Forest, LOF, SVM
LSTM (14)	AWID, ISCX	Authentication, ARP Flooding, Injection, Probe Request, Infiltrating, HTTP, DoS, IRC DDoS, SSH Brute Force	Accuracy, Recall, Precision	Logistic Regression
DNN (21)	Real Network, Simulation	Blackhole, Opportunistic Service, DDoS, Sinkhole, Wormhole	Precision, Recall, F1	IWC
Stacked Auto-Encoders (11)	NSL-KDD	DoS, R2L, U2R, Probing	Accuracy, DR, FAR	Shallow Model
Bi-Directional LSTM (15)	UNSW-NB15	Backdoor, DoS, Exploits, Fizzers, Generic, Port	Accuracy, Miscalculation rate,	Nill

		Scans, Reconnaissance, Shellcode, Spam, Worms	FPR, Precision, Recall, F1 score	
DBN4+LR (17)	KDDCUP'99	DoS, Probe, R2L, U2R	Accuracy, FN	RBM, DBM2
Auto-Encoder DNN (23)	AWID	Flooding, Injection, Impersonation	Accuracy	ML Algorithm
Bi-Directional LSTM (16)	A Secure Sandbox Environment (IoT Devices)	Mirai, UDP, ACK, DNS	Accuracy, Loss	LSTM
MLP, LSTM, CNN, LSTM+CNN (20)	CICIDS2017	DDoS	Accuracy, Precision, Recall	Comparison with ML Algorithm
DNN (18)	UNSW-NB15, CIDDS001, GPRS	Backdoor, DoS, Exploits, Fizzers, Generic, Port Scans, Reconnaissance, Shellcode, Spam, Worms, SSH Brute Force	Accuracy, Precision, Recall, FPR	Dataset Comparison
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	Accuracy, Detection, Recall	Comparison with ML, Algorithm

5. CONCLUSION

To identify assaults in IoT networks, we have examined the effectiveness of several deep learning models trained on diverse datasets in this study. The training phase determines how well deep learning models operate; so, the more effectively the network is trained, the better the accuracy and FAR outcomes will be determined. The neural networks dataset aids in the model learning and discovery of novel patterns during the training stage, which helps the network anticipate anomalies.

Using the CICIDS2017 and UNBW-NB15 datasets, LSTM+CNN, LSTM, and stacked deep auto-encoders provide excellent accuracy and low FAR since they replicate real traffic and include a range of threats. To replicate an actual IoT environment, we will build a solid and varied collection of datasets in the future that include packets from basic to multipurpose IoT devices. To establish an innovative paradigm in these deep learning techniques, a dataset is to be created to train several deep learning models and determine how well they perform in compromised circumstances.

Informed consent

Not applicable.

Conflicts of interests

The authors declare that there are no conflicts of interests.

Ethical approval

Not applicable.

Funding

The study has not received any external funding.

Data and materials availability

All data associated with this study are present in the paper.

REFERENCES

1. Abdul-Ghani HA, Konstantas D, Mahyoub M. A Comprehensive IoT attacks survey based on a building-blocked reference model. Int J Adv Compu Sci Appl 2018; 9 (3):355–373.
2. Abeshu A, Chilamkurti N. Deep learning: the frontier for distributed attack detection in fog-to-things computing. IEEE Commun Mag 2018; 56(2):169-175. doi: 10.1109/MCOM.2018. 1700332
3. Al-Garadi MA, Mohamed A, Al-Ali A, Du X, Ali I, Guizani M. A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Commun Surv Tutor 2020; 22 (3):1646-1685.
4. Alrawashdeh K, 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), Anaheim, CA, USA, 2016; 195-200. doi: 10.1109/ICMLA.2016.0040
5. Amanullah MA, Habeeb RAA, Nasaruddin FH, Gani A, Ahmed E, Nainar ASM, Akim NM, Imran M. Deep learning and big data technologies for IoT security. Comput Commun 2020; 151(1):495-517.
6. Atlam HF, Wills G. IoT security, privacy, safety, and ethics. In Digital Twin Technologies and Smart Cities (Internet of Things) Springer Cham, 2020; 1-27. doi: 10.1007/978-3-030-187 32-3 2020;123-149
7. Bengio Y. Deep learning of representations for unsupervised and transfer learning. In Proceedings of ICML workshop on unsupervised and transfer learning 2012; 17-36.
8. Brun O, Yin Y, Gelenbe E, Kadioglu YM, Augusto-Gonzalez J, Ramos M. Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments. International ISCIS Security Workshop, London, UK, 2018; 79-89.
9. Diro A, Chilamkurti N. Leveraging LSTM networks for attack detection in fog-to-things communications. IEEE Commun Mag 2018; 56(9):124-130.
10. Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Gener Comput Syst 2018; 82(1):761-768.
11. Gupta R, Tanwar S, Tyagi S, Kumar N. Machine learning models for secure data analytics: A taxonomy and threat model. Comput Commun 2020; 153(1):406-440.
12. Lee I, Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Bus Horiz 2015; 58(4):431-440.
13. Lu Y, Da XL. Internet of things (IoT) cybersecurity research: A review of current research topics. IEEE Internet Things J 2019; 6(2):2103-2115.
14. Marcus G. Deep learning: A critical appraisal. ArXiv preprint arXiv:1801.00631, 2018.
15. McDermott CD, Majdani F, Petrovski AV. Botnet detection in the internet of things using deep learning approaches. In 2018 International Joint Conference on Neural Networks (IJCNN) 2018; 1(8).
16. Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Shab-tai A, Breitenbacher D, Elovici Y. Network-based detection of IoT botnet attacks using deep auto-encoders. IEEE Pervasive Comput 2018; 17(3):12-22.
17. Mekki K, Bajic E, Chaxel F, Meyer F. A comparative study of LPWAN technologies for large-scale IoT deployment. ICT Express Press, 2019; 5(1):1–7.
18. Moustafa N, Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In 2015 military communications and information systems conference (MilCIS), Canberra, Australia, 2015; 1-6.
19. Muna AH, Moustafa N, Sitnikova E. Identification of malicious activities in industrial internet of things based on deep learning models. J Inf Secur Appl 2018; 41(1):1–11.
20. Oliver A, Odena A. Raffel C, Cubuk ED, Good-fellow IJ. Realistic evaluation of semi-supervised learning algorithms. Machine Learning, arXiv:1804.09170 [cs.LG], 2018.
21. Qingchen Z, Laurence TY, Zhikui C, Peng L. A survey on deep learning for big data. Inf Fusion 2018; 42(1):146-157.
22. Rezvy S, Luo Y, Petridis M, Lasebae A, 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), 2019; 1-6.
23. Roopak M, Tian GY, Chambers J. Deep learning models for cyber security in IoT networks. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019; 452-457.
24. Roy B, Cheung H. A deep learning approach for intrusion detection in internet of things using bi-directional long short-

term memory recurrent neural network. In 2018 28th International Telecommunication Networks and Applications Conference (ITNAC) 2019; 1(6).

25. Sharafaldin I, Lashkari AH, Ghorbani AA. A detailed analysis of the CICIDS2017 data set. ICISSP 2018.
26. Shin H, Lee HK, Cha HY, Heo SW, Kim H. IoT security issues and lightweight block cipher. International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2019; 381-384.
27. Siddiqi A. Adversarial security attacks and perturbations on machine learning and deep learning methods. ArXiv preprint arXiv:1907.07291, 2019.
28. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. IEEE Commun Surv Tutor 2020; 22(2):1191-1221.
29. Tama BA, Rhee KH. Attack classification analysis of IoT network via deep learning approach. Res. Briefs Inf Commun Technol Evol (ReBICTE) 2017; 3(1):1-9.
30. Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. IEEE symposium on computational intelligence for security and defense applications, Ottawa, 2009; 1-6.
31. Tawalbeh LA, Muheidat F, Tawalbeh M, Quwaider M. IoT Privacy and Security: Challenges and Solutions. Appl Sci 2020; 10(12):4102. doi: 10.3390/app10124102
32. Thamilarasu G, Chawla S. Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things. Sensors (Basel) 2019; 19(9):1977. doi: 10.3390/s19091977
33. Zhou Y, Han M, Liu L, He, JS, Wang Y. Deep learning approach for cyberattack detection. In IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 2018; 262-267. doi: 10.1109/INFCOMW.2018.8407032
34. Zhu X, Goldberg AB. Introduction to semi-supervised learning. Synthesis lectures on artificial intelligence and machine learning 2009; 3(1):1-130.