IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

A Novel Deep Learning Approach for IoT Security and Privacy Attack Detection

Aziz Ullah Karimy[1] and Dr. P Chandrasekhar Reddy[2]
Department of Electronics and Communication Engineering[1,2]
Jawaharlal Nehru Technological University, Hyderabad, India

Abstract: *The Internet of Things (IoT), often known as the Internet of Objects, is envisioned as a game-changing method of offering a variety of services. IoT is not complete without compact smart devices, which come in a wide variety of uses, sizes, energy capacities, and processing speeds. However, the incorporation of these smart devices into the traditional Internet poses a number of security issues because, in order to accommodate IoT, technologies and communication protocols were not created. Additionally, the commercialization of IoT has raised challenges with personal privacy, the potential of cyberattacks, and organized crime that are related to public security. In this context, significant attempts have been made, largely using conventional cryptographic techniques, to address the security and privacy challenges in IoT networks. The existing approaches, however, are insufficient to cover the complete security spectrum of IoT networks due to the distinctive features of IoT nodes. To deal with various security issues, machine learning (ML) and deep learning (DL) approaches that may embed intelligence in IoT devices and networks can be used. In this work, we offer a powerful model to recognize security concerns using deep learning techniques on the latest datasets, which were made available for undertaking research activities, we may identify privacy-related dangers in the IoT era. Here, we looked at the feature set of the data needed to use the suggested model to identify the various vulnerabilities stated in the given dataset. The classification of binary and multiclass assaults using deep learning techniques is examined in this work.*

Keywords: IoT, IoT threat, Internet of Objects, Security, Privacy, Deep Learning

I. INTRODUCTION

Recent advancements in technology have ushered in a new era of interconnectedness, enabling seamless interactions with objects in our surroundings. At the forefront of this technological revolution is the Internet of Things (IoT), a paradigm that offers a myriad of possibilities for enhancing communication with our environment. By leveraging IoT, the world around us is poised to become smarter and more intelligent, promising a simpler, safer, and smarter way of life.

The Internet of Things has rapidly become deeply ingrained in our daily lives, transforming the way we interact with the world. Its applications are vast and diverse, with the potential to reshape our lifestyles in significant ways [1], [2]. However, the widespread adoption of IoT faces numerous challenges that must be addressed to ensure its success. These challenges encompass scaling issues, managing massive volumes of data, interpreting and deriving insights from data, ensuring interoperability, maintaining fault tolerance, addressing power supply concerns, optimizing wireless communication, and upholding privacy and security [18], [21]-[22]. Among these challenges, security and privacy have emerged as the most critical areas that demand immediate attention and resolution.

As our understanding of IoT deepens and real-world application scenarios expand, the security issues surrounding IoT technology have garnered increasing attention. Scholars and researchers from around the globe have devoted substantial efforts to investigating and comprehending IoT security threats. This paper aims to shed light on the security threats that IoT poses from three distinct perspectives: physical device threats, network communication threats, and information data threats. By aligning with China's network security level protection network, which emphasizes cloud computing security expansion, the paper strives to provide a comprehensive overview of IoT security concerns. Through this analysis, it endeavors to offer valuable insights and guidance for the development of robust IoT security models and solutions [15-16].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

Device Threats

Traditional cybersecurity concerns include data tampering and deletion, as well as disguising, unlawful connections, unauthorized access, denial of service, repudiation, information leakage, traffic analysis, and faulty information flow. IoT security differs significantly from traditional network security in that there are many more IoT devices. Device and resource constraints are two main vulnerability points.

Network Communication Threats

The IoT security foundation includes physical risks, and network security is the most important aspect of IoT security. The IoT network is built with interoperability and operability in mind, but it also reveals weak controllability and heterogeneity as drawbacks [13]. Network communication occurs often at the middle layer of the IoT architecture, transferring, storing, and analysing the data transmitted from the underlying layer. The transfer, storage, and processing expose various security risks.

The major structural distinction between the Internet of Things network system and the traditional network system is that the former has manageability and weak controllability traits. This has made it extremely difficult to advance the Internet of Things. IoT data must be transferred, analysed, and stored before it can be used for network communication. The communication process makes use of numerous communication protocols, these protocols have vulnerabilities [17].

Information Data Threats

Confidentiality, integrity, availability, controllability, and non-repudiation are the five pillars of information security. IoT data transmission, processing, and storage will reveal many security vulnerabilities. The three qualities of "confidentiality, integrity, and availability" reflect the key information data vulnerabilities [12].

A significant volume of data produced by IoT devices can also be utilized to generate patterns, behaviors, and predictions in successive dataset generations. We must identify techniques in IoT frameworks to address various issues [9]. As a result, the primary goal of this work is to develop security strategies for IoT devices.

New approaches are needed to effectively utilize the vast amount of data generated in the IoT ecosystem, and deep learning (DL) stands out as the most effective method to incorporate intelligence into IoT networks and devices. Deep learning serves as a powerful data exploration technique, allowing for the understanding of both typical and abnormal behavior exhibited by specific machines [10]. By training algorithms on extensive data sets, these algorithms can distinguish between normal and anomalous activities within a network. Through continuous learning from new data, these algorithms automatically improve their performance.

Deep Learning

Deep Learning is a subset of machine learning that uses supervised, semi-supervised, and unsupervised learning as its three learning methods. It is made up of numerous artificial neural network layers. There are some neurons in each layer with activation capabilities that can be used to generate non-linear outputs. The neuronal structure of the human brain is presumably the source of inspiration for this technology[1].

Despite the fact that deep learning is not directly related to IoT security and safety, constant network and communication monitoring between IoT devices and systems can help identify and mitigate security breaches at an early stage. Deep learning's characteristics and features help identify security breaches. This is because deep learning is capable of processing very big datasets, categorizing legitimate and anomalous data with a greater accuracy rate, learning from complicated data, and learning from data at a much faster rate [11].

Application area of Deep learning in IoT Security

Anomaly detection, finding anomalies is the process of anomaly detection. An abstract definition of an anomaly is a pattern that deviates from typical, expected behavior. These anomalies are caused by strange behaviors like credit card fraud, cyberattacks etc. Three categories—point anomalies, contextual anomalies, and collective anomalies—are usually used to classify abnormalities[2].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

Point Anomalies, a point anomaly is the simplest type of anomaly and is defined as a data instance that can be considered abnormal compared to the rest of the data.

Contextual anomalies, contextual anomalies are instances of data that are unusual in one context but not in another. Contextual attributes and behavioral attributes are the two characteristics of contextual anomalies.

Collective anomalies, a group of related data instances that act abnormally when compared to the complete dataset are referred to as collective anomalies.

In our proposed study, we employ deep learning techniques to combat millions of network attacks in a heterogeneous network, utilizing the NSL-KDD dataset provided by the Canadian Institute for Cyber Security at the University of New Brunswick.

To detect anomalies in the IoT environment, we apply combinations of algorithms using open-source standard datasets [5]. This includes utilizing recurrent neural networks (RNN), convolutional neural networks (CNN), as well as machine learning algorithms such as Naive Bayes (NB), Support Vector Machine (SVM), and Decision Tree (DT). We perform binary classification on both the NSL-KDD and UNSW-NB15 datasets and compare the performance of these algorithms using various metrics. By leveraging open-source standard datasets and algorithms, we aim to detect anomalies within the context of IoT. We utilize deep neural networks (DNN) and machine learning techniques such as support vector machines (SVM). The NSL-KDD dataset is subjected to binary classification, and the effectiveness of the algorithms is evaluated using multiple metrics [8].

In conclusion, machine learning and deep learning techniques have emerged as powerful tools in enhancing IoT security. These advanced algorithms enable the detection of anomalies, identification of patterns, and prediction of potential threats within the IoT ecosystem. By leveraging machine learning and deep learning, IoT security systems can be significantly improved. The integration of smart devices into the Internet of Things has brought forth substantial security concerns and challenges that cannot be adequately addressed by conventional cryptographic techniques. To mitigate these vulnerabilities, the utilization of machine learning and deep learning approaches has become crucial. By embedding intelligence in IoT devices and networks, these techniques allow for the identification of security concerns and the detection of privacy-related dangers. This study proposes a robust model that utilizes deep learning techniques on the latest datasets to effectively recognize and classify various vulnerabilities within the IoT ecosystem. By leveraging machine learning and deep learning, we can enhance the security of IoT networks and ensure the protection of sensitive data in the IoT era.

II. LITERATURE STUDY

Harun Surej Ilango et al. [4] did a research on detecting Low Rate DoS attack in SDN environment at network layer using combined FeedForward CNN and CNN, CIC DoS 2017 dataset being used for this research in two phase of pre-processing and LR DoS detection phases. They removed features source IP, destination IP, ports, protocol and Zero variance features to generalize the dataset, a wrapper-based feature selection using SVM were used to select subset of important features. Due to time constrained in IoT environment for data processing feature reduction plays more important rule and this has been done in this study. FFCNN is used to further classify the attacks and benign with only seven features of dataset in the network, the performance of FFCNN is compared to the machine learning algorithms J48, Random Forest, Random Tree, REP Tree, SVM, and Multi-Layer Perceptron in order to further identify attacks and benign behavior in the network (MLP). Accuracy, precision, recall, F1 score, detection time per flow, and ROC curves are used to evaluate the models' performance. According to the empirical analysis, FFCNN performs better than other machine learning algorithms across the range (3). This study is more specific in detecting one kind of DoS attack and the performance of model to detect other attacks were not tested, so the hybrid of the method with other existing method may increase the processing time again for IoT devices.

Eva Rodríguez et al. studied performance of Transfer Learning (TL) to detect zero_day intrusions in an IoT environment, two phases were introduced in this study, in phase one BoT-IoT (4)dataset were used as source domain dataset to train the TL with 75% and 25% ratio as training and validation sets respectively, in this phase model is referred as base ID-model and applied knowledge learned in this source domain to target domain in second phase. In second phase USNW-NB15 (5) datasets were used to further train the model. The trained model is validated using two sub-categories of UNSW-NB15 datasets containing zero-day attacks and combined of zero-day and know attacks, the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

result they achieved were extremely well, 99.04% of accuracy in zero-day attacks and 97.89% in zero-day and known attacks (6).

Muhammad Fasih Ashfaq et al. [21] carried out a detailed study on Logistic Regression and Decision Tree algorithms to classify DDoS attacks and normal traffic in an IoT environment. In this experiment two different datasets were used for low rate DDoS and high rate DDoS real time data collected from Wireshark which has two features and KDD-Cup datasets containing 7 features. Accuracy and confusion matrices were considered for evaluating the performance of the model. Accuracy they achieved in this study in both the algorithms and datasets are very high compare to other methods been used as of now [7].

III. METHODOLOGY

Data Collection: The first step in our methodology is to gather relevant datasets for training and evaluation purposes. We utilized the NSL-KDD dataset provided by the Canadian Institute for Cyber Security at the University of New Brunswick. This dataset contains a wide range of network traffic data, including normal and anomalous activities, making it suitable for our IoT security analysis.

Preprocessing: Before applying machine learning and deep learning algorithms, the collected data needs to be preprocessed. This involves tasks such as data cleaning, normalization, and feature extraction. We ensure that the data is in a suitable format and ready for further analysis.

Algorithm Selection: In this step, we determine the algorithms that will be employed for anomaly detection and classification in the IoT context. We selected a combination of deep learning techniques such as recurrent neural networks (RNN) and convolutional neural networks (CNN), along with traditional machine learning algorithms including Naive Bayes (NB), Support Vector Machine (SVM), and Decision Tree (DT). This selection allows us to leverage the strengths of both deep learning and machine learning approaches.

Training and Testing: The selected algorithms are trained on the preprocessed data. We divide the dataset into training and testing sets in ratio of 80% and 20%, ensuring that both contain a representative distribution of normal and anomalous instances. The models are trained using the training set and evaluated on the testing set to measure their performance in detecting anomalies and classifying attacks.

IV. RESULTS AND DISCUSSION

Performance Evaluation: To assess the effectiveness of the algorithms, we employ various evaluation metrics. These metrics include accuracy, precision, recall, and F1-score, among others. By analyzing these metrics, we determine that deep learning outperform obtaining 99% accuracy, 94% recall and 97% precision in detecting IoT vulnerabilities.

Table 1. Metrics evaluation of algorithms

Algorithm	Accuracy	Precision	Recall	F1-Score
Deep Learning	90%	79%	97%	87%
SVM	78.8%	52%	100%	69%
RF	69.56%	55%	97%	68%

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

Prediction Results
Deep Neural Algorithm Accuracy, Classification Report & Confusion Matrix

Accuracy : 90.26232741617358

Report :	precision	recall	f1-score	support
0.0	0.79	0.97	0.87	1061
1.0	0.90	0.91	0.90	680
2.0	0.00	0.00	0.00	17
3.0	0.00	0.00	0.00	63
4.0	0.00	0.00	0.00	49
5.0	0.00	0.00	0.00	11
6.0	0.00	0.00	0.00	25
7.0	0.00	0.00	0.00	62
8.0	0.00	0.00	0.00	46
9.0	0.00	0.00	0.00	2
10.0	0.00	0.00	0.00	8
11.0	0.00	0.00	0.00	1
15.0	0.00	0.00	0.00	2
17.0	0.00	0.00	0.00	1

Figure1. Deep Learning Performance evaluation

The Figure 1 illustrates that the accuracy of the DNN algorithm is superior to the other two algorithms. However, it is important to note that the accuracy of the DNN algorithm may vary at different times due to the random selection of hidden layers from the dataset.

Comparison and Discussion: Finally, we compare the performance of the different algorithms and discuss the findings, same is demonstrated in Figure 2. We examine the advantages and disadvantages of machine learning and deep learning techniques in mitigating IoT vulnerabilities. This discussion helps us draw conclusions and provide recommendations for enhancing IoT security using these approaches.

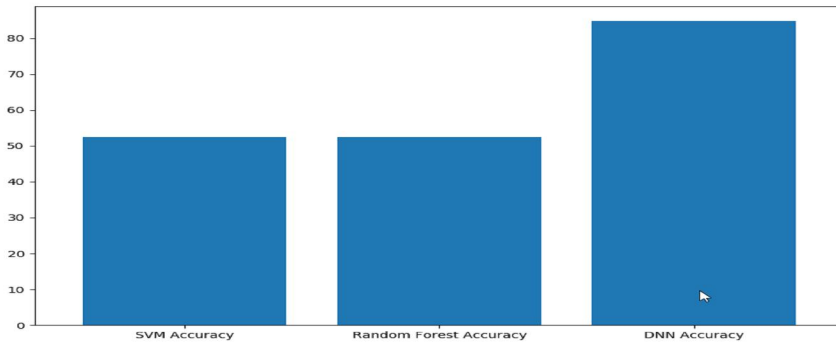

Figure 2. Comparison of ML Algorithms

V. CONCLUSION

In this study, we introduce a combined intrusion detection alarming system that has the capability to monitor networks and utilizes a highly scalable design on both commodity IoT devices and servers. The system incorporates a distributed deep learning model based on Deep Neural Networks (DNNs) to effectively handle and analyze massive amounts of data in real-time. The selection of the DNN model was made after conducting a comprehensive evaluation of its performance compared to traditional machine learning classifiers using various benchmark datasets.

By collecting real-time host-based and network-based data, we employed the recommended DNN model to accurately identify and detect attacks and intrusions. Our findings reveal that DNNs consistently outperformed traditional machine learning classifiers in all scenarios, showcasing their superiority in the context of intrusion detection. Furthermore, the architecture we propose demonstrates significant advancements over previously developed conventional machine learning classifiers. To the best of our knowledge, our system is the first of its kind to combine distributed DNNs with the capability to gather network-level and host-level activity, enabling more effective attack detection.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

Overall, our study presents a robust intrusion detection system that leverages distributed DNNs to analyze network data in real-time. The utilization of DNNs proves to be superior to traditional machine learning classifiers, leading to enhanced performance and more effective attack detection. This research contributes to the advancement of IoT security by providing a scalable and efficient solution for detecting and mitigating potential threats in IoT networks.

REFERENCES

[1] M. I. P. Z. S.-T. X. a. X. W. F. I. Zhong-Qiu Zhao, "Object Detection With Deep Learning: A Review," 2019.

[2] (. I. M. A. T. (. M. I. N. A. F. M. D. ALI BOU NASSIF, "Machine Learning for Anomaly Detection: A Systematic Review," 2021.

[3] M. M. R. S. Harun Surej Ilango, "A FeedForward–Convolutional Neural Network to Detect Low-Rate DoS in IoT," 2022.

[4] N. M. E. S. a. B. T. N. Koroniotis, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset,," vol. 100, 2019.

[5] S. J. Moustafa N, "a comprehensive data set for network intrusion detection systems (UNSW-NB15 network dataset)," 2015.

[6] P. V. B. O. J. J. C. ,. J. V. ,. M. A. P. Eva Rodríguez, "Transfer-Learning-Based Intrusion Detection Framework in IoT Networks," 2022.

[7] M. F. Ashfaq, M. Malik, U. Fatima and M. K. Shahzad, "Classification of IoT based DDoS Attack using Machine Learning Techniques," 2022.

[8] M. A. ,. K. A. ,. M. A. Shadi Al-Sarawi, "Internet of Things (IoT) Communication Protocols :," 2017.

[9] C. C. A. I. A. M. Marica Amadeo, "Information Centric Networking in IoT scenarios:," 2015.

[10] N. V. ,. D. R. R. A. A. N. R. Swapna Thouti, "Investigation on identify the multiple issues in IoT devices using Convolutional Neural Network," 2022.

[11] I. S. D. G. Rajiv Yadav, "Augmentation in performance and security of WSNs for IoT applications using feature selection and classification techniques," 2022.

[12] A. I. A. S. M. M. K. H. R. C.-P. Yakub Kayode Saheed, "A machine learning-based intrusion detection for detecting internet of things network attacks," 2022.

[13] A. J. O. R. P. B. Fatimah Aloraini, "Adversarial machine learning in IoT from an insider point of view," 2022.

[14] J. T. P. A. R. F. C. N. M. G. U. Regonda Nagaraju, "Attack prevention in IoT through hybrid optimization mechanism and deep learning framework," 2022.

[15] C. L. Xiaoyong Yuan and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," 2017.

[16] N. K. Sarika Choudhary, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT," 2020.

[17] N. K. Monika Vishwakarma, "DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT," 2022.

[18] A. Tasnim, N. Hossain, N. Parvin, S. Tabassum, R. Rahman and M. Iqbal, "Experimental Analysis of Classification for Different Internet of Things (IoT) Network Attacks Using Machine Learning and Deep learning," 2022.

[19] U. S. S Thavamani, "LSTM based Deep Learning Technique to Forecast Internet of Things Attacks in MQTT Protocol," 2022.

[20] F. C. D. D. M. T. A. G. A. M. A. P. Alfredo Nascita, "Machine and Deep Learning Approaches for IoT Attack Classification," 2022.

[21] M. O. R. L. B. H. Roumaissa Bekkouche, "Ultra-Lightweight and Secure Intrusion Detection System for Massive-IoT Networks," 2022.

[22] S. (. G. N. K. S. H. A. G. M. A. Aaisha Makkar, "An Efficient Spam Detection Technique for IoT Devices Using Machine Learning," vol. 17, no. 2, 2021.