IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Deep Learning-Based Intrusion Detection in IoT Networks: BoT-IoT Dataset

[1]Mohammad Shayaan Khan, [2]Mohammad Shadaab Adnan, [3]Syed Shahanawaz Hussain

[1]Student, [2]Student, [3]Student

[1]Department of Computer Science and Engineering,

[1]Malla Reddy University, Hyderabad, India

Abstract: The rapid expansion of Internet of Things (IoT) devices has been transformed into modern infrastructure around healthcare, industrial reformation, smart cities, and consumer applications. However, this rapid multiplication has never created security challenges, making IoT networks attractive targets for sophisticated cyberattacks [1]. Traditional signature-based intrusion detection systems (IDS) struggle to keep pace with the evolving nature of attacks, particularly botnet-based threats that exploit the inherent resource constraints of IoT devices. Deep learning has emerged as a promising solution for developing robust, adaptive intrusion detection systems capable of identifying both known and novel attack patterns in IoT environments [2]. The BoT-IoT dataset has become a critical standard for evaluating these advanced detection approaches, providing researchers with realistic network traffic data that captures the complexity of modern botnet attacks in IoT infrastructures.

Index Terms **-** Internet of Things (IoT), Intrusion Detection System, Deep Learning, Cybersecurity, BoT-IoT Dataset, Botnet Attacks.

I. Introduction

The Internet of Things (IoT) has undergone explosive growth over the past decade, fundamentally transforming how we live, work, and interact with our environment. From smart homes equipped with connected thermostats and security systems to industrial facilities leveraging IoT sensors for real-time monitoring, to healthcare systems utilizing wearable devices for patient monitoring, the proliferation of interconnected devices has created unprecedented opportunities for innovation and efficiency [1]. However, this rapid expansion has simultaneously introduced critical security vulnerabilities that threaten the integrity, confidentiality, and availability of IoT networks and the sensitive data they process and transmit [2]. IoT devices are uniquely vulnerable to cyber threats due to inherent design constraints that differentiate them from traditional computing systems. These devices typically operate with severely limited computational resources, memory constraints, and battery life considerations, necessitating trade-offs that often result in compromised security implementations [3]. Furthermore, the sheer heterogeneity of IoT ecosystems—encompassing diverse device manufacturers, communication protocols, operating systems, and network architectures—creates a complex attack surface that traditional security measures struggle to adequately protect [4]. The interconnected nature of IoT systems means that compromise of a single device can potentially propagate throughout an entire network, creating cascading failures and widespread disruption [5].

II. Literature Review

The spurt in the use of Internet of Things (IoT) devices has completely changed the face of the cybersecurity environment in ways that the conventional approaches of network security are not equipped to handle. This is because the IoT environment is distinguished by the fact that it has very severe resource constraints and is highly distributed, thereby making it extremely challenging to handle from the perspective of implementing any kind of central command and control over the entire network for purposes of security

[1]. The direct result of the spurt in the number of IoT devices being connected has led the attack surface area to grow exponentially [2]. The issues related to cybersecurity in IoT networks can be very complex. This is mainly because most IoT devices are designed with negligible security considerations in mind, which leads to the widespread use of default passwords, vulnerabilities in software, and weak encryption practices [1]. Moreover, IoT networks are very heterogeneous with regard to hardware components, communication protocols, operating systems, and IoT architecture. This adds to the complexity of implementing a common cybersecurity framework in IoT networks [3].

Compounding these issues, IoT devices often remain operational for extended periods without receiving timely security updates, thereby increasing the window of exposure during which known vulnerabilities can be exploited [3].

Among the most severe threats targeting IoT networks are botnet-based attacks, in which adversaries compromise large numbers of IoT devices and coordinate them to perform malicious activities at scale [4]. Unlike traditional botnets composed primarily of personal computers, IoT botnets exploit devices that are continuously connected to networks, frequently embedded within critical infrastructure, and difficult for end users to monitor or secure. The Mirai botnet highlighted the destructive potential of such attacks by compromising hundreds of thousands of IoT devices and launching large-scale distributed denial-of-service (DDoS) attacks, underscoring the significant risks posed by inadequately secured IoT systems [5]. Since then, IoT botnets have continued to evolve, adopting more advanced techniques for device exploitation, persistence, and command-and-control communication, thereby posing an ongoing and escalating threat to network security [6].

III. Problem Statement and Objectives

The Internet of Things has experienced exponential growth over the past decade, with billions of interconnected devices now deployed across critical infrastructure, healthcare systems, industrial facilities, smart homes, and transportation networks [1]. This proliferation of IoT devices has dramatically expanded the attack surface available to cybercriminals, fundamentally transforming the cybersecurity threat landscape. While IoT technology offers tremendous benefits in terms of automation, efficiency, and real-time data collection, it simultaneously introduces unprecedented security vulnerabilities that traditional network security mechanisms were not designed to address [2].

The fundamental challenge underlying IoT security stems from the inherent constraints of IoT devices themselves. IoT devices are characterized by severe resource limitations including minimal computational capacity, limited memory, restricted battery life, and constrained network bandwidth [3]. These resource constraints necessitate that IoT devices operate with simplified processing capabilities and reduced cryptographic implementations compared to traditional computing infrastructure. Consequently, manufacturers frequently prioritize cost reduction and rapid time-to-market over comprehensive security implementation, resulting in devices deployed with weak default credentials, unpatched software vulnerabilities, and inadequate encryption mechanisms [1]. Furthermore, the heterogeneous nature of IoT ecosystems—encompassing diverse device manufacturers, communication protocols, operating systems, and network architectures—creates enormous complexity in implementing uniform security solutions that can protect across this diversity [3].

Botnet attacks represent one of the most severe and rapidly evolving threats targeting IoT networks. Unlike traditional botnets composed primarily of compromised personal computers, IoT botnets exploit the always-connected nature of IoT devices, their frequent placement in critical infrastructure environments, and the relative difficulty end-users face in securing or monitoring them [4]. Recent high-profile incidents including the Mirai botnet attacks demonstrated the catastrophic potential of weaponized IoT devices, with compromised cameras and smart devices orchestrated to launch unprecedented, distributed denial-of-service attacks that temporarily incapacitated major internet infrastructure [5]. Subsequent botnet variants have continued to evolve, incorporating increasingly sophisticated techniques for initial device compromise, persistent access maintenance, and command-and-control communication orchestration [6]. The sophisticated, constantly evolving nature of modern botnet attacks demands correspondingly advanced detection capabilities that can adapt to emerging threats in real-time.

Existing intrusion detection systems for IoT environments face significant limitations in their capacity to effectively address this evolving threat landscape. Traditional signature-based detection systems, which identify attacks by matching network traffic against predefined patterns of known attacks, fundamentally cannot detect novel or previously unseen attacks [7]. As attackers continuously develop new attack variants and techniques, signature-based systems fall progressively behind the threat landscape, achieving poor detection rates for emerging attacks. While anomaly-based detection approaches that identify deviations from learned normal behavior patterns offer greater flexibility, traditional machine learning approaches for anomaly detection require extensive manual feature engineering effort and demonstrate limited capacity to capture complex, high-dimensional nonlinear relationships present in IoT network traffic data [7]. Additionally, many existing IDS approaches were developed and evaluated using outdated datasets that do not accurately reflect contemporary IoT network characteristics, attack patterns, or the scale of modern botnet operations [8].

The class imbalance problem presents a particularly acute challenge for machine learning-based intrusion detection in IoT networks. In real-world IoT deployments, benign network traffic vastly outnumbers malicious traffic, with attack instances often comprising less than 0.02% of total network traffic [8]. Machine learning models trained on such severely imbalanced data exhibit strong bias toward the majority class, achieving misleadingly high overall accuracy rates by simply predicting all instances as benign traffic while failing to detect the minority attack class [9]. This behavior proves catastrophic for intrusion detection applications where failure to detect even small percentages of attacks can enable significant damage to critical systems and infrastructure.

IV. Proposed Methodology

This section describes the methodology adopted to design and implement a deep learning-based intrusion detection system for Internet of Things (IoT) networks using the BoT-IoT dataset. The proposed approach follows a structured and systematic process that begins with dataset selection and preparation, followed by data preprocessing to remove irrelevant and non-numeric features. Subsequently, a deep learning model is constructed to learn patterns from network traffic data. The model is trained and validated using appropriate learning parameters to ensure effective performance. Finally, the trained system is evaluated using standard performance metrics to assess its ability to accurately detect malicious activities in IoT environments.

4.1 Dataset Description

The BoT-IoT dataset developed by the Cyber Range Lab at UNSW Canberra is used in this study. The dataset contains realistic IoT network traffic generated from a simulated network environment, including both normal and malicious activities. It comprises multiple attack categories such as Distributed Denial of Service (DDoS), Denial of Service (DoS), scanning attacks, keylogging, and data exfiltration. In this work, the CSV-based version of the dataset is utilized to facilitate efficient data handling and analysis.

4.2 Data Preprocessing

Before training the model, several preprocessing steps are applied to prepare the dataset. Initially, non-numeric features such as IP addresses, MAC addresses, and protocol identifiers are removed, as deep learning models require numerical inputs. The attack attribute is selected as the target variable to perform binary classification, where normal traffic is represented as 0 and attack traffic as 1. The remaining numerical features are then normalized using standard scaling to ensure uniform feature distribution and improve model convergence. Finally, the dataset is divided into training and testing sets using an 80:20 split.

4.3 Proposed Deep Learning Model

A deep neural network (DNN) is designed to classify IoT network traffic as either normal or malicious. The model consists of an input layer corresponding to the selected features, followed by multiple hidden layers with Rectified Linear Unit (ReLU) activation functions to capture complex patterns in the data. The output layer uses a sigmoid activation function to generate a binary classification output. The model is trained using the Adam optimizer and binary cross-entropy loss function, which are well-suited for binary classification problems.

4.4 Model Training

The training process is carried out using the preprocessed training dataset. The model is trained for multiple epochs with an appropriate batch size to ensure stable learning. During training, a portion of the training data is used for validation to monitor the model's performance and prevent overfitting. The learning process continues until the model achieves optimal accuracy and minimal loss.

4.5 Performance Evaluation

The performance of the proposed model is evaluated using the test dataset that was not seen during training. Standard evaluation metrics such as accuracy, precision, recall, F1-score, and confusion matrix are employed to assess the effectiveness of the intrusion detection system. These metrics provide insights into the model's ability to correctly identify malicious traffic while minimizing false detections.

4.6 Methodology Summary

The complete methodology ensures a systematic approach to intrusion detection in IoT networks by combining effective data preprocessing, deep learning-based classification, and comprehensive evaluation. The proposed system demonstrates strong capability in detecting botnet-based attacks within IoT environments.

V. Results and Discussion

5.1 Results of Descriptive Statistics of Study Variables

Table 5.1: Descriptive Statistics of Selected Network Traffic Features

Feature	Class	Count	Mean	Std Dev	Min	Max
pkts	**Normal (0)**	**19**	**7.32×10^7**	**1.29×10^5**	**7.31×10^7**	**7.34×10^7**
pkts	**Attack (1)**	**370424**	**7.31×10^7**	**1.06×10^5**	**7.30×10^7**	**7.34×10^7**
srate	**Normal (0)**	**19**	**16.88**	**33.47**	**0.00**	**4784.68**
srate	**Attack (1)**	**370424**	**0.000007**	**0.0021**	**0.00**	**4629.62**
drate	**Normal (0)**	**19**	**0.41**	**—**	**0.00**	**79.97**
drate	**Attack (1)**	**370424**	**0.00**	**—**	**0.00**	**0.66**

Table 4.1 presents the descriptive statistics of selected network traffic features from the BoT-IoT dataset, comparing normal and malicious traffic instances. The packet count (pkts) shows similar mean values for both classes; however, attack traffic exhibits more consistent packet generation, which is characteristic of automated botnet behavior. Significant differences are observed in traffic rate features. Normal traffic demonstrates higher variability in source packet rate (srate), indicating legitimate bursty communication patterns, whereas attack traffic shows an extremely low mean source rate, suggesting distributed low-rate packet generation from multiple compromised devices. Similarly, destination packet rate (drate) values for normal traffic are higher compared to attack traffic, reflecting controlled communication with IoT devices.
The table also highlights a substantial class imbalance, with attack samples significantly outnumbering normal traffic instances, which is common in real-world IoT security datasets. Despite this imbalance, the statistical differences between normal and malicious traffic remain evident, particularly in traffic rate-related features. These variations indicate distinct behavioral patterns that can be effectively learned by deep learning models. Consequently, the descriptive statistical analysis supports the suitability of the proposed deep learning-based intrusion detection system for accurately identifying malicious activities in IoT networks.

This section highlights the experimental results derived using the proposed deep learning-based intrusion detection system on the BoT-IoT dataset. To measure the efficacy of the proposed model, it is evaluated using various performance metrics such as accuracy, precision, recall, F1-score, and confusion matrix. These performance evaluation metrics help analyze the proposed IDS in detail in terms of ability to provide accurate outputs to differentiate between normal and malicious network traffic as well as to provide reliability in botnet-based attack detection in the IoT environment.

5.2 Experimental Results

The proposed deep learning system was able to obtain a detection accuracy of 99.99% on the test dataset, clearly showcasing the robustness of the system in identifying normal as well as malicious IoT traffic. The analysis of the confusion matrix reveals that the system was able to identify almost all the malicious instances correctly, thereby achieving a nearly perfect recall rate for the attack class. The successful detection of the attack pattern by the system in the sample testing of the network traffic instances not only guarantees generalization ability but also showcases the efficiency of the proposed system in the detection of botnet attacks that can be catastrophic in an IoT environment.

5.3 Discussion

The high performance of the proposed model can be attributed to the effectiveness of deep learning in capturing complex patterns within high-dimensional network traffic data. The descriptive statistical analysis revealed clear behavioral differences between normal and attack traffic, particularly in traffic rate-related features, which the model successfully learned during training. Although the dataset exhibits a significant class imbalance with a much larger proportion of attack samples, this scenario closely reflects real-world IoT security conditions. In such environments, achieving high recall for malicious traffic is more critical than minimizing false alarms. Therefore, the obtained results demonstrate that the proposed approach is suitable for practical intrusion detection in IoT networks. Future improvements may include addressing class imbalance through resampling techniques and extending the system for real-time deployment.

VI. Conclusion and Future Work

This study presented a deep learning-based intrusion detection system for Internet of Things (IoT) networks using the BoT-IoT dataset. The approach involved effective data preprocessing, feature selection, and designing a deep neural network to classify network traffic as normal or malicious. Experimental results showed that the model achieved very high detection accuracy, successfully identifying botnet attacks in IoT environments. The findings suggest that deep learning techniques work well for managing complex and large-scale IoT network traffic and can significantly improve network security by accurately detecting malicious activities.

Despite the promising results, there is room for improvement. Future work may focus on addressing the class imbalance in the dataset using sampling techniques to better detect normal traffic. Additionally, the system could be extended for real-time intrusion detection and implemented on edge or fog computing platforms to support practical IoT applications. Exploring other deep learning architectures and testing the model on more IoT security datasets may enhance robustness and generalization.

References

[1] Koroniotis, N., Moustafa, N., Sitnikova, E. and Turnbull, B. 2019. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: BoT-IoT dataset. *Future Generation Computer Systems*, 100: 779–796.

[2] Koroniotis, N., Moustafa, N. and Sitnikova, E. 2020. A new network forensic framework based on deep learning for Internet of Things networks. *Future Generation Computer Systems*, 110: 91–106.

[3] Moustafa, N., Turnbull, B. and Choo, K.K.R. 2019. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things. *IEEE Internet of Things Journal*, 6(3): 4815–4830.

[4] Khan, M.A., Karim, M. and Kim, Y. 2019. A scalable and hybrid intrusion detection system based on the convolutional-LSTM network. *Symmetry*, 11(4): 583–598.

[5] Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P. and Venkatraman, S. 2019. Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7: 41525–41550.

[6] Ferrag, M.A., Maglaras, L., Moschoyiannis, S. and Janicke, H. 2020. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50: 102419–102435.

[7] Shone, N., Ngoc, T.N., Phai, V.D. and Shi, Q. 2018. A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1): 41–50.

[8] Buczak, A.L. and Guven, E. 2016. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2): 1153–1176.

[9] Moustafa, N. and Slay, J. 2016. The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset. *Information Security Journal*, 25(1–3): 18–31.

[10] Alazab, M., Venkatraman, S., Watters, P. and Alazab, M. 2012. Zero-day malware detection based on supervised learning algorithms of API call signatures. *Proceedings of the Ninth Australasian Data Mining Conference*, 171–182.

[11] Zhang, Y., Chen, X., Guo, D., Song, M. and Teng, Y. 2018. A novel intrusion detection method based on deep learning. *Future Generation Computer Systems*, 86: 1172–1181.

[12] Yin, C., Zhu, Y., Fei, J. and He, X. 2017. A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, 5: 21954–21961.

[13] Javaid, A., Niyaz, Q., Sun, W. and Alam, M. 2016. A deep learning approach for network intrusion detection system. *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies*, 21–26.

[14] Aldweesh, A., Derhab, A. and Emam, A.Z. 2017. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 189: 105124–105139.

[15] Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y. and Gan, D. 2018. Cloud-based cyber-physical intrusion detection for vehicles using deep learning. *IEEE Access*, 6: 3491–3508.