International Journal of Electrical and Electronics Engineers
Volume 18, Issue No. 01, Jan-June 2026
ISSN (0) 2321-2055 ISSN (P) 2321-2045

CNN-Based Intrusion Detection for IoT Botnet Traffic

K. Nandini, N. Bhuvaneswari, Sk. Mohaseen Sulthana, K. Gopi
Department of Electronics & Communication Engineering
Tirumala Engineering College, Narasaraopet, India

***Abstract*—The rapid growth of Internet of Things (IoT) devices has significantly transformed modern communication systems by enabling seamless connectivity among billions of devices across various domains such as healthcare, smart cities, industrial automation, and smart homes. However, this rapid expansion has also introduced critical security challenges, particularly due to the increasing prevalence of botnet attacks that exploit vulnerable IoT devices. These attacks can lead to large-scale network disruptions, unauthorized access, data breaches, and degradation of system performance.**

Traditional intrusion detection systems, which rely on rule-based or signature-based approaches, are often ineffective in detecting modern and evolving threats due to their inability to adapt to dynamic network environments. In addition, the heterogeneous nature and high volume of IoT network traffic make it difficult for conventional methods to achieve accurate and real-time detection.

To address these challenges, this paper proposes a Convolutional Neural Network (CNN)-based intrusion detection system designed for analyzing IoT network traffic and detecting botnet attacks. The proposed system includes multiple stages such as data collection, preprocessing, feature extraction, and classification using a 1D-CNN model. The CNN architecture enables automatic feature learning and efficient classification of network traffic without the need for manual feature engineering.

Experimental results demonstrate that the proposed model achieves high accuracy, precision, recall, and F1-score in detecting various types of botnet attacks. The system also shows strong generalization capability and robustness when applied to complex network traffic patterns. Therefore, the proposed approach provides an effective, scalable, and reliable solution for enhancing IoT network security in real-time environments.

***Index Terms*—IoT, Botnet Detection, CNN, Deep Learning, Intrusion Detection**

I. Introduction

The Internet of Things (IoT) has emerged as one of the most rapidly growing technologies, connecting billions of devices such as sensors, cameras, smart appliances, and industrial systems. These devices enable automation and real-time communication across multiple domains, including healthcare, transportation, agriculture, and smart cities. However, the increasing number of connected devices has significantly expanded the attack surface, making IoT networks highly vulnerable to cyber threats.

One of the major security concerns in IoT environments is the presence of botnet attacks, where compromised devices are controlled remotely by attackers to perform malicious activities such as Distributed Denial of Service (DDoS), data theft, and unauthorized access [1]. These attacks are particularly dangerous because they can operate silently without affecting the normal functionality of devices, making detection difficult.

Traditional intrusion detection systems rely on rule-based or signature-based approaches, which are not effective in detecting new and evolving threats. These systems also struggle to process the large volume of heterogeneous data generated by IoT devices. As a result, there is a need for intelligent detection mechanisms that can automatically learn patterns and identify anomalies in network traffic.

Machine learning and deep learning techniques have been widely adopted to address these challenges. Conventional machine learning models require manual feature extraction and are limited in handling complex data patterns [2], [3]. In contrast, deep learning models such as Convolutional Neural Networks (CNNs) are capable of automatically extracting hierarchical features and identifying hidden relationships in data [4].Recent advancements in IoT technologies have significantly increased the scale and complexity of network traffic, making traditional security mechanisms inadequate. The diversity of IoT devices and communication protocols further complicates the detection of malicious activities. As highlighted in [5], [6], modern intrusion detection systems must be capable of handling heterogeneous data and adapting to evolving attack patterns.

Moreover, botnet attacks such as Mirai and Bashlite have demonstrated the ability to exploit weakly secured IoT devices and launch large-scale distributed attacks. These attacks generate complex traffic patterns that are difficult to detect using conventional techniques. Deep learning models, particularly CNNs, have proven effective in identifying such patterns due to their ability to learn hierarchical feature representations [4], [7].

In addition, the increasing demand for real-time detection requires models that are both accurate and computationally efficient. CNN-based models provide a balance between performance and efficiency, making them suitable for deployment in IoT environments [8]. In recent years, the rapid evolution of IoT ecosystems has significantly increased the volume, velocity, and variety of network traffic. This growth makes traditional monitoring techniques insufficient for identifying sophisticated cyber threats. IoT devices often operate in distributed and heterogeneous environments, where security mechanisms are limited due to hardware constraints.

Furthermore, the increasing adoption of smart devices in critical applications such as healthcare and industrial automa-

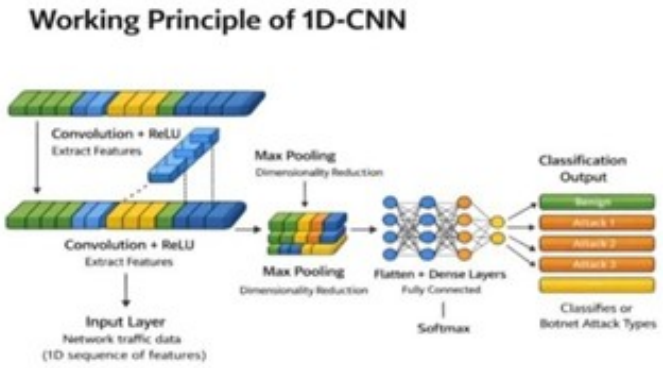

Fig. 1. Working Principle of 1D-CNN

tion raises serious concerns regarding data privacy and system integrity. Attackers exploit vulnerabilities in IoT devices to form botnets, which can be used for large-scale coordinated attacks. These attacks not only disrupt services but also compromise sensitive data.

Therefore, there is a strong need for intelligent and adaptive intrusion detection systems that can analyze complex traffic patterns and respond to evolving threats in real time. Deep learning-based approaches provide promising solutions to address these challenges by enabling automatic feature extraction and improved detection accuracy.

The working principle of the proposed CNN model is illustrated in Fig. 1. The model processes input data through convolutional layers, pooling layers, and fully connected layers to perform classification. As shown in Fig. 1, the CNN architecture enables automatic feature extraction and improves detection accuracy. The model is capable of handling large-scale data and adapting to variations in network traffic, making it suitable for real-time intrusion detection in IoT environments.

II. Related Work

Indoor intrusion detection and IoT botnet detection have been widely studied using various machine learning and deep learning techniques [8]. Early approaches focused on traditional machine learning algorithms such as decision trees and support vector machines, which require manual feature engineering and are limited in scalability.

Recent studies have explored deep learning models, particularly CNN-based approaches, due to their ability to automatically extract meaningful features from raw data [7]. The N-BaIoT dataset has become a standard benchmark for evaluating intrusion detection systems because it contains realistic IoT traffic data under both normal and attack conditions [1].

Hybrid models such as CNN-LSTM have been proposed to improve detection performance by combining spatial and temporal features [9]. However, these models often require higher computational resources and longer training time.

In addition, researchers have focused on improving system efficiency and scalability [10]. Recent advancements also include the development of lightweight models for real-time IoT environments [5]. Despite these improvements, challenges such as computational complexity and limited generalization capability remain.Several comparative studies have demonstrated that deep learning-based approaches outperform traditional machine learning methods in detecting IoT botnet attacks. In [3], various models were evaluated on the N-BaIoT dataset, where CNN-based approaches achieved higher accuracy and better generalization.

Furthermore, lightweight deep learning models have been proposed to address the resource constraints of IoT devices. These models aim to reduce computational complexity while maintaining detection performance [10]. However, achieving a balance between accuracy and efficiency remains a key challenge. Recent research also focuses on hybrid architectures that combine multiple learning techniques to improve detection capability. Despite these advancements, there is still a need for scalable and robust models that can handle diverse attack scenarios in real-world IoT environments [6]. Existing research in IoT security has explored various machine learning and deep learning techniques for intrusion detection. Traditional approaches rely on handcrafted features, which require domain expertise and may not generalize well across different datasets. Recent studies have focused on deep learning models due to their ability to automatically learn feature representations from raw data. Convolutional Neural Networks (CNNs) have been widely used for classification tasks, while Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are used for sequential data analysis.

In addition, hybrid models combining CNN and LSTM have been proposed to capture both spatial and temporal dependencies in network traffic. However, these models often require higher computational resources, making them less suitable for real-time IoT environments. Despite these advancements, challenges such as scalability, computational efficiency, and adaptability to new attack types remain open research problems.

III. System Architecture

The overall architecture of the proposed system is designed to efficiently capture, process, and classify IoT network traffic. The workflow of the system is illustrated in Fig. 2.

The system begins with the collection of network traffic generated by IoT devices. The captured data includes various attributes such as packet size, protocol type, and communication patterns. These features are essential for identifying anomalies in network behavior.

The collected data undergoes preprocessing steps such as normalization, cleaning, and labeling to improve data quality and consistency. Feature extraction techniques are then applied to identify relevant attributes that contribute to accurate classification.

The processed data is fed into the CNN model, which performs multiclass classification to detect different types of botnet attacks. The architecture is designed to be scalable and capable of handling large volumes of data in real-time environments. Each stage of the proposed architecture plays a

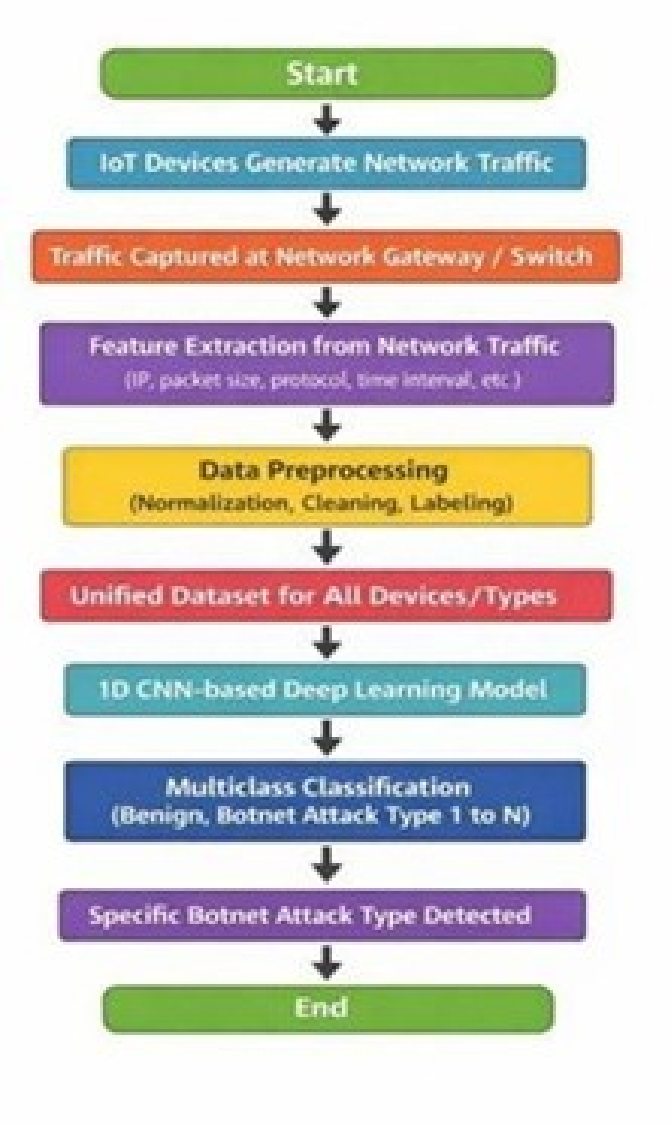

Fig. 2. Proposed Methodology

critical role in ensuring accurate intrusion detection. The data collection stage captures real-time traffic from IoT devices, providing a comprehensive view of network behavior. This is followed by preprocessing, which removes noise and ensures data consistency.

Feature extraction is a crucial step that identifies meaningful attributes from raw network traffic. These features help the model distinguish between normal and malicious patterns. According to [7], effective feature extraction significantly improves classification accuracy.

The classification stage utilizes a CNN model that learns complex patterns from the input data. The use of convolutional layers enables automatic feature learning, while pooling layers reduce computational complexity. This architecture allows the system to efficiently process large-scale data and detect various types of botnet attacks.

Overall, the integration of these stages creates a robust pipeline that enhances detection accuracy and system performance [4], [8].

IV. Implementation

The system is implemented using Python along with TensorFlow and Keras frameworks. These tools provide efficient platforms for developing deep learning models.

The dataset is preprocessed using normalization and cleaning techniques to remove noise and improve data quality. The CNN model is trained using labeled data and optimized using appropriate loss functions and optimization algorithms. The implementation of the proposed system focuses on achieving both accuracy and efficiency. The use of TensorFlow and Keras frameworks enables the development of scalable and optimized deep learning models. These frameworks provide support for parallel processing and efficient memory utilization.

During training, the model learns from labeled data and adjusts its parameters using optimization algorithms such as Adam. Proper tuning of hyperparameters plays a significant role in improving model performance.

In addition, techniques such as data normalization and regularization are applied to prevent overfitting and improve generalization. According to [2], preprocessing techniques significantly influence the performance of machine learning models in intrusion detection systems.

The implementation also ensures that the model can be deployed in real-time environments with minimal latency, making it suitable for practical IoT applications [5]. The implementation phase focuses on building an efficient and scalable model using modern deep learning frameworks. The use of Python, TensorFlow, and Keras provides flexibility in designing and training the CNN model.

The dataset is preprocessed to ensure that all features are normalized and labeled correctly. This step is crucial for improving model performance and reducing training time.

The CNN model is trained using multiple epochs, and its performance is monitored using validation data. Hyperparameters such as learning rate, batch size, and number of filters are tuned to achieve optimal results.

Additionally, techniques such as dropout and regularization are applied to prevent overfitting and improve generalization. The implementation ensures that the model can be deployed in real-time systems with minimal latency.

A. Performance Metrics

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

$$F1 = \frac{2(Precision \times Recall)}{Precision + Recall} \tag{4}$$

These metrics are used to evaluate the performance of the proposed model.

V. Results and Discussion

The performance of the proposed system is evaluated using multiple metrics including accuracy, confusion matrix, and loss analysis.

The accuracy graph shown in Fig. 3 illustrates the learning behavior of the model across training epochs.

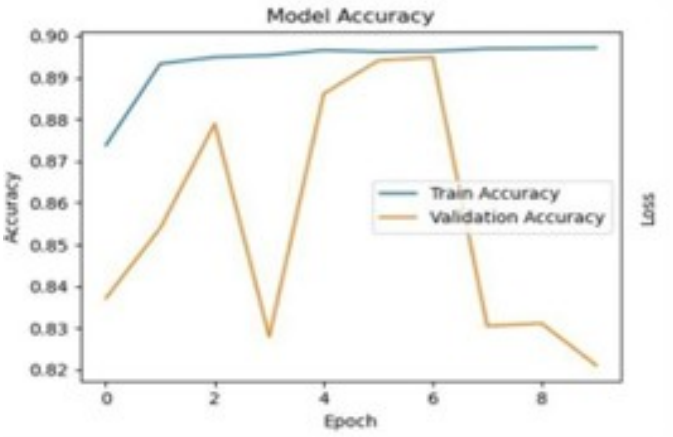

Fig. 3. Model Accuracy

The confusion matrix presented in Fig. 4 provides a detailed comparison between actual and predicted classes.

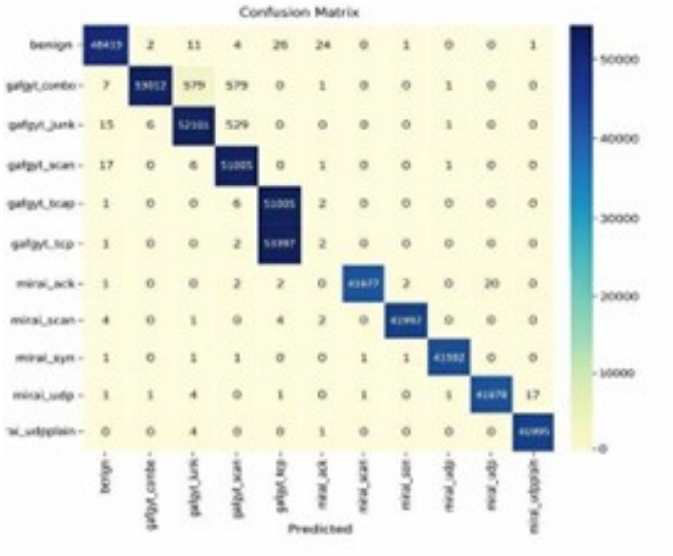

Fig. 4. Confusion Matrix

The loss graph shown in Fig. 5 indicates the convergence behavior of the model.

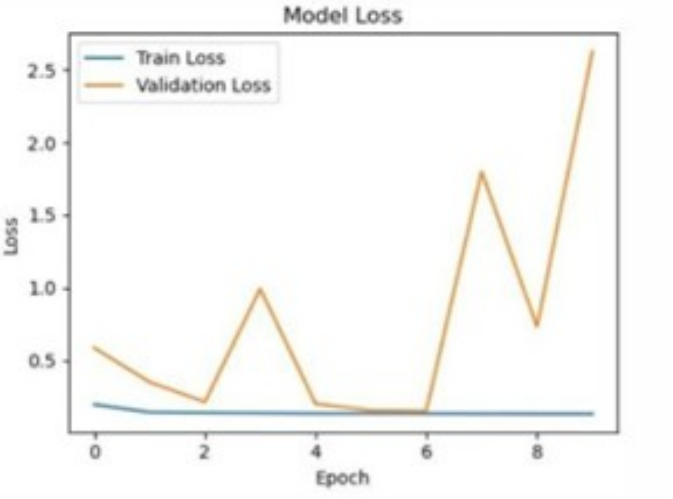

Fig. 5. Model Loss

The performance metrics summarized in Fig. 6 highlight the effectiveness of the model.

PERFORMANCE METRICS	PROPOSED METHADOLOGY
Precision	92%
Recall	89%
F1-Score	91%

Fig. 6. Performance Metrics

The results obtained from the experiments demonstrate the effectiveness of the proposed CNN-based model in detecting IoT botnet attacks. The accuracy graph shows consistent improvement during training, indicating stable learning behavior.

The confusion matrix provides detailed insights into classification performance, showing that the model accurately distinguishes between different attack types with minimal misclassification. This highlights the robustness of the model in handling complex traffic patterns.

The loss graph indicates proper convergence, confirming that the model is well-trained and does not suffer from overfitting. Similar observations have been reported in [3], [7], where CNN-based models achieved high performance on IoT datasets.

Overall, the experimental results validate that the proposed system provides reliable and efficient detection of botnet attacks in IoT environments.

Overall, the results demonstrate that the proposed system provides accurate and reliable detection of IoT botnet attacks.

VI. Conclusion

This paper presented a CNN-based intrusion detection system for IoT botnet traffic. The proposed model achieves high

accuracy and provides a scalable solution for IoT security. Future work includes real-time deployment and further optimization. The proposed system demonstrates the potential of deep learning techniques in improving IoT security. By leveraging CNN-based models, the system effectively detects complex attack patterns and provides high accuracy.

Future research can focus on integrating real-time monitoring systems and deploying the model in edge devices. Additionally, exploring hybrid models and optimization techniques can further enhance detection performance.

REFERENCES

[1] Z. Al-Othman, M. Alkasassbeh, *et al.*, "An efficient approach to detect iot botnet attacks using machine learning," *Journal of High Speed Networks*, 2020.

[2] A. Alaei and U. Pal, "Hybrid feature-based signature verification approach," in *International Conference on Document Analysis and Recognition (ICDAR)*, 2015.

[3] M. Hossain, R. A. M. Rudro, *et al.*, "Machine learning approaches for detecting iot botnet attacks: A comparative study of n-baiot dataset," in *IEEE Decision Aid Sciences and Applications Conference*, 2024.

[4] H. Gandhi, M. Mehra, V. J. Ribeiro, *et al.*, "Bond: Efficient and frugal dl model co-design for botnet detection on iot gateways," in *AI-ML Systems Conference*, 2021.

[5] K. P. Kumar, V. Madhava, *et al.*, "Comprehensive intrusion detection for investigating network traffic and botnet attacks," *International Journal of Engineering Research & Science Technology*, 2024.

[6] A. Rasool, N. S. Safa, *et al.*, "Exploring machine learning approaches for botnet detection in iot networks," in *International Conference on Green Sustainable Systems and Sciences*, 2025.

[7] N. E. Majd and D. S. K. R. Gudipelly, "Iot botnet classification using cnn-based deep learning," in *IEEE International Performance, Computing and Communications Conference (IPCCC)*, 2023.

[8] H. Chunduri, T. G. Kumar, *et al.*, "A multi-class classification for detection of iot botnet malware," in *International Conference on Computing Science, Communication and Security*, 2021.

[9] Y. Meidan, M. Bohadana, *et al.*, "N-baiot: Network-based detection of iot botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, 2018.

[10] C. Kunndra *et al.*, "Cnn-lstm: A deep learning model to detect botnet attacks in iot," in *International Conference on Cryptology and Network Security*, 2022.