International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

IOT Attack Detection Using Hybrid Deep Learning with Attention Mechanism

Mr. A. D. Talole[1], Riya Mahesh Wani[2], Pooja Ravindra Kankhar[3], Pradnya Rahul Gangurde[4], Shreya Sharad Nile[5]

[1.]Lecturer, Computer Technology, K. K. Wagh Polytechnic, Nashik
[2.]Student, Computer Technology, K. K. Wagh Polytechnic, Nashik
[3.]Student, Computer Technology, K. K. Wagh Polytechnic, Nashik
[4.]Student, Computer Technology, K. K. Wagh Polytechnic, Nashik
[5.]Student, Computer Technology, K. K. Wagh Polytechnic, Nashik

---

Abstract - The rapid proliferation of Internet of Things (IoT) networks has transformed modern society by enabling smart cities, healthcare systems, industrial automation, and intelligent homes through large-scale connectivity and real-time data exchange. However, this unprecedented growth has also widened the attack surface, making IoT devices highly vulnerable to cyberattacks such as denial of service, probing, information theft, and other advanced threats that can compromise device integrity, disrupt services, and expose sensitive information. These challenges are further compounded by the inherent limitations of IoT devices, including constrained computational resources, lack of standardized security protocols, and the diversity of communication technologies, which make them difficult to secure using conventional techniques. Traditional intrusion detection systems (IDS) and classical machine learning approaches have shown limited effectiveness in addressing these issues, as they often fail to capture complex traffic patterns, adapt to dynamic environments, and maintain low false positive rates in real-world conditions. To overcome these shortcomings, this project proposes a hybrid deep learning-based intrusion detection framework that integrates multiple complementary neural network architectures to enhance detection accuracy, scalability, and adaptability. In the proposed framework, Convolutional Neural Networks (CNN) are employed for spatial feature extraction from network traffic, Logistic Regression for balancing the Imbalanced IOT data. Furthermore, an attention mechanism is embedded within the model to dynamically highlight the most relevant features, improving interpretability and ensuring that the system focuses on patterns strongly associated with malicious activity. The framework is trained and validated using the widely recognized UNSW-NB15 dataset, which contains diverse attack scenarios and allows the model to generalize effectively to multiple categories of threats. Experimental evaluations demonstrate that the proposed hybrid architecture achieves superior performance compared to baseline IDS models, consistently delivering high accuracy, precision, recall, and F1-score while significantly reducing false positives. For practical implementation, the system is developed in Jupyter Notebook for model training and deployed using Flask, providing a user friendly web-based interface for real-time intrusion detection. This deployment enables network administrators and security professionals to input traffic data and receive immediate threat assessments, supporting rapid response to potential cyber incidents and reducing overall downtime.

Keywords: CNN (Convolutional Neural Networks), LR (Logistic Regression), Attention Mechanism, UNSW-NB15 dataset, Internet of Things (IoT), Intrusion Detection System (IDS), Threat Intelligence, Hybrid Deep Learning, Cybersecurity.

1.INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most transformative technologies of the modern era, enabling the interconnection of billions of devices that communicate and exchange data with minimal human intervention. From smart homes and wearable health monitors to industrial automation and intelligent transportation systems, IoT technology is now deeply integrated into daily life and critical infrastructure. This hyper-connectivity brings numerous benefits such as increased efficiency, automation, and data-driven decision-making. However, the very openness and interconnectedness that make IoT so powerful also render it highly vulnerable to a variety of cyber security threats. Among these threats, botnet attacks represent a particularly dangerous and rapidly evolving category. A

botnet is a network of compromised devices that are remotely controlled by an attacker to perform malicious activities such as Distributed Denial-of-Service (DDoS) attacks, Denial-of-Service (DOS) attacks, Reconnaissance attacks, spam distribution, data theft, and network disruption. In IoT environments, devices often have limited processing power, weak authentication mechanisms, and lack of regular security updates, making them easy targets for attackers. Once infected, these devices can be silently manipulated to participate in large scale attacks, posing risks to privacy, data integrity, and system availability. Notable botnet incidents, such as the Mirai botnet attack of 2016, demonstrated how vulnerable IoT ecosystems can be and how devastating the consequences of such attacks are for individuals, organizations, and even national infrastructure. Traditional intrusion detection systems (IDS) often struggle to address IoT botnet threats effectively. Conventional rule-based or signature-based methods fail to detect zero-day attacks or adapt to new attack patterns. The dynamic and heterogeneous nature of IoT traffic further complicates the detection process. In recent years, machine learning and, more importantly, deep learning techniques have shown significant promise in analyzing complex network traffic data, learning patterns of normal and malicious behavior, and detecting intrusions in real time. This project proposes a hybrid deep learning approach to detect IoT botnet attacks with high accuracy and low false alarm rates. The system combines Convolutional Neural Networks (CNN), Logistic Regression (LR) enhanced with an attention mechanism. The CNN is utilized to extract spatial features from network traffic data, LR is used for classifying network traffic or device behavior as normal or malicious using input features (like packet size, connection duration), while the attention mechanism selectively focuses on the most relevant features to improve classification performance. This stacked model architecture ensures robust detection of both known and emerging attack types. The model is trained and tested using the UNSW-NB15 dataset, a comprehensive benchmark dataset for network intrusion detection research. By leveraging hybrid deep learning, the system can handle large-scale IoT traffic data and adapt to complex variations in attack behavior. Furthermore, the proposed system is deployed via a Flask-based web interface, allowing realtime intrusion detection and instant feedback to users. The web interface enables network administrators to input live or recorded network traffic data and receive immediate predictions regarding potential botnet activity. This work addresses the urgent need for intelligent, adaptive, and real-time IoT botnet attack detection systems. By integrating multiple deep learning architectures with attention mechanism, this approach not only enhances detection accuracy but also ensures resilience against evolving threats in an increasingly connected digital ecosystem.

2.LITERATURE SURVEY

1] A. Khang, et al., Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy, CRC Press, 2024.

This book explains how advanced IoT technologies support Industry 4.0 by integrating with AI, big data analytics, and cloud computing. It improves industrial automation and efficiency while highlighting challenges like scalability and cybersecurity, emphasizing secure communication and strong threat detection mechanisms.

2] X. Qu, et al., Mfgan: multimodal fusion for industrial anomaly detection using attention-based autoencoder and generative adversarial network, Sensors 24 (2) (2024) 637.

This paper proposes MFGAN, which combines attention-based autoencoders and GANs to detect industrial anomalies. By using multimodal data and attention mechanisms, it improves detection accuracy and robustness in complex industrial IoT environments.

3] M. Al-Fawa'reh, et al., MalBoT-DRL: Malware Botnet detection using deep reinforcement learning in IoT networks, IEEE Internet Things J. (2023).

This study introduces a deep reinforcement learning framework to detect malware botnet attacks in IoT networks. The model adapts to new attack strategies, achieves high accuracy, and reduces false positives.

4] J. Zhang, et al., Towards detection of zero-day botnet attack in IoT networks using federated learning, in: Proceedings of the ICC 2023-IEEE International Conference on Communications, IEEE, 2023.

This paper presents a federated learning-based approach for detecting zero-day botnet attacks. It preserves data privacy by training models across distributed devices and effectively identifies new and unknown threats in large-scale IoT environments.

3.METHODOLOGY:

Proposed System: The proposed system is a hybrid deep learning–based intrusion detection framework designed to detect IoT botnet attacks in real time with high accuracy. It combines Convolutional Neural Networks (CNN) for automatic spatial feature extraction and Logistic Regression (LR) for efficient classification of normal and malicious network traffic. CNN learns important patterns from the data, while Logistic Regression provides reliable binary prediction, improving overall detection performance.The model is trained and evaluated using the UNSW-NB15 dataset to ensure coverage of diverse attack types and normal traffic behavior. After training, the system is deployed through a Flask-based web application that allows network administrators to upload traffic data and receive instant predictions, enabling adaptive and real-time security for modern IoT environments.

The proposed IoT Botnet Detection System follows a systematic and structured methodology to design, develop, and deploy a hybrid deep learning-based intrusion detection framework. The methodology consists of the following Modules:

1.Data Collection Module

Collects IoT network traffic data from the UNSW-NB15 dataset as the primary source for training and evaluation. This dataset contains both normal and malicious traffic records, including botnet attack patterns.

2. Data Preprocessing Module

Cleans and formats the dataset by handling missing values, normalizing numerical features, encoding categorical variables, and selecting the most relevant features for efficient model training.

3. Feature Extraction Module

Uses CNN layers to extract spatial features from the preprocessed data, preparing meaningful feature representations for classification. Logistic Regression (LR) then uses these extracted features to perform intelligent decision-making for traffic classification.

4. Model Training Module (CNN + LR)

Integrates CNN for feature extraction and Logistic Regression (LR) for final classification. The model is trained on labeled data and parameters are optimized to achieve the best detection performance.

5. Attack Detection & Classification Module

Classifies incoming network traffic as either benign or malicious using the trained CNN + Logistic Regression model, ensuring accurate detection of IoT botnet attacks.

6. Web Application Deployment Module

Implements the trained CNN + LR model into a Flask-based web interface, allowing real-time detection where users can upload or input network traffic data and receive instant predictions.

7. Testing & Evaluation Module

Validates system performance using metrics such as accuracy, precision, recall, F1-score, and confusion matrix, and fine-tunes the model based on testing results

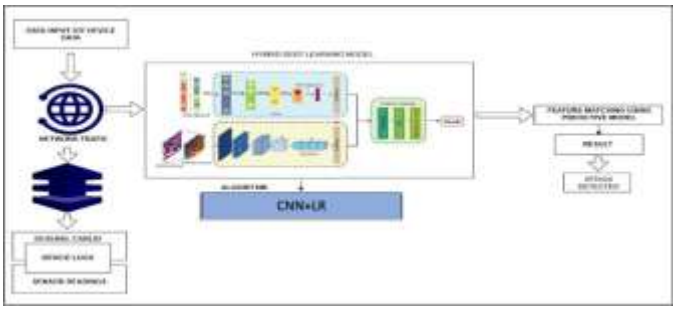

Figure 1. System Architecture

4. RESULT:

The proposed hybrid deep learning model (CNN + LSTM/RNN with Attention) trained on the UNSW-NB15 dataset achieved high accuracy, precision, recall, and F1-score in detecting botnet attacks.

The system:

- Correctly classifies network traffic as Normal or Botnet Attack
- Reduces false positives
- Detects complex and zero-day attacks
- Provides real-time prediction using Flask

Overall, the system performs efficiently and provides a reliable, real-time IoT botnet detection solution.

5. APPLICATIONS:

1. Smart Home Security – Detecting and preventing botnet attacks on smart appliances, cameras, and connected home automation systems.

2. Industrial IoT Protection – Securing manufacturing plants, sensors, and industrial control systems from malicious intrusions.
3. Healthcare IoT Networks – Protecting medical devices, patient monitoring systems, and hospital networks from cyber threats.
4. Smart City Infrastructure – Safeguarding traffic control systems, energy grids, and public surveillance from botnet disruptions.
5. Telecommunication Networks – Detecting and mitigating botnet-based DDoS attacks targeting IoT-enabled communication systems.

6. CONCLUSIONS

The proposed hybrid deep learning–based botnet detection system provides an efficient and intelligent solution for securing IoT networks against evolving cyber threats. By integrating CNN for spatial feature extraction and Logistic Regression (LR) for classification, the system achieves high accuracy and reliable real-time intrusion detection using the UNSW-NB15 dataset. The deployment through a Flask-based web interface ensures user-friendly operation and practical applicability. Overall, the system enhances network security, reduces response time to threats, and offers a scalable and robust framework for protecting IoT environments from sophisticated botnet attacks.

7. REFERENCES

1]. Khang, et al., Advanced Iot Technologies and Applications in the Industry 4.0 Digital Economy, CRC Press, 2024.

2] X. Qu, et al., Mfgan: multimodal fusion for industrial anomaly detection using attention-based autoencoder and generative adversarial network, Sensors 24 (2) (2024) 637.

3] A. Al-Obaidi, A Ibrahim, A.M. Khaleel, The Effectiveness of Deploying Machine Learning Techniques in Information Security to Detect Nine Attacks: UNSW-NB15 Dataset as A Case Study (2023).

4] S. Hamzenejadi, M. Ghazvini, S. Hosseini, Mobile detection: a comprehensive survey, Int. J. Inf. Secure. 22 (1) (2023) 137–175.

5] M. Al-Fawa'reh, et al., MalBoT-DRL: Malware detection using deep reinforcement learning in IoT networks, IEEE Internet Things J. (2023).

6] S.S. Silva, et al., Botnets: a survey, Comput. Netw. 57 (2) (2013) 378–403.

7] J. Zhang, et al., towards detection of zero-day attack in iot networks using federated learning. in: Proceedings of the ICC 2023-IEEE International Conference on Communications, IEEE, 2023.

8] A. Darem, Anti-phishing awareness delivery methods, Eng., Technol. Appl. Sci. Res. 11 (6) (2021) 7944–7949.

9] N. Koroniotis, N. Moustafa, J. Slay, A new Intelligent Satellite Deep Learning Network Forensic framework for smart satellite networks, Comput. Electr. Eng. 99 (2022) 107745.

10] K. Geetha, S. Brahmananda, Network traffic analysis through deep learning for detection of an army of bots in health IoT network, Int. J. Pervasive Comput. Commun. (2022).