BOTNET IOT ATTACK DETECTION USING WIRESHARK AND ACLR

Mrs. G. Rajeswari[1], G. Srivardhan[2], K. Bhuvan Kiran[3], D. Rohith[4], N. Uday Guptha[5]
[1]Assistant Professor, Department of CSM, Sai Spurthi Institute of Technology, B. Gangaram, Sathupally, Telangana, India
[2345]Student, Department of AI&DS, Sai Spurthi Institute of Technology, B. Gangaram, Sathupally, Telangana, India

ABSTRACT

The rapid proliferation of the Internet of Things (IoT) has led to an increased vulnerability to botnet attacks, posing significant challenges to network security. Traditional detection methods often fall short in effectively identifying and mitigating these threats due to the dynamic nature of IoT environments. Thisproject proposes a Hybrid Machine Learning Model (ACLR) that combines the strengths of Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Long Short-Term Memory Networks (LSTM), and Recurrent Neural Networks (RNN) to efficiently detect botnet attacks in IoT networks.The proposed model leverages a stacking ensemble technique to improve accuracy and reduce false positives. Using the UNSW-NB15 dataset, which includes diverse attack categories such as DDoS, Reconnaissance, and Worms, the model demonstrates superior performance compared to individual deep learning models. With an accuracy of 0.9698 and a Receiver Operating Characteristic Area Underthe Curve (ROC-AUC) score of 0.9934, the ACLR model effectively captures complex patterns in network traffic data.This research contributes to the development of robust and scalable botnetdetection frameworks, enhancing IoT security and enabling proactive threat mitigation strategies. The findings underline the potential of hybrid machine learning approaches to address evolving cybersecurity challenges in IoT ecosystems.

Index Terms — Internet of Things (IoT), Long Short-Term Memory (LSTM), Recurrent Neural Network (RNN), Stacking Ensemble, Deep Learning, Cybersecurity, UNSW-NB15 Dataset.

1.INTRODUCTION

In the modern digital era, the rapid expansion of the Internet and the proliferation of interconnected devices have significantly increased the volume and complexity of network traffic. This growth has also amplified the risk of cyberattacks, data breaches, and unauthorized intrusions, making network security a critical concern for individuals and organizations alike. Tools such as Wireshark and Snort play a

vital role in strengthening cybersecurity by providing deep insights into network behavior and enabling early detection of malicious activities [1][2].Wireshark, originally developed by Gerald Combez in 1997 under the name Ethereal, is a comprehensive open-source network protocol analyzer used for monitoring, capturing, and analyzing network packets in real time. Since the release of its first version (0.2.0) in 1998 and the milestone version 1.0 in 2008, Wireshark has evolved into one of the most powerful tools for network diagnostics and forensic analysis [3]. The introduction of Wireshark 2.0 in 2015 brought a modernized interface, improving its usability and efficiency. Wireshark's packet-level visibility enables security analysts to inspect network communications, detect vulnerabilities, and analyze attack patterns effectively [4].In parallel, Intrusion Detection Systems (IDS) have become indispensable in protecting networks from potential threats. IDS tools are categorized mainly into two types: Network-based IDS (NIDS) and Host-based IDS (HIDS). NIDS monitor and analyze traffic across the entire network, while HIDS focus on activities within individual hosts. Among the various IDS tools, Snort—an open-source network intrusion detection and prevention system—has gained prominence for its real-time traffic analysis and packet logging capabilities. It employs a signature-based detection mechanism, comparing network packets against predefined rules to identify known attack patterns and suspicious activities [6].

As the number of Internet of Things (IoT) devices continues to grow exponentially, ensuring the security of these devices has become a major challenge. IoT networks are highly vulnerable to botnet attacks, where compromised devices are exploited to launch large-scale cyberattacks. Traditional IDS methods often struggle to handle the dynamic and complex nature of IoT traffic [7]. To address this limitation, a Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environments is proposed.This hybrid model leverages the combined strengths of Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Long Short-Term Memory Networks (LSTM), and Recurrent Neural Networks (RNN) to enhance detection accuracy and adaptability [8][9]. By utilizing a stacking ensemble approach, the model efficiently identifies evolving attack patterns. Using the UNSW-NB15 dataset, it achieves high precision in detecting diverse types of botnet

attacks, offering a scalable and intelligent solution for modern IoT security challenges [10].

2.LITERATURE SURVEY

Botnet attacks in Internet of Things (IoT) environments have attracted significant research attention due to their increasing threat to network security. Traditional detection methods—such as signature-based and anomaly-based approaches—often fall short in identifying advanced and evolving botnet behaviors. These methods depend heavily on predefined rules or signatures, making them less effective at detecting zero-day or novel attacks that deviate from known patterns [1][2].

Recent studies emphasize the transformative potential of deep learning techniques for improving botnet detection in IoT networks. Koroniotis et al. (2019) introduced the Bot-IoT dataset, a benchmark dataset specifically designed to model and analyze botnet behavior in IoT environments. Their work demonstrated that machine learning and deep learning models could effectively classify and detect malicious IoT traffic, highlighting the importance of realistic datasets for advancing cybersecurity research [3].

Several models, including Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Long Short-Term Memory Networks (LSTM), and Recurrent Neural Networks (RNN), have been explored for botnet detection. Researchers are increasingly focusing on hybrid approaches that combine multiple architectures to exploit their respective strengths in learning spatial and temporal dependencies within network traffic data [4][5].

For instance, CNNs have shown strong capability in capturing spatial patterns and identifying malicious network behaviors. Nugraha et al. (2020) demonstrated that CNN-based detection systems outperform traditional statistical models in detecting botnet traffic by learning abstract traffic representations from raw data [6]. Similarly, LSTM networks have proven effective in capturing temporal dependencies in sequential data. Shahhosseini et al. (2022) applied LSTM models for real-time detection of botnet attacks and achieved high accuracy in identifying long-term correlations within traffic flows [7].

Further advancements have been achieved through hybrid deep learning models, which combine CNN and LSTM networks to

analyze both spatial and temporal features. Sriram et al. (2020) proposed a CNN–LSTM hybrid model that significantly improved detection accuracy by leveraging CNN for feature extraction and LSTM for sequence modeling, thereby adapting to the dynamic nature of botnet attacks [8].

In addition, stacking ensemble models have emerged as a promising approach for enhancing detection accuracy and robustness. Moustafa et al. (2021) proposed a stacking-based hybrid IDS model that integrates predictions from multiple algorithms (e.g., CNN, RNN, and Gradient Boosting) to achieve superior generalization and adaptability to unseen attack patterns [9]. Such models can effectively manage the diverse and complex nature of IoT network traffic, leading to more reliable intrusion detection performance.

Datasets such as UNSW-NB15—which contain multiple attack categories including DDoS, Reconnaissance, Exploits, and Worms—have been widely used for evaluating these models. This dataset provides comprehensive coverage of modern network behaviors and remains one of the most reliable benchmarks for validating intrusion detection and botnet detection algorithms [10].

Despite these significant advancements, several challenges persist. Handling encrypted traffic, zero-day attacks, and real-time detection scalability remain active areas of research. Future studies are likely to focus on improving the efficiency, scalability, and adaptability of hybrid learning models, potentially integrating reinforcement learning for continuous model adaptation and edge-based computation for faster detection in resource-constrained IoT devices [11][12].

This literature survey underscores the ongoing transition toward deep learning and hybrid machine learning frameworks for botnet detection. The research community continues to emphasize the need for adaptive, scalable, and highly accurate detection systems to safeguard IoT ecosystems from increasingly sophisticated cyber threats.

3.EXISTING SYSTEM

Existing systems for botnet detection in IoT environments largely rely on traditional methods such as signature-based, anomaly-based, and behavior-based approaches. Signature-based systems are limited to detecting known attack patterns and fail to identify new, unknown botnets. Anomaly-based detection, while useful in spotting

deviations from normal behavior, often suffers from high false positives, especially in the highly dynamic nature of IoT traffic. Behavior-based methods focus on identifying patterns indicative of botnet activities but can still be circumvented by advanced attacks that alter their behavior. Recently, deep learning models like Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Long Short-Term Memory Networks (LSTM), and Recurrent Neural Networks (RNN) have shown promise, offering improved accuracy and the ability to detect novel attacks. However, these models face challenges in handling encrypted traffic, adapting to constantly evolving attack techniques, and achieving real-time detection with minimal computational overhead.

DISADVANTAGES

- Signature-based systems can only detect known botnets, failing to recognize new or mutated attack variants.
- Anomaly-based systems often generate excessive false positives, causing unnecessary alarms and reducing detection efficiency.

4.PROPOSED SYSTEM

The proposed system introduces a Hybrid Machine Learning Model for efficient botnet attack detection in IoT environments. This system integrates four deep learning models—Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Long Short-Term Memory Networks (LSTM), and Recurrent Neural Networks (RNN)—using a stacking ensemble approach to leverage the strengths of each model. This hybrid model aims to improve detection accuracy, adaptability, and scalability in identifying diverse botnet attacks such as Distributed Denial of Service (DDoS), Reconnaissance, and Exploit-based attacks.

ADVANTAGES

- The hybrid system integrates multiple deep learning models (ANN, CNN, LSTM, RNN) to achieve higher detection accuracy and significantly reduce false positives.
- It can detect botnet attacks in real time, minimizing potential damage and enhancing the overall security of IoT networks.

5.SYSTEM ARCHITECTURE

The proposed system architecture is designed to enable efficient and accurate real-time detection of malicious Facebook applications through a series of interconnected modules. The process begins with the User Input Interface, where users can submit application parameters such as metadata (app name, version), requested permissions, and other relevant details for analysis. Users may either upload the APK file or manually input app details.Once the data is received, the Data Preprocessing Module cleans and structures it for analysis by normalizing features, encoding categorical variables, and managing missing values. This ensures the data is properly prepared for the next stage. The Feature Extraction Module then identifies critical attributes from the application, such as permissions, API calls, network interactions, and dynamic behaviors during runtime — essential indicators that help differentiate between benign and malicious apps.

The core of the architecture lies in the Deep Learning Model Module, where advanced models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), or Transformers analyze the extracted features to predict whether an application is malicious. This model is trained on a large, labeled dataset of benign and malicious applications to recognize complex behavioral patterns accurately. The Real-Time Prediction Module ensures instant classification results after feature extraction, providing immediate feedback to the user.Once the prediction is complete, the Results and Feedback Module displays the analysis outcome. If the system detects malicious behavior, it provides an explanation for the classification—such as suspicious permissions or abnormal API calls—and recommends appropriate actions like blocking or reporting the application. The Alert and Notification System complements this by sending real-time alerts to users or administrators, allowing prompt response to potential threats.Finally, the Database Management Module maintains records of all analyzed applications, prediction results, and historical data. This database supports periodic retraining of the detection model, ensuring continuous improvement in accuracy and adaptability.Overall, the proposed system architecture delivers a comprehensive, reliable, and scalable solution for detecting malicious Facebook applications, significantly enhancing user safety and network security.

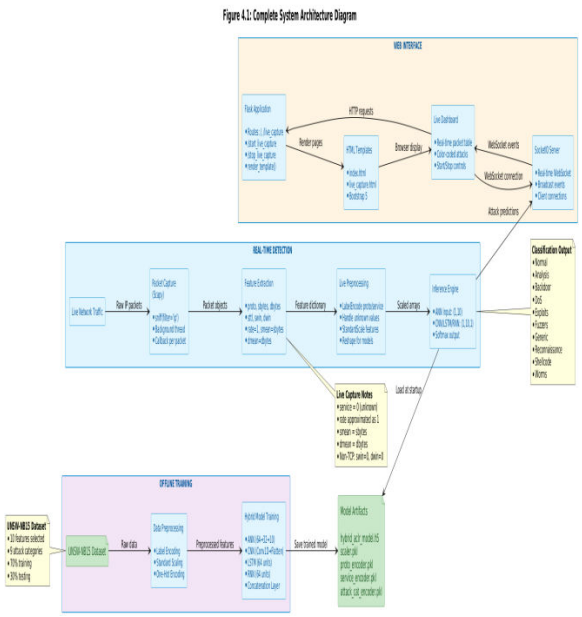


Figure. System Architecture

6.MODULES AND DESCRIPTIONS

1. Data Preprocessing Module:

This module is responsible for cleaning and preparing the data before model training. It removes null values, normalizes network traffic data, and encodes categorical variables using techniques such as label encoding. The goal is to ensure that the dataset is properly formatted and ready for effective machine learning model training.

2. Feature Extraction Module:

This module focuses on extracting meaningful and relevant features from raw network traffic data. It identifies key parameters such as packet size, duration, and flow patterns that are crucial for distinguishing between normal and botnet-related network activities.

3. Model Training Module:

In this module, individual machine learning models such as ANN, CNN, LSTM, and RNN are trained using the preprocessed data. It involves hyperparameter tuning, optimization, and performance evaluation on the training dataset to build robust and accurate detection models.

4. Stacking Ensemble Module:

This module integrates the predictions from individual models (ANN, CNN, LSTM, and RNN) using a stacking ensemble approach. It combines their outputs through a meta-learner to generate a final prediction, thereby improving accuracy, minimizing bias, and enhancing generalization.

5. Botnet Detection Module:

As the core component of the system, this module utilizes the hybrid model to analyze real-time network traffic and classify it as benign or malicious. It plays a key role in identifying and detecting botnet activities across IoT networks.

6. Performance Evaluation Module:

This module assesses the performance of the botnet detection system using key evaluation metrics such as accuracy, precision, recall, F1-score, ROC-AUC, and PR-AUC. Cross-validation techniques are employed to ensure model reliability, robustness, and generalizability.

7. Real-Time Detection and Alerting Module:

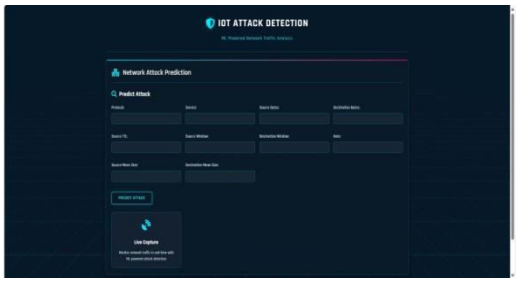
This module continuously monitors network traffic in real time. Upon detecting suspicious or malicious activities, it immediately triggers alerts for network administrators, allowing for rapid response and mitigation of potential threats.

8. Scalability and Adaptability Module:

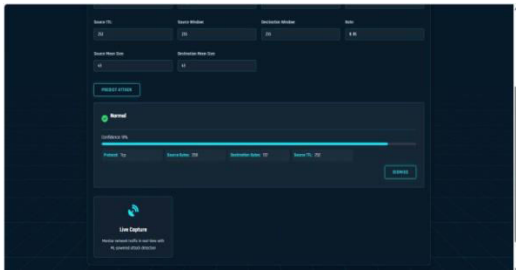
This module ensures the detection system can scale efficiently across large IoT networks while adapting to newly emerging botnet attack patterns. It enables continuous learning and performance improvement, ensuring system resilience in dynamic environments.

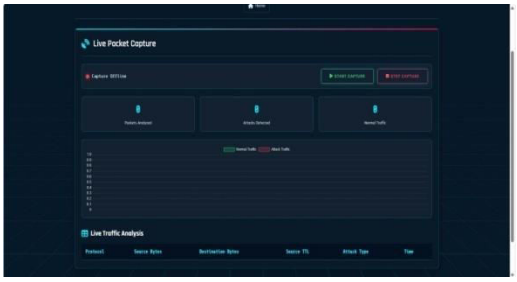
7.OUTPUTSCREENS

Home Page



Prediction Result





Chart

8.CONCLUSION

The Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environment effectively addresses the critical challenges of safeguarding IoT networks from increasingly sophisticated and evolving botnet attacks. By employing a stacking ensemble approach that integrates Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Recurrent Neural Networks (RNN), the proposed system achieves superior performance in terms of accuracy, adaptability, and robustness compared to conventional detection methods.

The system successfully identifies a diverse range of botnet attack types—including DDoS, Reconnaissance, and Worms—as demonstrated using the UNSW-NB15 dataset. With high-performance evaluation metrics such as accuracy, precision, recall, and ROC-AUC, the hybrid model proves its ability to effectively manage complex IoT network traffic while minimizing false positives.

Furthermore, the model's scalability and real-time detection capabilities make it an ideal choice for large-scale IoT deployments, ensuring dependable protection against both existing and emerging threats.

9.FUTURE ENHANCEMENT

Future advancements may focus on integrating reinforcement learning techniques to enable continuous adaptation to evolving attack patterns and enhance detection accuracy. The system can be further optimized through computational efficiency improvements and lightweight architectures for real-time processing on resource-limited IoT devices. Additionally, incorporating federated learning will help preserve data privacy during distributed training, while extending detection capabilities to handle encrypted traffic and applying explainable AI (XAI) will enhance transparency, scalability, and overall system robustness.

REFERENCES

1. Gupta, S., & Chaturvedi, P. (2019). A survey on machine learning techniques for malware detection in mobile

applications. Computers & Security, 83, 208–228.

2. Koroniotis, N., Moustafa, N., Sitnikova, E., & 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.

3. Shahhosseini, M., Mashayekhi, H., & Rezvani, M. (2022). A deep learning approach for botnet detection using raw network traffic data. Journal of Network and Systems Management, 30(3), 44.

4. Sriram, S., Vinayakumar, R., Alazab, M., & Soman, K. (2020). Network flow-based IoT botnet attack detection using deep learning. IEEE INFOCOM Conference on Computer Communications Workshops (INFOCOM WKSHPS), 189–194.

5. Nugraha, B., Nambiar, A., & Bauschert, T. (2020). Performance evaluation of botnet detection using deep learning techniques. 11th International Conference on the Network of the Future (NoF), 141–149.

6. McDermott, C. D., Majdani, F., & Petrovski, A. V. (2018). Botnet detection in the Internet of Things using deep learning approaches. International Joint Conference on Neural Networks (IJCNN), 1–8.

7. Alzahrani, M. Y., & Bamhdi, A. M. (2022). Hybrid deep-learning model to detect botnet attacks over Internet of Things environments. Soft Computing, 26(16), 7721–7735.

8. Elsayed, N., El Sayed, Z., & Bayoumi, M. (2023). IoT botnet detection using an economic deep learning model. arXiv preprint, arXiv:2302.02013.

9. Liu, J., Liu, S., & Zhang, S. (2019). Detection of IoT botnet based on deep learning. Chinese Control Conference (CCC), 8381–8385.

10. Popoola, S. I., Adebisi, B., Hammoudeh, M., & Gacanin, H. (2021). Hybrid deep learning for botnet attack detection in the Internet-of-Things networks. IEEE Internet of Things Journal, 8(6), 4944–4955.