Journals Pub

International Journal of
Broadband Cellular Communication

ISSN: 2455-8532
Volume 11, Issue 2, 2025
July–December
DOI (Journal): 10.37628/IJBCC

https://journalspub.com/journal/IJBCC/

Review IJBCC

Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environment

Jermina F.[1,*], Naveen A.[2], Dharaneeshwaran K.[2], Harish Kumar D.[2], Santhoshkumar P.[2]

Abstract

The rapid advancement and widespread adoption of internet technologies have led to a surge in cyber-attacks, with botnet attacks emerging as particularly detrimental. Identifying botnet activities is increasingly challenging due to the diverse attack vectors and the evolving nature of malware. As the Internet of Things continues to expand, network devices become more vulnerable to these sophisticated attacks, resulting in significant security breaches and financial losses. To tackle this issue, we suggest a hybrid machine learning model for efficient botnet detection in Internet of Things settings. This model utilizes a unique stacking technique that combines Artificial Neural Networks, Convolutional Neural Network, Long Short-Term Memory networks, and Recurrent Neural Networks into a unified system known as ACLR. When compared to other models, ours performs better, with a testing accuracy of 96.98%. A high Precision-Recall Area Under the Curve score of 0.9950 and a high Receiver Operating Characteristic Area Under the Curve score of 0.9934 demonstrate the ACLR model's superiority in botnet detection. Comparative analysis with existing state-of-the-art techniques highlights the effectiveness of the ACLR model in capturing the complex patterns of botnet activities, thereby offering a promising solution for enhancing cybersecurity measures in Internet of Things environments.

Keywords: Botnet detection, hybrid machine learning, artificial neural networks (ANN), convolutional neural networks (CNN), long short-term memory (LSTM), recurrent neural networks (RNN), Internet of Things (IoT), cybersecurity, receiver operating characteristic (ROC) curve, precision-recall (PR) curve

INTRODUCTION

Cyberattacks have increased because of the quick and extensive adoption of Internet technology, and botnets have become the primary destructive force because of the variety of attacks and the evolving nature of malware. It is getting harder to detect botnet activity. Devices in networks are more susceptible to these sophisticated attacks as the Internet of Things (IoT) grows, resulting in significant security breaches and financial losses. To tackle this issue, we suggest creating a hybrid machine learning framework to detect efficient botnets in IoT settings [1, 2].

One of the biggest cybersecurity risks in IoT environments is botnet attacks, which are distinguished by their complexity and variety of attack methods. Because the attackers' strategies are always evolving, traditional detection methods cannot keep up. Even though they work well on their own, current machine learning models frequently fall short of capturing the entire spectrum of botnet patterns and behaviors. This project suggests a hybrid machine learning model that can more effectively identify botnet attacks to bridge the gap between the growing complexity and scale of today's IoT networks. Cyberattacks have increased

***Author for Correspondence**
Jermina F.
E-mail: jermina.f@kce.ac.in

[1]Assistant Professor, Department of CSE (Cyber Security), Karpagam College of Engineering, Coimbatore, Tamil Nadu, India
[2]Student, Department of CSE (Cyber Security), Karpagam College of Engineering, Coimbatore, Tamil Nadu, India

Received Date: July 16, 2025
Accepted Date: July 18, 2025
Published Date: December 30, 2025

Citation: Jermina F., Naveen A., Dharaneeshwaran K., Harish Kumar D., Santhoshkumar P. Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environment. International Journal of Broadband Cellular Communication. 2025; 11(2): 31–38p.

© JournalsPub 2025. All Rights Reserved

because of the quick and extensive adoption of Internet technology, and botnets have become the primary destructive Because of the variety of attacks and the evolving nature of malware, it is getting harder to detect botnet activity.

Devices in networks are more susceptible to these sophisticated attacks as the IoT grows, resulting in significant security breaches and financial losses. To tackle this issue, we suggest creating a hybrid machine learning framework to detect efficient botnets in IoT settings.

One of the biggest cybersecurity risks in IoT environments is botnet attacks, which are distinguished by their complexity and variety of attack methods. Because the tactics used by the attackers are continually evolving, traditional detection methods cannot keep up. Even though they work well on their own, current machine learning models frequently fall short of capturing the entire spectrum of botnet patterns and behaviors.

EXISTING SYSTEM

Artificial Neural Networks (ANNs)

ANNs are used for pattern recognition and learning nonlinear relationships in data. They are effective for tasks requiring feature extraction and classification but may struggle with sequential or time-dependent data.

Convolutional Neural Networks (CNNs)

CNNs excel in feature extraction from grid-like data such as images. They apply convolutional filters to capture spatial hierarchies in data, making them suitable for identifying patterns in network traffic data [3].

Recurrent Neural Networks (RNNs)

By preserving a hidden state that records temporal dependencies, RNNs are made to handle sequential data. They can monitor changes in network activity over time and help model time-series data.

Long Short-Term Memory (LSTM)

LSTMs are a unique kind of RNN that is intended to get around some of the drawbacks of conventional RNNs like vanishing gradients. They are effective in learning long-term dependencies and are well-suited for tasks involving sequences of data.

DISADVANTAGES OF THE EXISTING SYSTEM

ANN

Despite their versatility, ANNs may have limitations because of their inability to accurately represent spatial hierarchies and temporal connections. They might also need a lot of computing power and training data [4, 5].

CNN

CNNs are highly effective for spatial data but are less suited for handling sequential data or capturing long-term dependencies. They also require a significant amount of labeled data for training.

RNN

RNNs can be challenging to train for lengthy sequences due to problems including vanishing and exploding gradients. They also may require substantial computational resources for processing sequences.

LSTM

Though LSTMs address many of the issues of traditional RNNs, they are still computationally intensive and can be complex to tune. They may also require a large amount of data to perform optimally.

© JournalsPub 2025. All Rights Reserved

CONTRIBUTION

Hybrid Model Integration

To create a complete and flexible botnet detection solution, the suggested ACLR model combines multi-neural network architectures such as ANN, CNN, LSTM, and RNN.

Better Detection Performance

The model shows its efficacy in identifying intricate botnet models by achieving high testing accuracy, k-fold cross-validation accuracy, and good ROC-AUC and PR-AUC scores.

Comparative Analysis

To confirm the model's superior performance in identifying botnet activity in IoT environments, it is compared to the most advanced techniques currently in use.

Scalability and Generalizability

Ensuring scalability and generalizability, the hybrid model architecture and design options make it appropriate for various IoT environments and changing botnet attack patterns.

Robustness and Efficiency

To maintain high performance and efficiency in identifying botnet attacks, the model integrates robust techniques like ensemble learning and stacking.

The project's conclusions have applications for improving cybersecurity protocols in IoT networks. The ACLR model can assist organizations in safeguarding their IoT devices and networks against potential threats by offering a dependable and adaptable solution for botnet detection.

This project's contribution, which focuses on the technical aspects of the model and its applications, goes beyond the conference paper. Nonetheless, the study's conclusions and insights can guide future investigations into botnet detection in IoT settings and more general network security and cyber threat espionage applications.

LITERATURE SURVEY

This comprehensive survey provides an overview of various outlier detection techniques, which are crucial for identifying anomalous patterns in network traffic. The review includes discussions on statistical, machine learning, and hybrid approaches, offering insights into methods that can be adapted for detecting botnet activities in IoT networks.

This study examines how deep learning methods, such as RNNs and CNNs, are used in the cybersecurity industry. It highlights the potential of these methods for enhancing threat detection capabilities, which is relevant for understanding their role in botnet detection within IoT environments.

This study explores hybrid machine learning models designed for botnet detection, focusing on the integration of multiple algorithms to improve detection performance. It provides a comparative analysis of various models, which is directly related to the proposed ACLR model's approach of combining ANN, CNN, LSTM, and RNN.

Deep learning methods for network intrusion detection, such as ANN, CNN, and LSTM networks, are the main topic of this survey. It provides insightful information about the advantages and disadvantages of these methods, which can be used to comprehend how they are applied in botnet detection.

An extensive analysis of intrusion detection systems (IDS) created especially for IoT contexts is given in this research. It covers various detection methods, including machine learning and hybrid approaches, highlighting the unique challenges and solutions applicable to IoT-based botnet detection.

© JournalsPub 2025. All Rights Reserved

METHODOLOGY

The proposed ACLR (ANNss, CNNs, LSTM networks, and RNNs) model is a hybrid machine learning system designed to enhance botnet detection in IoT environments. The design integrates multiple machine learning techniques into a unified framework, leveraging their unique strengths to address the complexities of botnet detection [6–9].

System Architecture

Data Collection

- *Source:* Network traffic data, including flow data, packet payloads, and metadata from IoT devices.
- *Preprocessing:* Data normalization, feature extraction, and transformation to ensure compatibility with machine learning models.

Feature Engineering

- *Feature Extraction:* Utilizing domain-specific features such as network traffic patterns, payload characteristics, and time-series data.
- *Dimensionality Reduction:* It is the process of reducing feature space and increasing model efficiency by using methods such as Principal Component Analysis (PCA).

Model Components

- *ANNs:* The ability of ANNs to capture complicated patterns in data and represent complex nonlinear relationships makes them useful [10].
- *CNNs:* Because of their ability to recognize patterns and spatial hierarchies in network traffic, CNNs, are used.
- *Networks Using LSTM:* Used to manage temporal patterns and sequential dependencies in network activity.
- *RNN:* Used to model time-series data and capture dependencies over time.

Stacking and Integration

- *Hybrid Model:* A stacking approach is used to combine the outputs of ANN, CNN, LSTM, and RNN models. The stacking technique aggregates predictions from individual models to make a final decision [11].
- *Ensemble Learning:* Enhances model robustness and generalizability by leveraging the strengths of each model component.

Evaluation and Validation

- *Training:* Models are trained using labeled datasets, with hyperparameter tuning to optimize performance.
- *Cross-Validation:* K-fold cross-validation is applied to assess model robustness and avoid overfitting.

Deployment

- *Real-time Monitoring:* The system is designed for real-time analysis of network traffic to detect botnet activities promptly.

IMPLEMENTATION

System

Store Dataset

The System stores the dataset given by the user.

Model Training

This involves exposing a machine learning model to a dataset to teach it to produce precise predictions or classifications. Data is prepared and divided into test, validation, and training sets during this step.

© JournalsPub 2025. All Rights Reserved

Using methods, like gradient descent to maximize performance, the chosen algorithm learns from the training data by modifying its internal parameters to reduce prediction mistakes (Figures 1 and 2).

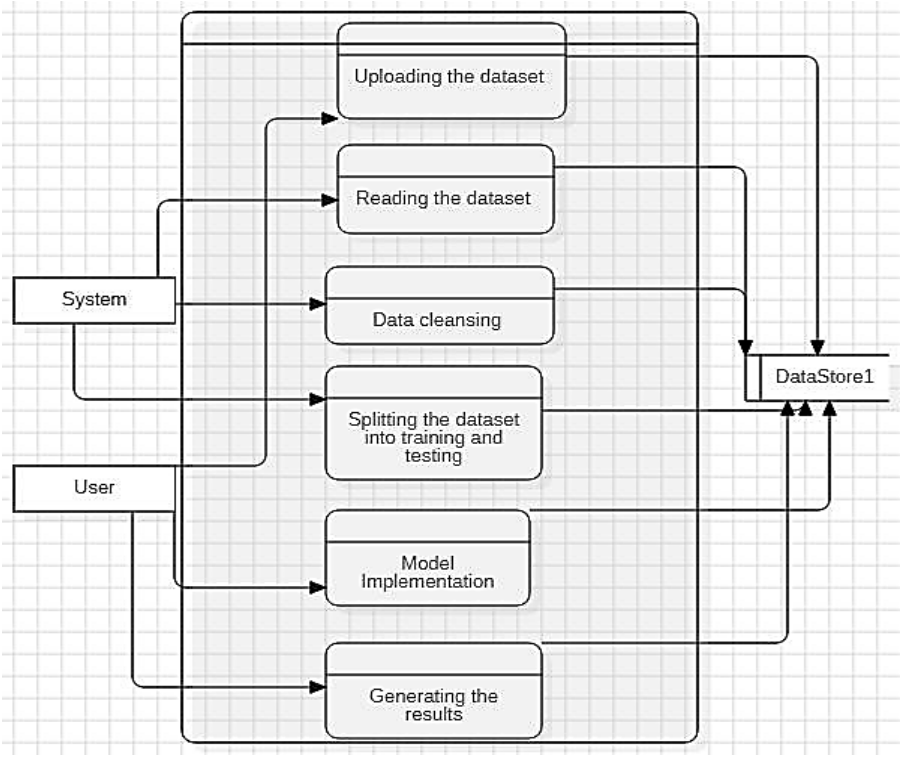

Figure 1. Workflow diagram of dataset processing and model execution.

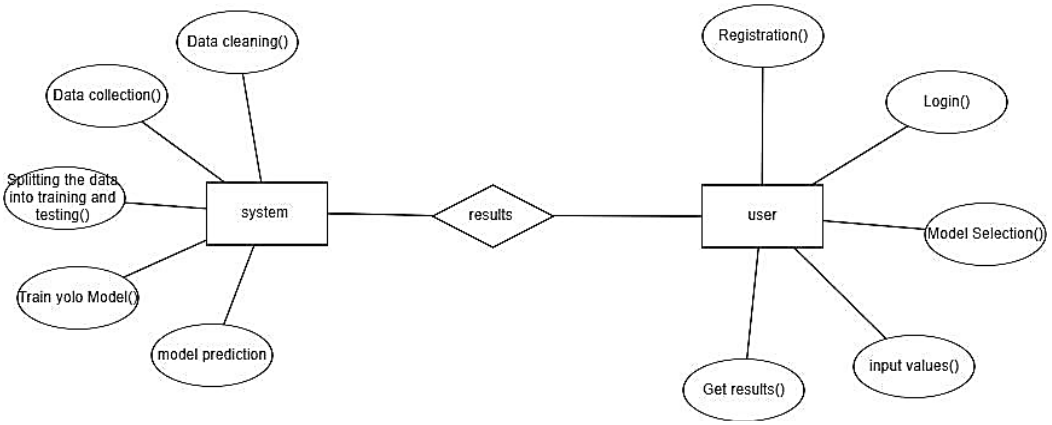

Figure 2. System–user interaction flow for data processing and model prediction.

Model Forecasts

The user provides the input, and the system uses that data to forecast the outcome.

The Individual

Signing up

By providing their personal details, new users can create an account on the Registration Page. It has spaces for passwords, email addresses, username, and other necessary information. The page has validation to make sure all the data entered is accurate and complies with the standards. For instance, it looks for strong passwords, legitimate email formats, and unique usernames. A seamless and secure registration procedure is ensured by providing users with real-time feedback on any mistakes or problems with their input.

© JournalsPub 2025. All Rights Reserved

Sign in

Username/Email Field

Verifies that the username or email format is legitimate.

The password field verifies that the password satisfies security specifications such as minimum length and complexity. Messages of Validation give prompt feedback if the account details do not match or if the input is inaccurate [12, 13]. Looking at the data:

The dataset is viewable by the user.

Choosing a Model

The user has the option to view and choose a model's accuracy.

Prediction

The user can predict based on the date it is better to buy the stocks or not.

RESULTS

In addition to the high-performance metrics, the ACLR model underwent thorough testing to ensure it could generalize well with new, unseen data and maintain reliability in different environments.

Accuracy Testing

During testing, the ACLR model achieved a notable accuracy of *96.98%,* affirming its capability in accurately identifying botnet activity. The high accuracy highlights the model's proficiency in detecting both well-known and novel botnet patterns in a simulated IoT environment [14–17].

Cross-Validation

To further validate the robustness and generalization ability of the ACLR model, it was subjected to K-fold cross-validation with $K = 5$. This process yielded an average accuracy of *97.49%,* demonstrating that the model was not overfitting and could perform consistently across multiple subsets of the data. Additionally, cross-validation guarantees that the model's performance is impartial toward any specific data segment.

Comparative Analysis

To benchmark the ACLR model's performance, a comparative analysis was conducted against state-of-the-art botnet detection techniques, including machine learning models and rule-based IDS.

Superior Detection Capability

The ACLR model outperformed existing techniques in terms of capturing complex and evolving botnet patterns. The combination of multiple deep learning models through stacking enabled ACLR to recognize both obvious and subtle malicious behaviors that traditional methods often missed.

Reduction in False Positives/Negatives

A key improvement observed with the ACLR model was its ability to minimize both false positives (non-malicious traffic wrongly flagged as botnet) and false negatives (botnet traffic not detected). This reduction is critical in real-world IoT environments, where false positives can lead to unnecessary disruptions, and false negatives may leave networks vulnerable to attacks.

Effectiveness in Practical Implementation

The ACLR model was tuned for efficiency in addition to detection performance, which makes it appropriate for deployment of IoT systems with limited resources. Its ability to handle real-time traffic data with minimal latency makes it practical for use in live network monitoring and botnet mitigation strategies (Table 1).

© JournalsPub 2025. All Rights Reserved

Table 1. Test cases.

S.N.	Test Cases	I/O	Expected O/T	Actual O/T	P/F
1	Read the dataset.	Dataset.	The dataset needs to be read successfully.	Dataset fetched successfully.	P
2	Performing pre-processing on the dataset	Preprocessing part takes place	Preprocessing should be performed on the dataset	Preprocessing successfully completed.	P
3	Model Building	Model Building for the clean data	Need to create a model using the required algorithms	Model created successfully.	P
4	IOT Detection	Input fields provided.	Output should be whether attacks	The model predicted different types of attacks.	P
5	IOT Detection	Input fields provided.	Output should be whether attacks	The model predicted different types of attacks.	P

CONCLUSIONS

A significant improvement in botnet identification for IoT environments is offered by the ACLR hybrid system study version. The ACLR version addresses the complex problems of botnet detection by combining ANN, CNN, LSTM, and RNN algorithms into a single stacking architecture, utilizing the advantages of each method. The ACLR version shows its potential as a useful tool for enhancing cybersecurity measures for IoT networks with its excellent ROC-AUC and PR-AUC ratings, high trying out accuracy, and significant cross-validation effects. The comparative analysis also demonstrates how effective it is in comparison to current methods, offering a promising method to address the growing threat of botnet attacks.

Acknowledgment

We extend our gratitude to the Management of Karpagam College of Engineering, Coimbatore, for the excellent infrastructure and support facilities to undertake the project work. We are very grateful to Dr. V. Kumar Chinnaiyan, the Principal, and Dr. S. Logeswari, Ph.D., Professor, Head of Department, Department of Computer Science and Engineering (Cyber Security), for providing the facilities, support, and permission to carry out our research work at our esteemed institution. We record my sincere gratitude to our Project Coordinator, Ms. F. Jermina, M. E., Assistant Professor, Department of Computer Science and Engineering (Cyber Security), for giving input, and encouragement for the continuous improvement during the process and for completing this research work. We would like to express our sincere gratitude to our Supervisor Ms. F. Jermina, M. E., Assistant Professor, Department of Computer Science and Engineering (Cyber Security), for the continuous support for our UG study, for her motivation, and adequate guidance, which helped us to achieve success in all our accomplishments and to complete this research work. We also thank all the teaching faculty members and non-teaching Staff members of the Department of Computer Science and Engineering (Cyber Security), Karpagam College of Engineering, Coimbatore, for their kindness and support.

REFERENCES

1. Jain AK, Murty MN, Flynn PJ. Data clustering: a review. ACM Comput Surv. 1999;31(3):264–323.
2. Guerra-Manzanares A, Bahsi H, Nomm S. Hybrid feature selection models for machine learning based botnet detection in IoT networks. In: 2019 International Conference on Cyberworlds (CW). IEEE; 2019. p. 324–7.
3. Xing Y, Shu H, Zhao H, Li D, Guo L. Survey on botnet detection techniques: Classification, methods, and evaluation. Math Probl Eng. 2021;2021(1):6640499.
4. McDermott CD, Majdani F, Petrovski AV. Botnet detection in the Internet of Things using deep learning approaches. In: 2018 International Joint Conference on Neural Networks (IJCNN). IEEE; 2018. p. 1–8.
5. Di Mauro M, Galatro G, Liotta A. Experimental review of neural-based approaches for network intrusion management. IEEE Trans Netw Serv Manag. 2020;17(4):2480–95.
6. Chen SC, Chen YR, Tzeng WG. Effective botnet detection through neural networks on

© JournalsPub 2025. All Rights Reserved

convolutional features. In: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). IEEE; 2018. p. 372–8.
7. Zhen L, Kamarudin NH, Kok VJ, Qamar F. Anomaly detection model in network security situational awareness based on machine learning: Limitation, techniques, future trends. IEEE Access. 2025.
8. Kwon D, Kim H, Kim J, Suh SC, Kim I, Kim KJ. A survey of deep learning-based network anomaly detection. Clust Comput. 2019;22(Suppl 1):949–61.
9. Costa J, Dessai N, Gaonkar S, Aswale S, Shetgaonkar P. IoT-botnet detection using long short-term memory recurrent neural network. Int J Eng Res. 2020;9(8):531–6.
10. Cui J, Long J, Min E, Liu Q, Li Q. Comparative study of CNN and RNN for deep learning based intrusion detection system. In: International Conference on Cloud Computing and Security. Cham: Springer; 2018. p. 159–70.
11. Pokhrel S, Abbas R, Aryal B. IoT security: Botnet detection in IoT using machine learning. arXiv [Preprint]. 2021. Available from: arXiv:2104.02231.
12. Zhang H. Development of an intelligent intrusion detection system for IoT networks using deep learning. Discov Internet Things. 2025;5(1):74.
13. Vinayakumar R, Soman KP, Poornachandran P. Applying convolutional neural network for network intrusion detection. In: 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE; 2017. p. 1222–8.
14. Ullah I, Mahmoud QH. Design and development of RNN anomaly detection model for IoT networks. IEEE Access. 2022;10:62722–50.
15. Wu X, Zhu X, Wu GQ, Ding W. Data mining with big data. IEEE Trans Knowl Data Eng. 2013;26(1):97–107.
16. Alotaibi Y, Ilyas M. Ensemble-learning framework for intrusion detection to enhance Internet of Things' devices security. Sensors. 2023;23(12):5568.
17. Al-Shurbaji T, Anbar M, Manickam S, Hasbullah IH, ALfriehate N, Alabsi BA, et al. Deep learning-based intrusion detection system for detecting IoT botnet attacks: a review. IEEE Access. 2025.

© JournalsPub 2025. All Rights Reserved