International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 1, 2026

Detecting Botnet Attacks in IoT Environments Using an Optimized Lightweight Hybrid Deep Learning Model

Aileni Abhinaya[1], Dr. Md. Asif[2]

[1]B.Tech Student, Department of Electronics and Computer Engineering,J.B. Institute of Engineering & Technology, Telangana, India.

[2]Associate Professor, Department of Electronics and Computer Engineering,J.B. Institute of Engineering & Technology, Telangana, India.

asif.ecm@jbiet.edu.in

Abstract

The rapid expansion of the Internet of Things (IoT) has resulted in billions of interconnected devices operating in smart homes, healthcare systems, industrial automation and intelligent transportation. Although IoT technology provides significant advantages, its limited computational capability and weak security mechanisms expose networks to large-scale cyber threats, particularly botnet attacks. Botnets exploit vulnerable IoT devices and launch coordinated attacks such as distributed denial of service (DDoS), data theft and reconnaissance. Conventional intrusion detection systems based on static rules and signatures fail to effectively detect evolving and previously unseen attacks.

This paper presents an optimized deep learning-based intrusion detection framework for detecting botnet attacks in IoT environments. The framework evaluates existing deep learning models including Convolutional Neural Networks (CNN), Long Short-Term Memory networks (LSTM) and Recurrent Neural Networks (RNN). In addition, a novel lightweight hybrid deep learning model called Advanced Custom Lightweight Recurrent (ACLR) is proposed. The ACLR model integrates Conv1D, LSTM and Simple RNN layers to efficiently capture both spatial and temporal characteristics of network traffic while maintaining low computational complexity.

The Bot-IoT 2018 dataset is used for experimental evaluation. The proposed model achieves an accuracy of 96.42%, outperforming CNN, LSTM and RNN models. The results demonstrate that the proposed framework is effective, scalable and suitable for deployment in resource-constrained IoT environments.

Keywords: *Internet of Things, Botnet attacks, Intrusion Detection System, Deep Learning, CNN, LSTM, RNN, Hybrid model.*

1. Introduction

The Internet of Things (IoT) paradigm has significantly transformed modern digital infrastructure by enabling large numbers of heterogeneous devices to communicate and exchange information autonomously. IoT systems are widely deployed in several domains such as smart homes, industrial control systems, healthcare monitoring, smart agriculture and intelligent transportation systems. These environments rely heavily on continuous data transmission and real-time decision making.

Despite the advantages offered by IoT technologies, security remains a major challenge. Most IoT devices are developed with strict cost and power constraints, which often results in weak authentication mechanisms, limited encryption support and infrequent firmware updates. Consequently, IoT devices have become prime targets for cyber attackers.

One of the most dangerous threats in IoT environments is the botnet attack. In a botnet attack, a large number of compromised devices are remotely controlled by an attacker and used to perform malicious activities such as distributed denial-of-service attacks, scanning, data exfiltration and malware propagation. The Mirai botnet and its variants have demonstrated the severe impact of IoT botnets on global network infrastructure.

Traditional intrusion detection systems (IDS) are mostly based on predefined signatures or handcrafted rules. Although these methods are effective in detecting known attacks, they are unable to cope with new, evolving and sophisticated attack patterns. Furthermore, the diversity and scale of IoT traffic make manual feature engineering and rule creation extremely difficult.

Machine learning and deep learning techniques have emerged as promising alternatives for intrusion detection. These approaches are capable of automatically learning complex patterns from network traffic and adapting to changing attack behaviors. However, many deep learning models are computationally intensive and require high memory and processing resources, which limits their applicability in resource-constrained IoT environments.

In this context, this paper proposes a lightweight and optimized deep learning framework for detecting botnet attacks in IoT networks. The main objective is to design a hybrid model that achieves high detection accuracy while maintaining low computational overhead. The proposed ACLR model combines convolutional and recurrent learning mechanisms to efficiently capture both spatial and temporal features of network traffic.

ISSN 2347–3657
Volume 14, Issue 1, 2026

The main contributions of this work are summarized as follows:

- A comprehensive evaluation of CNN, LSTM and RNN models for botnet detection in IoT networks.
- Design of a novel lightweight hybrid deep learning architecture tailored for resource-constrained environments.
- Performance evaluation using a realistic and widely used IoT attack dataset.
- Demonstration of improved detection accuracy and robustness compared to conventional deep learning models.

2. Related Work

A large number of studies have investigated intrusion detection in networked systems using machine learning and deep learning techniques. Early research focused on classical machine learning algorithms such as Decision Trees, Support Vector Machines, k-Nearest Neighbors and Random Forests. These techniques rely heavily on feature engineering and often struggle with high-dimensional and sequential network traffic.

In recent years, deep learning methods have gained attention due to their ability to automatically extract meaningful representations from raw data. Convolutional Neural Networks have been used to detect spatial correlations in network traffic features. CNN-based intrusion detection systems can capture localized patterns and have shown promising detection accuracy.

Recurrent Neural Networks and Long Short-Term Memory networks are particularly suitable for modeling time-dependent data. Network traffic exhibits strong temporal characteristics, as attack behaviors often evolve over time. LSTM networks have been widely adopted to capture long-term dependencies and have demonstrated improved performance in detecting slow and stealthy attacks.

Several hybrid models have been proposed to combine the strengths of convolutional and recurrent networks. These architectures aim to capture both spatial and temporal information. However, most existing hybrid models are designed for high-performance computing environments and require significant computational resources.

Furthermore, many previous studies do not explicitly address the deployment constraints of IoT environments, such as limited processing power, memory and energy consumption. As a result, although high detection accuracy is achieved, practical deployment on IoT gateways or edge devices remains challenging.

This motivates the need for an optimized and lightweight hybrid architecture that can maintain strong detection performance while remaining suitable for real-world IoT deployments.

3. System Overview

The proposed intrusion detection framework consists of the following major components:

1. Data acquisition and preprocessing module
2. Deep learning model training module
3. Performance evaluation module
4. Prediction and classification module

The framework supports training and evaluation of multiple deep learning models, including CNN, LSTM, RNN and the proposed ACLR model. All models operate on the same preprocessed dataset to ensure a fair and consistent comparison.

The system workflow begins with the collection of labeled network traffic data. The dataset is preprocessed to remove noise and transform features into a suitable representation for deep learning models. The processed data is then used to train baseline models as well as the proposed hybrid model. Finally, the trained models are evaluated using standard classification metrics.

4. Dataset Description

The experiments in this study are conducted using the Bot-IoT 2018 dataset. The dataset is specifically designed for evaluating intrusion detection systems in IoT environments. It contains both normal and malicious traffic generated in a realistic network testbed.

The dataset includes multiple categories of attacks, such as:

- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Reconnaissance
- Information theft

Each record in the dataset consists of several network flow features representing communication behavior between devices. A binary class label is used to indicate whether the traffic instance is normal or malicious.

The diversity and scale of the Bot-IoT dataset make it suitable for evaluating deep learning-based detection models and for studying the performance of intrusion detection systems in realistic IoT scenarios.

5. Data Preprocessing

Effective preprocessing is essential for achieving stable and accurate learning in deep neural networks. The following preprocessing steps are applied to the dataset:

5.1 Data Cleaning

Records containing missing or inconsistent values are removed. This ensures that the learning process is not affected by incomplete information.

5.2 Categorical Encoding

Categorical attributes such as protocol type and service type are transformed into numerical representations using category encoding. This

allows the deep learning models to process these attributes effectively.

5.3 Feature Normalization

All numerical features are normalized using standard scaling techniques. Normalization improves convergence during training and prevents features with large numeric ranges from dominating the learning process.

5.4 Train–Test Split

The dataset is divided into training and testing subsets using an 80:20 split. The training subset is used to learn the model parameters, while the testing subset is used exclusively for performance evaluation.

5.5 Data Reshaping

The processed feature vectors are reshaped into a three-dimensional format to satisfy the input requirements of one-dimensional convolutional and recurrent layers.

6. Baseline Deep Learning Models

To establish reliable reference performance, three deep learning models are implemented and evaluated.

6.1 Convolutional Neural Network

The CNN model employs one-dimensional convolutional layers followed by pooling and fully connected layers. The convolutional layers extract spatial patterns from the input feature sequences. The CNN model is effective in identifying localized anomalies in traffic flows.

6.2 Long Short-Term Memory Network

The LSTM model is designed to capture long-term temporal dependencies in network traffic. The memory cells and gating mechanisms enable the model to retain useful historical information and suppress irrelevant patterns.

6.3 Recurrent Neural Network

The RNN model is implemented using simple recurrent units. It models the sequential nature of network traffic and learns short-term temporal dependencies.

All baseline models are trained under similar experimental conditions to ensure a fair comparison with the proposed ACLR model.

7. Proposed ACLR Model

The Advanced Custom Lightweight Recurrent (ACLR) model is designed as a compact hybrid architecture that integrates convolutional and recurrent components.

The architecture consists of the following main layers:

- A one-dimensional convolutional layer for spatial feature extraction.
- An LSTM layer for learning long-term temporal dependencies.
- A Simple RNN layer for lightweight sequential representation.
- Fully connected layers for classification.

The convolutional layer captures local correlations among features, while the LSTM and Simple RNN layers capture temporal relationships in network traffic behavior. The model is carefully optimized to reduce the number of trainable parameters and to minimize computational complexity.

This hybrid structure enables the ACLR model to benefit from the complementary strengths of convolutional and recurrent learning mechanisms while remaining suitable for deployment in IoT gateways and edge devices.

8. Experimental Setup

The proposed framework is implemented using Python and the Keras deep learning library. The Adam optimizer is employed to update network weights, and categorical cross-entropy is used as the loss function.

To prevent overfitting and improve generalization performance, early stopping is applied during training. The same training and testing splits are used for all evaluated models.

The following evaluation metrics are used to measure detection performance:

- Accuracy
- Precision
- Recall
- F1-score
- Area under the ROC curve

These metrics provide a comprehensive assessment of the classification capability of the models.

9. Results and Performance Analysis

The performance of the baseline models and the proposed ACLR model is summarized below:

Model	Accuracy (%)
CNN	95.35
LSTM	94.44
RNN	95.12
Proposed ACLR	**96.42**

The results clearly show that the ACLR model achieves the highest detection accuracy among all evaluated models.

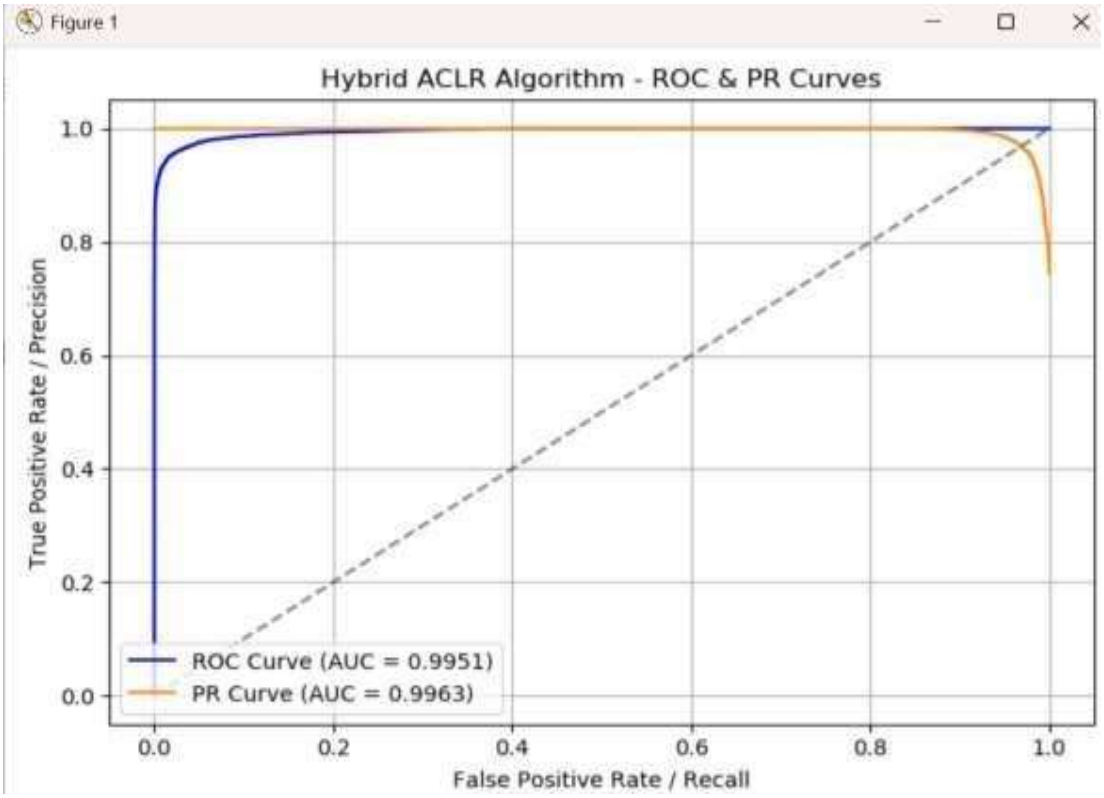
In addition to accuracy, the ACLR model demonstrates improved precision and recall values. High precision indicates that the model produces fewer false alarms, while high recall shows that it successfully detects a large proportion of attack instances. The improved F1-score further confirms the balanced performance of the proposed approach.

The superior performance of the ACLR model can be attributed to its ability to jointly capture spatial and temporal characteristics of network traffic. The convolutional layer extracts discriminative patterns from traffic features, and the recurrent layers model sequential behaviors that are commonly associated with botnet activities.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

Furthermore, the lightweight structure of the ACLR model reduces training time and computational overhead
compared to deeper and more complex architectures. This makes the model suitable for real-time deployment

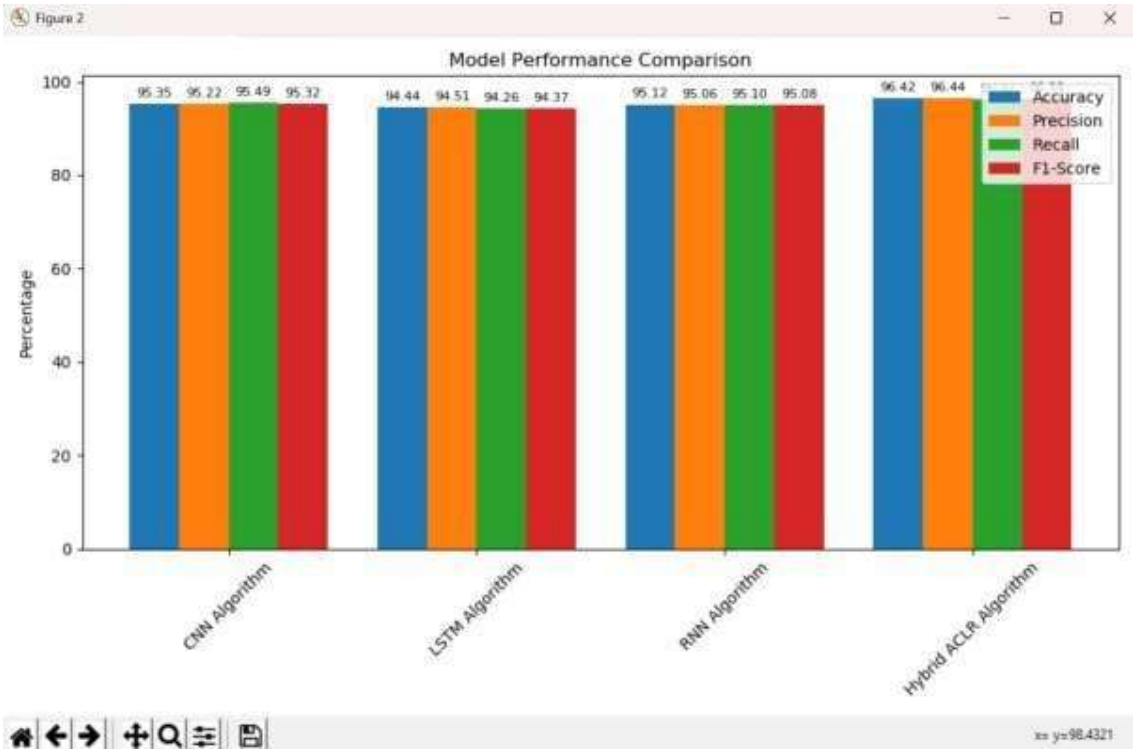
scenarios.Home Screen



International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

ACLR ROC & PR Curves

Comparison Graph



10. Discussion

The experimental results demonstrate that hybrid architectures are more effective for IoT intrusion detection than standalone CNN or RNN models. Botnet attacks often exhibit both spatial correlations among features and temporal patterns over time. Models that fail to exploit both aspects may miss important indicators of malicious behavior.

The proposed ACLR model successfully integrates these two learning perspectives while maintaining a compact structure. This is particularly important for IoT environments, where computational resources and energy availability are limited.

The framework also supports real-time prediction of unseen traffic instances, making it practical for deployment in operational networks. Network administrators can use the model to automatically classify incoming traffic as either normal or malicious, enabling timely response to security threats.

Although the results are promising, further improvements can be achieved by incorporating advanced optimization techniques and by exploring distributed learning strategies for large-scale IoT deployments.

11. Conclusion

This paper presented a lightweight and optimized deep learning-based intrusion detection framework for detecting botnet attacks in IoT environments. A novel hybrid architecture called ACLR was proposed by combining Conv1D, LSTM and Simple RNN layers.

Experimental evaluation using the Bot-IoT 2018 dataset demonstrated that the proposed model outperforms conventional CNN, LSTM and RNN models, achieving an accuracy of 96.42%. The results confirm that the proposed approach effectively captures both spatial and temporal patterns in network traffic while remaining computationally efficient.

The proposed framework provides a practical and scalable solution for securing modern IoT infrastructures against botnet threats.

12. Future Work

Future research directions include:

- real-time deployment using streaming network data,
- multi-class classification to identify specific attack categories,
- deployment and optimization on embedded edge devices,
- and integration of explainable artificial intelligence techniques to improve transparency and trust in automated intrusion detection systems.

REFERENCES

1. Cisco, "Cisco Predicts More IP Traffic in the Next Five Years Than in the History of the Internet," Nov. 2018.
2. Z. Alansari, S. Soomro, M. R. Belgaum, and S. Shamshirband, "The rise of internet of things (iot) in big healthcare data: review and open research issues," in Progress in Advanced Computing and Intelligent Engineering. Springer, 2018, pp. 675–685.
3. H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, and P. Siano, "Iot-based smart cities: A survey," in 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), 2016, pp. 1–6.
4. I. Al Ridhawi, M. Aloqaily, B. Kantarci, Y. Jararweh, and H. T. Mouftah, "A continuous diversified vehicular cloud service availability framework for smart cities," Computer Networks, vol. 145, pp. 207–218, 2018.
5. Z. Doffman, "Cyberattacks on iot devices surge 300% in 2019,'measured in billions,'report claims," 2019.
6. A. Moubayed, A. Refaey, and A. Shami, "Software-defined perimeter (sdp): State of the art secure solution for modern networks," IEEE Network, vol. 33, no. 5, pp. 226–233, Sep.- Oct. 2019.
7. P. Kumar, A. Moubayed, A. Refaey, A. Shami, and J. Koilpillai, "Performance analysis of sdp for secure internal enterprises," in 2019 IEEE Wireless Communications and Networking Conference (WCNC), Apr. 2019, pp. 1–6.
8. H. Hindy, D. Brosset, E. Bayne, A. K. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," IEEE Access, vol. 8, pp. 104 650–104 675, 2020.
9. A. Moubayed, M. Injadat, A. B. Nassif, H. Lutfiyya, and A. Shami, "Elearning: Challenges and research opportunities using machine learning data analytics," IEEE Access, vol. 6, pp. 39 117–39 138, 2018.
10. A. Moubayed, M. Injadat, A. Shami, and H. Lutfiyya, "Student engagement level in an e- learning environment: Clustering using k-means," American Journal of Distance Education, vol. 34, no. 2, pp. 137–156, 2020.
11. M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, "Systematic ensemble model selection approach for educational data mining," Knowledge-based Systems, vol. 200, p. 105992, Jul. 2020.
12. A. Moubayed, M. Injadat, A. Shami, and H. Lutfiyya, "DNS TypoSquatting Domain Detection: A Data Analytics & Machine Learning Based Approach," in 2018 IEEE Global Communications Conference (GLOBECOM), Dec. 2018, pp. 1–7.
13. A. Moubayed, E. Aqeeli, and A. Shami, "Ensemble-based feature selection and classification model for dns typo-squatting detection," in 2020 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Aug. 2020.
14. L. Yang and A. Shami, "On hyperparameter optimization of

machine learning algorithms: Theory and practice," Neurocomputing, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925231220311693
A. Moubayed, "Optimization Modeling and Machine LearningZ. Alansari, S. Soomro, M. R. Belgaum, and S. Shamshirband, "The rise of internet of things (iot) in big healthcare data: review and open research issues," in Progress in Advanced Computing and Intelligent Engineering. Springer, 2018, pp. 675–685.

15. H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, and P. Siano, "Iot-based smart cities: A survey," in 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), 2016, pp. 1–6.
16. I. Al Ridhawi, M. Aloqaily, B. Kantarci, Y. Jararweh, and H. T. Mouftah, "A continuous diversified vehicular cloud service availability framework for smart cities," Computer Networks, vol. 145, pp. 207–218, 2018.
17. Z. Doffman, "Cyberattacks on iot devices surge 300% in 2019,'measured in billions,'report claims," 2019.
18. A. Moubayed, A. Refaey, and A. Shami, "Software-defined perimeter (sdp): State of the art secure solution for modern networks," IEEE Network, vol. 33, no. 5, pp. 226–233, Sep.- Oct. 2019.
19. P. Kumar, A. Moubayed, A. Refaey, A. Shami, and J. Koilpillai, "Performance analysis of sdp for secure internal enterprises," in 2019 IEEE Wireless Communications and Networking Conference (WCNC), Apr. 2019, pp. 1–6.
20. H. Hindy, D. Brosset, E. Bayne, A. K. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," IEEE Access, vol. 8, pp. 104 650–104 675, 2020.
21. A. Moubayed, M. Injadat, A. B. Nassif, H. Lutfiyya, and A. Shami, "Elearning: Challenges and research opportunities using machine learning data analytics," IEEE Access, vol. 6, pp. 39 117–39 138, 2018.
22. A. Moubayed, M. Injadat, A. Shami, and H. Lutfiyya, "Student engagement level in an e- learning environment: Clustering using k-means," American Journal of Distance Education, vol. 34, no. 2, pp. 137–156, 2020.
23. M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, "Systematic ensemble model selection approach for educational data mining," Knowledge-based Systems, vol. 200, p. 105992, Jul. 2020.
24. A. Moubayed, M. Injadat, A. Shami, and H. Lutfiyya, "DNS TypoSquatting Domain Detection: A Data Analytics & Machine Learning Based Approach," in 2018 IEEE Global Communications Conference (GLOBECOM), Dec. 2018, pp. 1–7.
25. A. Moubayed, E. Aqeeli, and A. Shami, "Ensemble-based feature selection and classification model for dns typo-

ISSN 2347–3657
Volume 14, Issue 1, 2026

squatting detection," in 2020 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Aug. 2020.