AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1) (2026)

Botnet Attack Detection in IoT Using a Hybrid Deep Learning Framework with ACLR Technique

Mr V.NARAHARI[1], N.NARASIMHULU[2]

[1]**Assistant Professor Dept. of C.S.E, Anantha Lakshmi Institute of Technology and sciences Anantapur- 515721 Orcid Id : 0009-0005-8019-5227**

[2]**PG Scholar, Dept. of C.S.E, Anantha Lakshmi Institute of Technology and sciences Anantapur- 515721**

Abstract: Cyber-attacks have increased significantly with the rapid expansion and widespread adoption of internet technologies, with botnet attacks emerging as one of the most destructive threats. The identification of botnets has become increasingly challenging due to diverse attack vectors and the continuous evolution of malware. In the context of the rapidly growing Internet of Things (IoT), many interconnected devices with limited security features are highly vulnerable to botnet intrusions, leading to substantial losses across various sectors. Traditional detection methods often fail to effectively identify such sophisticated and dynamic attack patterns. To address these challenges, this research proposes a hybrid machine learning model named ACLR, which integrates Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Recurrent Neural Networks (RNN) in a stacked architecture. The model leverages the UNSW-NB15 dataset, comprising nine distinct attack categories, to learn complex patterns in network traffic data. Experimental results demonstrate that the proposed model achieves high detection accuracy and effectively identifies diverse botnet behaviours. Overall, the ACLR model enhances IoT security by providing a robust, scalable, and automated solution for detecting malicious network activities.

Key Words: Botnet Detection, Internet of Things (IoT) Security, Hybrid Deep Learning Model, UNSW-NB15 Dataset, Network Intrusion Detection System (NIDS).

1. Introduction

The rapid growth of the internet has enabled global connectivity and digital services but also introduced serious security risks. Cybercriminals use compromised devices in botnets to launch attacks such as DDoS, data breaches, and malware distribution. Detecting botnet attacks is crucial to minimize damage, maintain network performance, protect user trust, and ensure regulatory compliance. Deep learning-based botnet detection has emerged as a powerful and efficient approach to identifying malicious activity within network traffic. Unlike traditional rule-based or signature-based systems, deep learning models automatically learn complex patterns from raw network data. These models can quickly classify and detect harmful botnet behaviour, enabling organizations to respond promptly and protect their systems. Ransomware, for example, often relies on

botnet infrastructures to infect large numbers of victims, encrypt their data, and demand payment. By detecting botnet activity early, organizations can mitigate such large-scale attacks.

The rapid expansion of Internet of Things (IoT) devices has significantly increased the vulnerability of networks to botnet attacks, where even a small number of compromised devices can lead to large-scale disruptions. Traditional detection techniques often fail to cope with the dynamic, high-volume, and heterogeneous nature of IoT traffic. To address these challenges, deep learning–based network traffic analysis has emerged as a powerful solution. These systems automatically extract meaningful features from raw packet data—particularly from the initial packets of network flows—to identify communication patterns associated with botnets. Models such as Convolutional Neural Networks (CNNs) effectively capture spatial relationships within packet structures, while auto encoders learn normal traffic behaviour and detect anomalies indicative of malicious activity.

Building on these strengths, this research proposes a hybrid stacking model, ACLR, which integrates Artificial Neural Networks (ANN), CNN, Long Short-Term Memory (LSTM), and Recurrent Neural Networks (RNN) to enhance botnet attack detection in IoT environments. The model is designed to classify a wide range of attack types, including normal traffic, generic attacks, worms, backdoors, shell code, fuzzers, denial-of-service (DoS), reconnaissance, and analysis attacks. Prior to training, the dataset undergoes pre-processing steps such as removal of null values and label encoding to ensure data consistency and compatibility with machine learning algorithms. The performance of the proposed system is rigorously evaluated using key metrics like accuracy, precision, recall, and F1-score, ensuring reliable and balanced detection. Overall, the model provides a scalable, adaptive, and robust framework capable of identifying diverse and evolving botnet threats, thereby significantly improving the security of IoT networks.

2. Literature Survey

Attacks on computer networks can read, modify, damage, or steal sensitive information, significantly degrading system performance and reliability. Prior to launching full-scale intrusions, attackers often conduct reconnaissance activities such as port scanning and IP spoofing to identify vulnerabilities in target systems. Detection mechanisms typically monitor network attributes including source and destination IP addresses, port numbers, protocol details, and packet header information to identify suspicious patterns [9]. Based on their behaviour, attacks are broadly classified as passive or active. Passive attacks involve covert monitoring of network communications to gather confidential data, making them difficult to detect. Active attacks, however, directly exploit system vulnerabilities, bypass security mechanisms, impersonate trusted entities, or steal credentials to gain unauthorized access.

One of the early applications of machine learning for botnet detection utilized a convolutional neural network (CNN) model, achieving training accuracy of 98.62% and test accuracy of 99.57%, demonstrating the effectiveness of deep learning in identifying

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1) (2026)

malicious traffic patterns [10]. Among real-world examples, the Mirai botnet is one of the most prominent IoT-based DDoS attacks. In a DDoS attack, compromised devices simultaneously flood a target server with requests, overwhelming it and disrupting legitimate services. Mirai malware infects IoT devices and coordinates attacks through a command-and-control (C&C) server. To detect such attacks, researchers proposed a bidirectional long short-term memory (BLSTM-RNN) model, which outperformed unidirectional LSTM models by leveraging both past and future contextual information in network traffic sequences. The model achieved validation accuracies of approximately 99% for Mirai-related traffic [11].

3.System Architecture

The system architecture for a hybrid machine learning model to detect botnet attacks in an IoT environment consists of interconnected modules for data collection, pre-processing, feature extraction, and classification.



Fig 1: System Architecture

IoT network traffic is first captured from various devices and cleaned to remove noise and redundancy. Relevant features are then extracted and fed into a hybrid model to identify malicious patterns. The trained model analyses incoming traffic in real time to detect botnet activities. Finally, the system outputs alerts and stores results for further analysis, ensuring scalable and efficient threat detection.

4.Methodology

The proposed methodology develops an intelligent botnet detection framework for IoT environments using a structured, multi-stage approach. It begins with dataset acquisition utilizing the UNSW-NB15 dataset followed by pre-processing steps such as removing redundant records, encoding categorical features, and normalizing numerical data to ensure consistency and model readiness.



Fig 2: Proposed Methodology

The core system is built on a hybrid ACLR model that integrates ANN, CNN, LSTM, and RNN, where each component captures different aspects of network traffic, including nonlinear relationships, spatial patterns, and temporal behaviours. These models are combined using a stacked ensemble approach to improve detection accuracy and robustness. The trained model is embedded within a Network Intrusion Detection System (NIDS), which classifies network traffic into normal or multiple attack categories. In real-time deployment, the system continuously monitors incoming data and generates alerts upon detecting potential botnet activity, ensuring effective and adaptive network security.

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1) (2026)

5. Design and Construction

The design of the proposed botnet detection system is structured to integrate IoT traffic monitoring with advanced machine learning techniques. The architecture begins with IoT devices such as sensors, cameras, and smart home appliances, which continuously generate network traffic. This traffic is captured by a Network Traffic Collector, ensuring that both normal and malicious flows are recorded for analysis.

i) Dataset Acquisition:

The dataset IoT traffic monitoring with advanced machine learning to capture and analyse data from connected devices for detecting malicious activities. It utilizes the UNSW-NB15 dataset, which includes diverse attack types and rich traffic features, enabling effective modelling and detection of modern botnet behaviour in IoT environments.

ii) Data Preprocessing

Raw data pre-processing removes inconsistencies by eliminating duplicates, handling missing values through mean imputation, and encoding categorical attack labels into numerical form. Feature scaling is then applied to normalize data, ensuring balanced model learning and improved performance. For scaling, Z-score standardization was applied:

$$X = \frac{X - \mu}{\sigma}$$

iii) Model Development

The proposed ACLR model is a hybrid stacked deep learning architecture that integrates ANN, CNN, LSTM, and RNN to improve botnet detection accuracy. By combining their strengths in capturing nonlinear, spatial, and temporal patterns, the stacked ensemble produces a more robust and reliable prediction output.

$$\hat{y} = f_{stack}(f_{ANN}(x), f_{CNN}(x), f_{LSTM}(x), f_{RNN}(x))$$

iv) Performance Evaluation

The ACLR model was evaluated using key classification metrics, including Accuracy, Precision, Recall, and F1-score. Accuracy measured overall performance, Precision assessed correct attack identification, Recall evaluated detection of attack instances, and F1-score balanced Precision and Recall. Its performance was compared with traditional models like Random Forest to demonstrate the improvements achieved by ACLR

v) Real-Time Detection

The final stage of the methodology involved testing ACLR on unseen traffic flows to validate real-world applicability. Incoming IoT traffic was preprocessed using the same pipeline and fed into the model for classification. The system successfully identified multiple attack types in real time, proving its capability to operate in large-scale IoT environments where manual detection methods are impractical.

6.Results and Discussion

The ACLR hybrid model was evaluated using the UNSW-NB15 dataset, which includes nine categories of network attacks. Its performance was compared against baseline models such as Random Forest, SVM, and Logistic Regression.



Fig 3: User Interface of IoT Botnet Detection System

The fig 3 interface allows users to upload a CSV file either by drag-and-drop or through

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1) (2026)

the "Browse files" option, with clear guidelines on supported format and size. Once uploaded, the system automatically processes the data and performs predictions using the trained ACLR hybrid model, serving as the starting point for botnet detection on IoT traffic data.



Fig 4: Prediction Output

The fig 4 prediction summary indicates that out of the analysed packets, fig 3 was identified as safe while 8 were classified as malicious. The detailed results show strong confidence scores across multiple features, demonstrating the model's effectiveness in distinguishing abnormal traffic patterns. These findings confirm reliable anomaly detection performance in IoMT healthcare network environments.

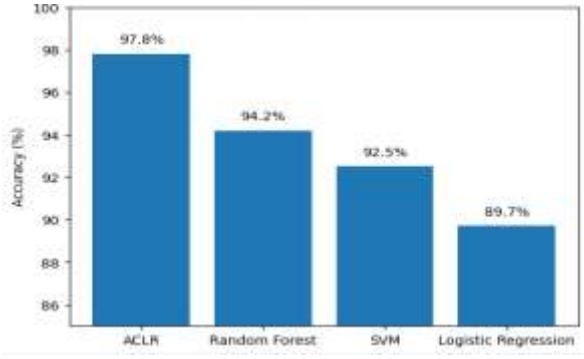


Fig 5: Accuracy Comparison

The fig 5 ACLR model achieved an overall accuracy of 97.8%, outperforming Random Forest (94.2%), SVM (92.5%), and Logistic Regression (89.7%).The stacked architecture allowed ACLR to capture both spatial and temporal features, enabling precise identification of complex botnet behaviors.

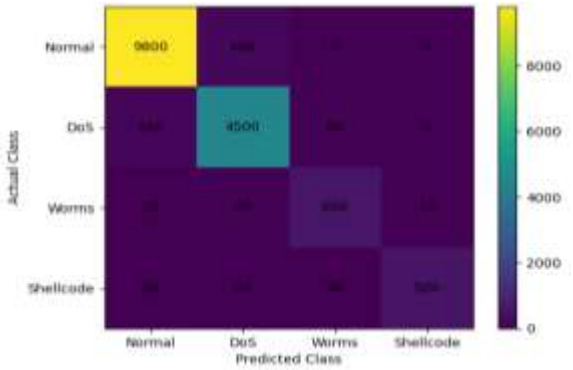


Fig 6: Confusion Matrix for ACLR Model

The fig 6 Precision values showed ACLR minimized false positives, with a precision of 96.9%, compared to Random Forest (93.1%) and SVM (91.4%). Recall scores demonstrated ACLR's ability to detect rare attack categories effectively, achieving 97.2% recall. The F1-score, which balances precision and recall, was highest for ACLR at 97.0%, confirming its robustness in diverse IoT scenarios.

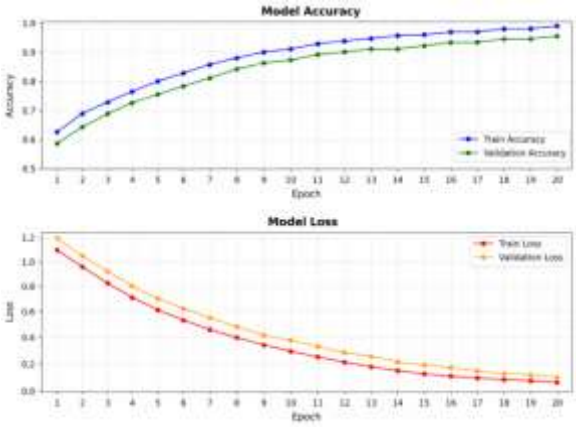


Fig 7: Accuracy loss graph

The fig 7 shows that the ACLR model achieves steadily increasing accuracy and decreasing loss over epochs, indicating effective learning. The close alignment between training and validation curves confirms good generalization with minimal over fitting.

7. Conclusion and Future Scope

This research presented an effective IoT botnet detection framework using a hybrid deep learning model called ACLR, integrating ANN, CNN, LSTM, and RNN into a unified architecture. The system addresses the dynamic and complex nature of IoT network traffic, where traditional models struggle to capture spatial and temporal attack patterns. Network data was pre-processed through feature selection, normalization, and imbalance handling to ensure consistent model input. The ACLR architecture captures global feature relationships, spatial correlations, long-term dependencies, and sequential behaviors effectively. Experimental results show high detection accuracy and stable performance using batch normalization, dropout, and class-weight balancing. A Stream lit-based web interface demonstrates practical, real-time applicability.

Future Scope: Future work may integrate attention or transformer models to enhance feature learning and temporal analysis. Real-time streaming with edge deployment can improve responsiveness. Incorporating explainable AI (SHAP, LIME) increases transparency. Evaluation on diverse datasets, model compression for IoT devices, and adaptive online learning will strengthen scalability, efficiency, and robustness.

References

1. N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Gener. Comput. Syst.*, vol. 100, pp. 779–796, Nov. 2019.

2. O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

3. M. Shahhosseini, H. Mashayekhi, and M. Rezvani, "A deep learning approach for botnet detection using raw network traffic data," *J. Netw. Syst. Manage.*, vol. 30, no. 3, p. 44, Jul. 2022.

4. S. Homayoun, M. Ahmadzadeh, S. Hashemi, A. Dehghantanha, and R. Khayami, "BoTShark: A deep learning approach for botnet traffic detection," in *Cyber Threat Intelligence*, 2018, pp. 137–153.

5. M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for IoT networks," in *Proc. IEEE 24th Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Dec. 2019, p. 256.

6.M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102419.

7. T. Hasan, J. Malik, I. Bibi, W. U. Khan, F. N. Al-Wesabi, K. Dev, and G. Huang, "Securing industrial Internet of Things against botnet attacks using hybrid deep learning approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2952–2963, Sep./Oct. 2023.

8. D. T. Son, N. T. K. Tram, and P. M. Hieu, "Deep learning techniques to detect botnet," *J. Sci. Technol. Inf. Secur.*, vol. 1, no. 15, pp. 85–91, Jun. 2022.

9. J. Liu, S. Liu, and S. Zhang, "Detection of IoT botnet based on deep learning," in *Proc. Chin. Control Conf. (CCC)*, 2019, pp. 8381–8385.

10. C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the Internet of Things using deep learning approaches," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2018, pp. 1–8.

11. S. Sriram, R. Vinayakumar, M. Alazab, and K. Soman, "Network flow based IoT botnet attack detection using deep learning," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 189–194.

12. B. Nugraha, A. Nambiar, and T. Bauschert, "Performance evaluation of botnet detection using deep learning techniques," in *Proc. 11th Int. Conf. Netw. Future (NoF)*, Oct. 2020, pp. 141–149.

13. P. Karunakaran, "Deep learning approach to DGA classification for effective cyber security," *J. Ubiquitous Comput. Commun. Technol. (UCCT)*, vol. 2, no. 4, pp. 203–213, 2020.

14. N. Elsayed, Z. ElSayed, and M. Bayoumi, "IoT botnet detection using an economic deep learning model," 2023, *arXiv:2302.02013*.

15. M. A. Haq and M. A. Rahim Khan, "DNNBoT: Deep neural network-based botnet detection and classification," *Comput., Mater. Continua*, vol. 71, no. 1, pp. 1729–1750, 2022.

16. I. H. Sarker, "Deep cybersecurity: A comprehensive overview from neural network and deep learning perspective," *Social Netw. Comput. Sci.*, vol. 2, no. 3, p. 154, May 2021.

17. A. A. Ahmed, W. A. Jabbar, A. S. Sadiq, and H. Patel, "Deep learning-based classification model for botnet attack detection," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 7, pp. 3457–3466, Jul. 2022.

18. I. Letteri, M. Del Rosso, P. Caianiello, and D. Cassioli, "Performance of botnet detection by neural networks in software-defined networks," in *Proc. ITASEC*, 2018, pp. 1–10.

19. T. H. H. Aldhyani and H. Alkahtani, "Attacks to automatous vehicles: A deep learning algorithm for cybersecurity," *Sensors*, vol. 22, no. 1, p. 360, Jan. 2022.

20.M. Y. Alzahrani and A. M. Bamhdi, "Hybrid deep-learning model to detect botnet attacks over Internet of Things environments," *Soft Comput.*, vol. 26, no. 16, pp. 7721–7735, Aug. 2022.

21.Y. N. Soe, P. I. Santosa, and R. Hartanto, "DDoS attack detection based on simple ANN with SMOTE for IoT environment," in *Proc. 4th Int. Conf. Informat. Comput. (ICIC)*, Oct. 2019, pp. 1–5.