Emerging Trends in Digital Transformation
Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-26***

HYBRID MACHINE LEARNING FRAMEWORK FOR BOTNET ATTACK DETECTION IN IOT NETWORKS

[#1]GUNTHA GIRI PRASAD, *M.Tech(SE) Student,*
[#2]Dr. V.HEMA SREE, *Professor &HoD of AI & DS,*
[#3]Mrs.T. SUBBALAKSHMAMMA, *Assistant Professor, Dept of CSE,*
VISWAM ENGINEERING COLLEGE(AUTONOMOUS), MADANAPALLE, AP.

ABSTRACT: The goal of this research is to create a hybrid machine learning model that can quickly detect botnet assaults in Internet of Things (IoT) settings. As the number of Internet of Things (IoT) devices grows, networks are more vulnerable to botnets that take advantage of device flaws and send large volumes of unsolicited traffic. Because IoT networks are complex and always changing, traditional security measures often fail to detect these kinds of threats. In order to improve identification accuracy and lower the number of false positives, the suggested method integrates a number of machine learning approaches. By combining the best elements of several algorithms, the hybrid model expertly analyzes network traffic patterns, detects unusual behavior, and arranges botnet activities. Experiments on IoT network datasets show that the proposed system performs better than single-model techniques in terms of scalability, reliability, and detection. The results show that using a combination of machine learning approaches can improve the security of the Internet of Things (IoT) and help people defend against new botnet threats.

Keywords:*Botnet attack detection, Internet of Things (IoT), Hybridmachine learning, Network security, Intrusion detection system, Cybersecurity.*

1. INTRODUCTION

The Internet of Things (IoT) has revolutionized the manner in which we communicate by connecting billions of intelligent devices, including sensors, wearable technology, industrial controls, and smart home products. These devices generate substantial quantities of data and provide substantial advantages in sectors such as transportation, healthcare, industrial automation, and smart cities. However, significant security concerns have arisen due to the proliferation of interconnected devices. A significant number of IoT devices are susceptible to hacking due to their inadequate security measures and processing capabilities. Botnet attacks have emerged as one of the most perilous risks, as attackers can remotely manage infected devices to execute harmful actions such as Distributed Denial of Service (DDoS), data theft, and network disruption.

Botnets are centralized command and control (C&C) computers that manage a collection of infected devices. Bad actors can transform a number of IoT devices into agents in an IoT environment without the users' knowledge by exploiting device vulnerabilities. When these devices are infected, they collaborate to execute coordinated attacks that can significantly compromise network security and performance. Traditional security methods, such as signature-based intrusion detection systems, are not always effective against botnet attacks that evolve over time, as they are predicated on established attack patterns. Due to this, it is imperative to develop enhanced detection algorithms that can identify botnet behaviors that are both known and unknown in IoT networks.

DOI: https://doi.org/10.65713/etdtv2i126

Machine learning (ML) algorithms are effective at identifying cyber hazards because they have the capacity to analyze large datasets and identify concealed patterns in network traffic. A variety of machine learning techniques, including Neural Networks, Support Vector Machines, Decision Trees, and Random Forest, have been employed to identify intrusions and classify malware. These methods have the capacity to detect hazardous behavior and differentiate it from typical network activity. However, the optimal outcomes may not always be achieved by relying on a single machine learning method, as various algorithms possess distinct advantages and disadvantages when addressing intricate IoT network data.

2.PROPOSED METHODOLOGY

DATASET DESCRIPTION

The University of New South Wales (UNSW) created the dataset used in this study to examine network behavior, and it was acquired via the Kaggle dataset source. A popular tool for testing intrusion detection systems in cybersecurity research is the UNSW-NB15 dataset.
There are two main files in the UNSW-NB15 dataset:

- UNSW_NB15_training-set.csv
- UNSW_NB15_testing-set.csv

These files contain network transit data that has been classified to show both good and bad behavior. Each of the 82,332 recordings in the collection relates to a different facet of network traffic.
In addition to typical traffic data, the data includes nine different categories of assault. The classes are as follows:

- Normal
- Generic
- Exploits
- Fuzzers
- DoS (Denial of Service)
- Reconnaissance
- Analysis
- Backdoor
- Shellcode
- Worms

These breaches are just one of the many harmful things that botnets may do. Consequently, the dataset offers a thorough way to assess how well deep learning and machine learning models identify cyberthreats.

TYPES OF BOTNET ATTACKS

Generic Attack: Block cipher encryption systems are the target of generic attacks, which do not take into account how they are constructed. These techniques take use of cryptographic systems' limitations on key length and block capacity. Among the methods used to get around encryption systems and obtain access without authorization are dictionary attacks, rainbow table assaults, and thorough key searches.
Exploits: Attackers use software bugs or system vulnerabilities to gain unauthorized access to network data or system resources. We call this an exploit assault. These breaches could

either make systems unusable or provide people unauthorized access to them. Because they take advantage of flaws that software developers have not yet discovered, zero-day attacks are especially harmful.

Fuzzers: When fuzzer attacks are used to find vulnerabilities, a substantial volume of random or corrupted data is sent to systems. Unexpected data flooding may cause the system to malfunction, crash, or have security flaws that could be exploited by bad actors.

Denial of Service (DoS): By flooding systems with too much data, denial of service attacks try to stop network services. This suggests that those who should be able to use network tools are unable to do so. Denial-of-service (DoS) assaults are commonly carried out by botnets. These attacks are becoming more complex thanks to machine learning capabilities.

Reconnaissance: Scouting attacks gather information about a target system before the main attack. Attackers use methods including packet sniffing, port scanning, and ping sweeps to gather information about open ports, services, and security flaws within a network.

Analysis: Analytical attacks look into how a network functions using methods like port surveillance, spam email sending, and web applications. In order to find any weaknesses that they may exploit in the future, attackers examine system behavior.

Backdoor: By getting around security barriers, backdoor attacks allow anybody to remotely access systems without authorization. Once a backdoor is created, hackers can access confidential information, carry out destructive orders, and take over a computer covertly.

Shellcode: Shellcode is a short malicious code segment used to take advantage of security flaws in software. Attackers may use it to carry out commands and take over susceptible systems.

Worms: The phrase "worm attack" describes malware that spreads over networks by taking advantage of security flaws. Worms can spread quickly to a large number of devices, using up network resources and causing serious problems.

3. LITERATURE SURVEY

Khan et al. (2025): A hybrid machine learning model that integrates classical and deep learning algorithms is introduced for the purpose of detecting IoT botnets. The methodology identifies illicit communication patterns related to botnets in the traffic data of IoT networks. Feature selection methods are implemented to enhance the accuracy of detection and decrease the complexity of computing. Experimental results indicate that the hybrid model outperforms the single-model botnet detection capability.

Santos & Oliveira (2024): This paper introduces a hybrid machine learning framework that is capable of detecting IoT botnet assaults. In order to identify dubious activities and evaluate network behavior, we implement Deep Neural Network and Random Forest models. Data preparation and traffic feature extraction are the sources of attack signs. It appears that the hybrid strategy enhances the accuracy of IoT security system detection and minimizes false positives.

Verma & Tiwari (2023): The objective of the investigation is to develop a hybrid machine learning-based intrusion detection system that can identify botnet attacks in Internet of Things environments. Artificial Neural Networks and Support Vector Machines are implemented in the proposed system to evaluate network traffic. The hybrid approach

enhances network security and detects enormous botnet attacks, as demonstrated by experimental results. The significance of advanced security protocols for IoT infrastructures is underscored in this study.

Park et al. (2022): IoT botnet intrusions are detected by a hybrid learning model that employs ensemble learning and neural networks. Botnet-like communication patterns in IoT network traffic are detected by the device. In order to enhance detection, we train machine learning algorithms with annotated datasets. The proposed architecture is more precise and efficient than conventional detection methods.

Ahmed & Rahman (2021): This paper suggests a hybrid machine learning approach for the detection of botnet incursions in smart environments that are based on the Internet of Things. Decision tree classifiers and deep learning models are employed to analyze substantial quantities of IoT network traffic data by the system. The hybrid system differentiates between benign and malevolent network activity. The model is capable of detecting botnet attacks while maintaining computational performance, as demonstrated by experimental results.

4.RELATED WORK

The security and efficacy of computer networks can be compromised by cyberattacks that read, modify, or steal critical data. IP spoofing and port surveillance are frequently employed prior to an attack. The analysis of source and destination IP addresses, ports, protocols, and packet headers can be used to identify these attacks. Attacks may be passive or aggressive, contingent upon their characteristics. Passive attacks monitor network activity for confidential information, while active attacks exploit system vulnerabilities to access or modify data.

Cyber Security

Cybersecurity is necessary to safeguard digital data, networks, and devices from internet threats. The frequency and complexity of intrusions have increased as a result of the widespread use of the internet and networked devices. When an attacker commandeers a network of hacked devices to perpetrate crimes such as data exfiltration, spam distribution, and DDoS, botnet attacks pose a significant threat to modern networks.

Anomaly detection and signature-based detection, which are conventional cybersecurity technologies, are incapable of identifying novel attacks. Sophisticated assailants, such as those who employ encrypted traffic or evasive actions, occasionally render conventional methods ineffective. In order to circumvent these constraints, researchers implement deep learning and machine learning models to identify intrusions.

Machine Learning Approaches for Botnet Attack Detection

Cyberattacks, particularly botnet attacks, are being identified through the application of machine learning. These methods can evaluate the adverse consequences of an action by analyzing network traffic data.

DOI: https://doi.org/10.65713/etdtv2i126

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-26***

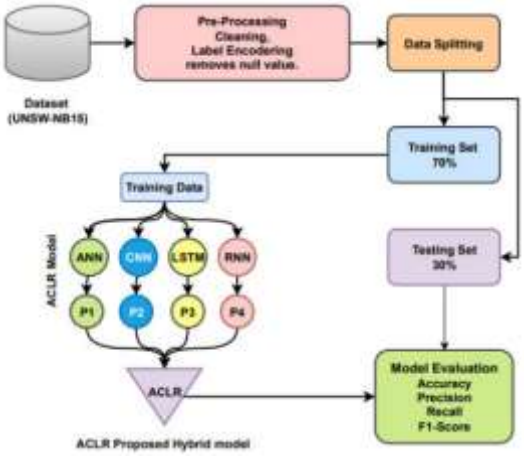


Figure1. Architecture of the proposed approach.

Artificial Neural Networks (ANN): Artificial Neural Networks are frequently employed in the classification and pattern recognition processes. They have the ability to identify intricate data connections and draw inspiration from the architecture of the brain. ANN models were evaluated by researchers on CTU-13, and they achieved a detection accuracy of approximately 99%. DDoS attacks and other network hazards can be identified using Artificial Neural Network models.

Convolutional Neural Networks (CNN): CNNs are frequently employed to extract critical features from extensive datasets. They are capable of independently recognizing network traffic patterns. The CICIDS2017 dataset was employed by researchers to identify intrusions using CNN and LSTM models, achieving a 97.16% accuracy, 97.41% precision, and 99.1% recall.

Long Short-Term Memory (LSTM): Sequential data is analyzed by recurrent neural networks, such as LSTM. It identifies patterns in time-series data, such as network traffic. In binary classification experiments, researchers employed LSTM models to accurately identify botnet domain evolution techniques with 98.7% accuracy.

Recurrent Neural Networks (RNN): RNN models are advantageous for the analysis of sequential network traffic data due to their ability to retain input knowledge. According to research, layered RNN models enhance the categorization of botnet detection systems and minimize bogus detections.

Furthermore, hybrid methodologies that integrate numerous models outperform their individual counterparts. CNN-based models identified 98.6% of peer-to-peer botnets with a false positive rate of no more than 0.5%.

DOI: https://doi.org/10.65713/etdtv2i126

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-26***

5.RESULTS

Fig5.1 User login

Fig5.2 View all remote users

Fig5.3 IOT Datasets Trained and Tested Results

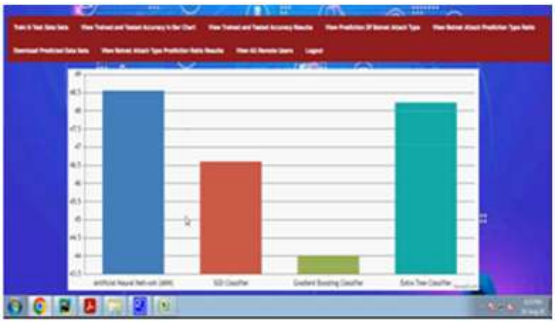
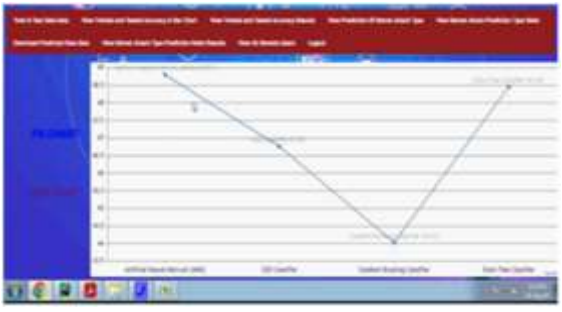


Fig5.4 Bar graph



DOI: https://doi.org/10.65713/etdtv2i126

Volume-2, Issue-1, January-March 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-26***

Fig5.5 Line chart

Fig5.6 Pie chart

Fig5.7 View Predicted Botnet Attack Type Ratio Details

6. CONCLUSION

In conclusion, the hybrid machine learning model detects IoT botnet intrusions well. Combining various approaches improves detection accuracy and reliability. IoT networks generate massive amounts of different data yet are vulnerable to assaults due to poor device security. A range of machine learning algorithms let the hybrid model evaluate network traffic patterns, identify botnet attacks (known and novel), and identify malicious activities. This strategy increases IDS performance and reduces false positives. Thus, hybrid machine learning detection solutions are necessary to protect connected devices against botnet attacks and secure the Internet of Things.

REFERENCES

[1] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, ‘‘Towards thedevelopment of realistic botnet dataset in the Internet of Things for networkforensic 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 attacksagainst 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 learningapproach 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, andR. Khayami, ‘‘BoTShark: A deep learning approach for botnet trafficdetection,’’ in Cyber Threat Intelligence, 2018, pp. 137–153.

DOI: https://doi.org/10.65713/etdtv2i126

[5] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, ‘‘Deeplearning-based intrusion detection for IoT networks,’’ in Proc. IEEE 24thPacific Rim Int. Symp. Dependable Comput. (PRDC), Dec. 2019, p. 256.
[6] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, ‘‘Deeplearning 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, andG. Huang, ‘‘Securing industrial Internet of Things against botnet attacksusing 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 techniquesto detect botnet,’’ J. Sci. Technol. Inf. Secur., vol. 1, no. 15, pp. 85–91,Jun. 2022.
[9] M. Gandhi and S. Srivatsa, ‘‘Detecting and preventing attacks usingnetwork intrusion detection systems,’’ Int. J. Comput. Sci. Secur., vol. 2,no. 1, pp. 49–60, 2008.
[10] J. Liu, S. Liu, and S. Zhang, ‘‘Detection of IoT botnet based on deeplearning,’’ in Proc. Chin. Control Conf. (CCC), 2019, pp. 8381–8385.
[11] C. D. McDermott, F. Majdani, and A. V. Petrovski, ‘‘Botnet detection inthe Internet of Things using deep learning approaches,’’ in Proc. Int. JointConf. Neural Netw. (IJCNN), Jul. 2018, pp. 1–8.
[12] S. Sriram, R. Vinayakumar, M. Alazab, and K. Soman, ‘‘Network flowbased IoT botnet attack detection using deep learning,’’ in Proc. IEEEINFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS),Jul. 2020, pp. 189–194.
[13] B. Nugraha, A. Nambiar, and T. Bauschert, ‘‘Performance evaluation ofbotnet detection using deep learning techniques,’’ in Proc. 11th Int. Conf.Netw. Future (NoF), Oct. 2020, pp. 141–149.
[14] P. Karunakaran, ‘‘Deep learning approach to DGA classification foreffective cyber security,’’ J. Ubiquitous Comput. Commun. Technol.(UCCT), vol. 2, no. 4, pp. 203–213, 2020.