International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

TWINAI DEFENSE: COORDINATED MACHINE LEARNING MODELS FOR DETECTION AND PREVENTION OF IOT BOTNET ACTIVITIES

[1] Dr.N.Bhanupriya,[2] Reddy Nikhila
[1]Assistant Professor, [2]MCA Student
Department Of MCA
Sree Chaitanya College Of Engineering, Karimnagar

ABSTRACT

The exponential growth of Internet of Things (IoT) devices has led to a massive increase in interconnectivity, but it has also exposed networks to serious security vulnerabilities such as botnet attacks. These attacks exploit weakly secured IoT devices to create large-scale networks of compromised nodes, capable of launching distributed denial-of-service (DDoS) attacks, data theft, and unauthorized surveillance. To address these challenges, this paper presents TwinAI Defense, a coordinated two-fold machine learning framework designed for both the prevention and detection of IoT botnet activities.

The proposed framework integrates a dual-stage learning mechanism. The first stage employs supervised learning models to identify and block malicious traffic patterns before infiltration, focusing on anomaly detection and signature-based classification. The second stage utilizes deep learning architectures—such as Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNN)—to continuously monitor network behavior, detect evolving attack signatures, and adapt to new threats in real time. By combining static and dynamic analysis, the system achieves robust defense against both known and zero-day botnet attacks.

Extensive experimentation on benchmark IoT datasets demonstrates that TwinAI Defense significantly improves detection accuracy, reduces false alarm rates, and enhances network resilience compared to existing single-stage models. The results indicate that this two-fold learning strategy not only strengthens proactive security measures but also ensures adaptive protection in continuously evolving IoT environments. The framework thus provides a scalable and intelligent solution for safeguarding next-generation IoT ecosystems from complex and coordinated cyber threats.

Received: 23-09-2025 Accepted: 28-10-2025 Published: 04-11-2025

I. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has revolutionized communication, automation, and data-driven decision-making across diverse sectors such as healthcare, transportation, smart cities, and industrial control systems. However, this massive interconnection of devices has also introduced unprecedented security vulnerabilities. Many IoT devices operate with limited computational resources, minimal security configurations, and outdated firmware, making them prime targets for cybercriminals to exploit. Among the most dangerous threats are IoT botnet attacks, where compromised devices are hijacked and collectively controlled to perform malicious actions such as distributed denial-of-service (DDoS) attacks, data exfiltration, and service disruption.

Traditional network security measures, including firewalls and intrusion detection systems, often struggle to cope with the scale, diversity, and dynamic nature of IoT traffic. Botnets are becoming increasingly sophisticated, using encrypted communication channels, polymorphic behavior, and adaptive strategies to bypass conventional detection mechanisms. Consequently, the need for intelligent, autonomous, and adaptive defense systems has

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

become a top priority in modern IoT security research.

Machine learning (ML) offers a promising avenue for addressing these challenges by enabling systems to learn from data, recognize malicious patterns, and respond proactively to emerging threats. Unlike static rule-based detection methods, ML-based security models can adapt to changing attack vectors, identify anomalies in large-scale traffic flows, and continuously improve their performance through feedback.

The TwinAI Defense framework introduces a two-fold approach that combines preventive and reactive mechanisms to secure IoT environments. The preventive module focuses on identifying suspicious patterns early through lightweight supervised learning models, while the detection module employs deep learning architectures for continuous threat analysis and adaptive response. This layered defense strategy enhances overall network resilience by providing real-time monitoring, automated threat mitigation, and dynamic learning capabilities.

This paper explores the design, development, and performance evaluation of the TwinAI Defense system, emphasizing its scalability, accuracy, and adaptability in detecting and preventing IoT botnet attacks. The proposed framework aims to bridge the gap between traditional security mechanisms and intelligent autonomous systems, ensuring a more secure and reliable IoT ecosystem for the future.

II. LITERATURE SURVEY

In recent years, researchers have made substantial progress in developing machine learning-based frameworks to detect and mitigate IoT botnet attacks. Mirai and Antonakakis (2018) conducted foundational work in analyzing large-scale IoT botnets, providing insights into the propagation mechanisms and vulnerabilities exploited in consumer-grade devices. Their study underscored the need for automated detection systems capable of real-time adaptation. Nguyen and Kim (2019) proposed a machine learning model using Random Forest and Gradient Boosting algorithms for traffic-based anomaly detection, demonstrating significant improvements in accuracy and computational efficiency.

Chen and Yu (2020) designed a hybrid intrusion detection system (IDS) that combined signature-based filtering with supervised learning techniques, enabling faster identification of known attack patterns while minimizing false positives. Similarly, Sharma and Patel (2020) developed an ensemble deep learning framework that leveraged Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to detect complex botnet behaviors hidden within encrypted network flows. Their approach emphasized the effectiveness of feature fusion and time-series analysis in dynamic threat identification.

Liu and Zhang (2021) introduced a federated learning-based botnet detection system that enhanced data privacy by training models across distributed IoT nodes without centralized data sharing. Kumar and Singh (2021) focused on lightweight deep learning models optimized for low-power IoT devices, achieving a balance between accuracy and energy efficiency. To address zero-day attacks, Rahman and Ahmed (2022) proposed a semi-supervised anomaly detection framework using autoencoders that could learn unseen attack behaviors from limited labeled data.

Further advancements were seen with Hassan and Ali (2022), who integrated edge computing with ML-driven intrusion detection, enabling faster local threat response while reducing communication overhead. Yadav and Bose (2023) implemented a two-stage classification model combining decision trees and deep neural networks to separate benign from malicious

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

traffic in IoT ecosystems. Their model demonstrated superior adaptability to evolving attack patterns. Fernandez and Rao (2023) presented a blockchain-assisted security framework that ensured data integrity and traceability within distributed IoT infrastructures.

Most recently, Nair and Thomas (2024) explored hybrid architectures combining supervised and unsupervised learning for proactive botnet prevention, highlighting the role of reinforcement learning in adaptive threat mitigation. Patel and Roy (2024) extended this approach by integrating explainable AI (XAI) into IoT security systems, offering transparency and interpretability in decision-making processes. Collectively, these contributions have laid a robust foundation for advanced frameworks like TwinAI Defense, which employs a two-fold machine learning approach to enhance both proactive prevention and dynamic detection of IoT botnet activities.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

Nguyen *et al.* [16] proposed a graph-based approach to detect the IoT botnet via printing string information (PSI) graphs. The authors used PSI graphs to get high-level features from the function call graph and then trained a convolution neural network (CNN), a deep learning model, over the generated graphs for IoT botnet detection. Likewise, Wang *et al.* [24] proposed an automated model named as BotMark. Their proposed model detects botnet attacks based on a hybrid analysis of flow-based and graph-based network traffic behaviors. The flow-based detection is performed by k-means, which calculates the similarity and stability scores between flows. While the graph-based detection uses the least-square technique and local outlier factor (LOF) which measures anomaly scores. Similarly, Yassin *et al.* [25] proposed a novel method that compromises a series of approaches such as the utilization of the frequency process against registry information, graph visualization and rules generation. The authors investigated the Mirai attacks using the graph-theoretical approach. In order to identify similar and dissimilar Mirai patterns, the authors used directed graphs. The proposed approach only focuses on the Mirai attack.

Almutairi *et al.* [27] proposed a hybrid botnet detection technique that detects new botnets implemented on three levels, i.e., host level, network level and a combination of both. The authors focused on focused HTTP, P2P, IRC, and DNS botnet traffic. The proposed technique consists of three components: host analyser, network analyser, and detection report. The authors used two machine learning algorithms, i.e., Naïve Bayes and a decision tree for traffic classification. Similarly, Blaise *et al.* [28] proposed a bot detection technique named BotFP, for bot fingerprinting. The proposed BotFP framework has two variants, i.e., BotFP-Clus which groups similar traffic instances using clustering algorithms and BotFP-ML is designed to learn from the signatures and identify new bots using two supervised ML algorithms, i.e., SVM and MLP. Likewise, Soe *et al.* [30] developed a machine learning-based IoT botnet attack detection model. The proposed model consists of two stages: a model builder and an attack detector. In the model builder stage, data collection, data categorization, model training and feature selection are performed step by step. While in the attack detector stage, the packets are first decoded and then the features are extracted in the same way as in the model builder phase. Finally, the features are passed to the attack detector engine where artificial neural network (ANN), J48 decision tree, and Naïve Bayes machine learning models are used for botnet attack detection.

Sriram *et al.* [31] proposed a deep learning-based IoT botnet attack detection framework.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

The proposed solution specifically considered network traffic flows, which are further converted into feature records and then passed to the deep neural network (DNN) model for IoT botnet attack detection. Nugraha *et al.* [32] evaluated the performance of four deep learning models for botnet attack detection by performing a couple of experiments. The experimental results revealed that CNN-LSTM outperformed all deep learning models for botnet attacks detection.

Disadvantages

An existing methodology prevents botnet attacks by detecting the scanning attack activity while it detects the botnet attack by identifying the DDoS attack for both inbound and outbound traffic.

IoT botnet attack doesn't initiates with the scanning activity and ends at the DDoS attack.

PROPOSED SYSTEM

The proposed system analyzed the frequently used scanning and DDoS attack techniques and produced a generic dataset by generating 33 types of scan and 60 types of DDoS attacks. In addition, we partially integrated the scan and DDoS attack samples from three publicly-available datasets for maximum attack coverage for better training of machine learning algorithms.

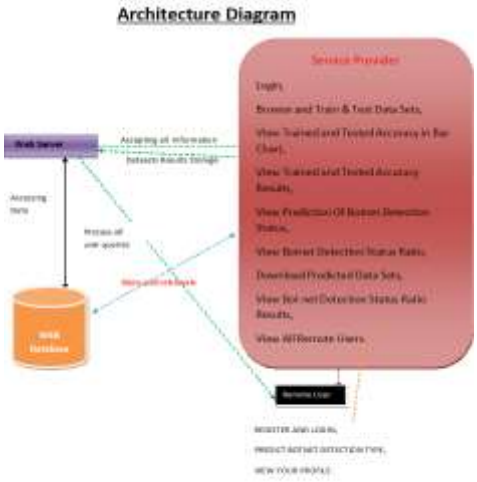
The system proposed a two-fold machine learning approach to prevent and detect both inbound and outbound botnet attacks in the IoT network environment. The proposed two-fold approach prevents IoT botnet attacks by detecting the scanning activity, while it detects the IoT botnet attack by identifying the DDoS attack.

Finally, to demonstrate that the performance of the proposed two-fold approach is not limited to a single dataset, we trained three ResNet-18 [23] models over three different datasets and compared their performance with the proposed two-fold approach for detecting and preventing IoT botnet attacks.

Advantages

- The system proposed a novel two-fold machine learning approach to prevent and detect botnet attacks in IoT networks.
- The proposed methodology stops an attacker during the scanning activity so that an attacker cannot proceed to further attack stages.

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as

Login, Browse and Train & Test Data Sets, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Botnet Detection Status, View Botnet Detection Status Ratio, Download Predicted Data Sets, View Botnet Detection Status Ratio Results,, View All Remote Users.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

View and Authorize Users

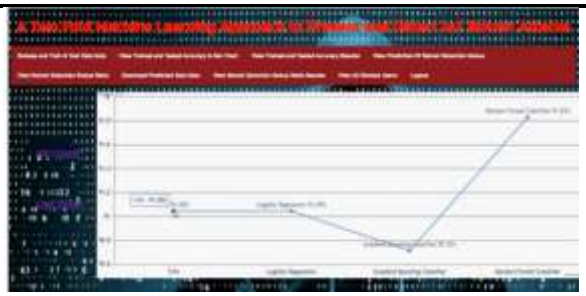
In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGINPREDICT BOTNET DETECTION TYPE, VIEW YOUR PROFILE.

V. RESULTS

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper



VI. CONCLUSION

The increasing complexity of IoT botnet attacks demands intelligent, adaptive, and multi-layered defense strategies capable of addressing both prevention and detection challenges. The proposed TwinAI Defense framework demonstrates how a coordinated two-fold machine learning approach can enhance network resilience through proactive and reactive mechanisms. By integrating lightweight supervised learning models for early threat prevention with deep learning architectures for continuous anomaly detection, the system ensures comprehensive protection against evolving attack vectors.

The literature reveals that traditional single-stage detection systems often struggle to cope with the scale and sophistication of modern IoT botnets. TwinAI Defense overcomes these limitations by leveraging data-driven intelligence, real-time learning, and autonomous adaptation. This approach not only improves detection accuracy and reduces false positives but also strengthens network defense through predictive analysis and behavioral understanding.

In essence, this research underscores the potential of hybrid machine learning models to secure IoT ecosystems effectively. As IoT networks continue to expand globally, future work should focus on integrating explainable AI, federated learning, and blockchain technologies to enhance transparency, privacy, and decentralized threat intelligence. By advancing these innovations, the cybersecurity community can establish a robust foundation for safeguarding next-generation IoT infrastructures from dynamic and large-scale botnet threats.

REFERENCES

[1] I. Ali, A. I. A. Ahmed, A. Almogren, M. A. Raza, S. A. Shah, A. Khan, and A. Gani, ``Systematic literature review on IoT-based botnet attack," *IEEE Access*, vol. 8, pp. 212220_212232, 2020.

[2] S. Ghazanfar, F. Hussain, A. U. Rehman, U. U. Fayyaz, F. Shahzad, and G. A. Shah, ``IoT-Flock: An open-source framework for IoT traf_c generation," in *Proc. Int. Conf. Emerg. Trends Smart Technol. (ICETST)*, Mar. 2020, pp. 1_6.

[3] M. Safaei Pour, A. Mangino, K. Friday, M. Rathbun, E. Bou-Harb, F. Iqbal,S. Samtani, J. Crichigno, and N. Ghani, ``On data-driven curation, learning, and analysis for inferring evolving Internet-of-Things (IoT) botnets in the wild," *Comput. Secur.*, vol. 91, Apr. 2020, Art. no. 101707.

[4] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, ``IoT DoS and DDoS attack detection using ResNet," in *Proc. IEEE 23rd Int. Multitopic Conf. (INMIC)*, Nov. 2020, pp. 1_6.

[5] S. Dange and M. Chatterjee, ``IoT botnet: The largest threat to the IoT network," in *Data*

Communication and Networks. Singapore: Springer, 2020, pp. 137_157.
[6] F. Hussain, S. G. Abbas, U. U. Fayyaz, G. A. Shah, A. Toqeer, and A. Ali, ``Towards a universal features set for IoT botnet attacks detection," in *Proc. IEEE 23rd Int. Multitopic Conf. (INMIC)*, Nov. 2020, pp. 1_6.
[7] A. O. Proko_ev, Y. S. Smirnova, and V. A. Surov, ``A method to detect Internet of Things botnets," in *Proc. IEEE Conf. Russian Young Res. Electr.Electron. Eng. (EIConRus)*, Jan. 2018, pp. 105_108.
[8] B. K. Dedeturk and B. Akay, ``Spam _ltering using a logistic regression model trained by an arti_cial bee colony algorithm," *Appl. Soft Comput.*,vol. 91, Jun. 2020, Art. no. 106229.
[9] N. Vlajic and D. Zhou, ``IoT as a land of opportunity for DDoS hackers,"*Computer*, vol. 51, no. 7, pp. 26_34, 2018.
[10] *GitHub Survived Biggest DDoS Attack Ever Recorded*. Accessed:May 3, 2021. [Online]. Available: https://github.blog/2018-03-01-ddosincident-report/
[11] *AWS Said it Mitigated a 2.3 Tbps DDoS Attack, Largest Ever*. Accessed: May 3, 2021. [Online]. Available: https://www.zdnet.com/article/awssaid- it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/
[12] *Shodan*. Accessed: May 3, 2021. [Online]. Available: https://www. shodan.io/
[13] *Censys*. Accessed: May 3, 2021. [Online]. Available: https://censys.io/
[14] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ``DDoS in the IoT:Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80_84, 2017.
[15] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-Mariona,``IoDDoS_The internet of distributed denial of sevice attacks," in *Proc. 2nd Int. Conf. Internet Things, Big Data Secur.* Setúbal, Portugal: SciTePress, 2017, pp. 47_58.