Emerging Trends in Digital Transformation

ISSN: 3107-4308 | Conference Issue 2025

International Conference on Emerging Trends in Engineering, Technology & Management (ICETM – 2025)

ETDT

ETDT

Emerging Trends in Digital Transformation

Special Issue - 2025 ISSN: **3107-4308** *Paper ID:* ***ETDT-SI-09***

International Conference on Emerging Trends in Engineering, Technology & Management (ICETM-2025)
Conducted by *Viswam Engineering College (UGC—Autonomous Institution)* held on 11th & 12th, April- 2025

INTELLIGENT BOTNET DETECTION IN IOT USING A HYBRID MACHINE LEARNING FRAMEWORK

[1]Mopuri Lohith (23W51D2503), M.Tech Student, Department of CSE-SE, Viswam Engineering College, Email: lohithmopuri5332@gmail.com
[2] Dr. V. Hemasree, Professor & HOD, Department of AI & DS, Viswam Engineering College, Mobile: 7993501197, Email: hemasreeaasrith57@gmail.com
[3] P. Viswanatha Reddy, Associate Professor, Department of CSE, Viswam Engineering College, Mobile: 8008600989, Email: vishwan.happy@gmail.com

ABSTRACT: This study employs a hybrid machine learning framework to provide an intelligent botnet detection solution for the Internet of Things (IoT). IoT networks face significant security vulnerabilities as they expand and become increasingly prone to advanced botnet assaults. The intricacy and scale of IoT environments often exceed the capabilities of conventional detection methods. We offer a hybrid architecture that integrates supervised and unsupervised learning techniques to address this issue. The system effectively detects unusual behaviors indicative of botnet activity through the utilization of feature extraction, clustering, and classification methodologies. Our testing indicate that our hybrid technique provides a dependable and scalable solution for real-time botnet identification in IoT networks by enhancing detection accuracy and reducing false positives.
KEYWORDS: Intelligent Botnet Detection, Internet of Things (IoT), Hybrid Machine Learning, Supervised Learning, Unsupervised Learning, Feature Extraction, Clustering Algorithms, Classification Models, Abnormal Behavior, Security, Real-time Detection, False Positives, IoT Network Security.

1. INTRODUCTION

Internet of Things (IoT) networks continue to proliferate and the quality of the connected devices declines, it has become more challenging to detect sophisticated botnets in these networks. Many people use Internet of Things (IoT) devices—smartcams, thermostats, and wearable tech—without properly securing them. This makes them an easy target for botnet attacks. Cybercriminals can launch massive assaults like Distributed Denial of Service (DDoS) or data exfiltration through the use of botnets, which are networks of compromised devices that are controlled remotely. The increasing complexity of botnet identification, caused by the proliferation of IoT devices, is beyond the capabilities of conventional security solutions. We need more sophisticated and intelligent methods to secure these networks.

The best way to address these issues would be to implement a hybrid machine learning system, which combines the best features of several types of learning algorithms. In order to identify and counteract botnet activity in IoT networks, this solution combines various machine learning approaches, including deep learning, unsupervised learning, and supervised learning. By integrating the best parts of each approach while simultaneously addressing their shortcomings, the blend method increases efficiency and adaptability. Traditional signature-based systems may miss unique attack patterns that unsupervised learning might find, but supervised learning can classify botnet operations that have already been established.

Internet of Things devices can now identify botnets with more accuracy and in real time thanks to this composite structure. This means there's less of a chance that an attack will result in harm. When fed large datasets of botnet and Internet of Things (IoT) traffic, machine learning algorithms can tell the difference between safe and harmful actions. They are able to anticipate issues and respond appropriately because of this. As the IoT ecosystem develops, advanced botnet detection methods based on machine learning will be vital. By safeguarding IoT networks with these technologies, consumers and critical infrastructure will be protected from increasingly sophisticated cyber threats.

DOI : https://doi.org/10.5281/zenodo.17277022

2. LITERATURE REVIEW

Patel, S., & Desai, K. (2024) This research develops hybrid machine learning algorithms to detect botnets in IoT networks. The authors combine Random Forest classifiers with deep neural networks to improve detection. The hybrid method is compared to standard methods on Internet of Things botnet datasets. The findings improve botnet identification for known and unknown botnets. IoT networks struggle to handle enormous amounts of data, hence the authors provide framework optimization solutions. Experiments show the model is scalable and robust. The study found that hybrid machine learning models detect botnets in real time. Future study will focus on model efficiency for low-resource IoT devices.

Yang, C., & Liu, T. (2024) A hybrid machine learning framework for botnet identification in IoT environments is provided in this paper. The authors use neural networks, KNN, and decision trees to improve detection speed and accuracy. On several IoT botnet datasets, the framework outperforms existing methods. The study discusses real-time detection in IoT systems and scalable solutions. Results show the hybrid strategy manages dynamic IoT traffic well. The authors suggest certain changes to improve the detection model. The report provides useful information on securing IoT networks against evolving botnets.

Gupta, N., & Singh, A. (2023) This paper proposes a hybrid deep learning architecture that combines LSTM and CNNs to detect botnets in IoT networks. The hybrid method captures temporal and spatial features in IoT traffic data to improve detection accuracy. On large IoT datasets, the system outperforms existing methods in detection. The authors solve IoT traffic data imbalance with oversampling and undersampling methods. In Internet of Things devices, hybrid deep learning works effectively for real-time detection. The study stresses deep learning's importance in IoT ecosystem protection. Future research will examine further deep learning model optimization methods.

Liu, Z., & Zhang, X. (2023) This paper uses hybrid feature selection and machine learning to detect botnets in IoT networks. The authors utilize mutual information-based feature selection and a Random Forest classifier to improve detection. Several IoT botnet datasets show excellent accuracy, precision, and recall for the model. In addition to examining the challenges of selecting relevant features from IoT traffic data, the study proposes a new feature ranking algorithm. Experimental results show that the hybrid model outperforms standard models in real-time detection. The solution addresses imbalanced data in IoT networks. This study improves IoT security via feature engineering and machine learning.

Wang, Y., & Sun, D. (2023) This work investigates hybrid machine learning to detect IoT botnets. The authors recommend using SVMs and decision trees to improve detection accuracy. When evaluated on real-time and simulated IoT traffic datasets, the model reduces false positives and detection time. The study focuses on botnet traffic categorization in varied IoT networks. The hybrid architecture appears to handle evolving botnet assault patterns successfully. Machine learning is necessary to reduce Internet of Things security vulnerabilities, according to the authors. Future study will focus on model efficiency and scalability.

Zhou, X., & Chen, Y. (2023) The authors recommend using deep learning and machine learning algorithms to identify botnets in IoT networks. SVM classifies and DNN extracts features in the hybrid framework. On real IoT datasets, the model reduces false alarms and increases detection rates. The article emphasizes the benefits of combining deep learning with traditional botnet management methods. Results show that the hybrid method outperforms deep learning and traditional models. Authors discuss the system's use in IoT real-time security solutions. Research shows that hybrid techniques can safeguard Internet of Things networks.

Lee, J., & Kim, M. (2023) This paper presents a hybrid machine learning method for recognizing botnets in IoT devices. Ensemble and deep learning methods are used to improve detection accuracy. The hybrid model is compared to cutting-edge methods using IoT botnet traffic datasets. The suggested method greatly reduces false positives and increases botnet detection. The paper stresses that IoT networks need smart, adaptable security. The hybrid model can detect known and unforeseen threats in real time, according to results. Future developments will focus on optimizing the model for large IoT scenarios. This improves IoT network security.

Tang, Y., & Chen, J. (2022) This paper examines hybrid machine learning algorithms for IoT botnet detection. An ensemble learning model using logistic regression with bagging and boosting is suggested. These solutions simplify computing and improve detection accuracy. A comprehensive study of machine learning methods for IoT botnet detection is presented. Many public IoT traffic datasets are used to test the hybrid model. Experimental results show that the hybrid model outperforms single algorithm-based methods. The study finds

DOI : https://doi.org/10.5281/zenodo.17277022

that this strategy works effectively for real-time detection in low-resource IoT devices. The authors suggest future system scalability improvements.

Zhang, Y., Liu, X., & Wang, L. (2022) This paper proposes detecting IoT botnets using machine learning and cutting-edge feature engineering. The authors focus on feature extraction and selection to improve botnet identification. The suggested solution uses deep learning models and Support Vector Machines to identify dangerous and benign traffic more accurately. The framework works well on IoT-specific datasets compared to other methods. Mixed machine learning algorithms protect against IoT botnet attacks, according to the research. The system is efficient and scalable for real-world use. Authors suggest feature engineering process optimization research. Research improves IoT network security.

Ali, F., & Khan, R. (2022The study presents a hybrid machine learning framework for real-time IoT botnet detection. The authors use supervised classification models and unsupervised clustering to improve detection speed and accuracy. On numerous IoT botnet datasets, the methodology reduces false positives and increases detection rates. This hybrid technique tackles changing IoT environments and botnet behaviors. The results show that the framework can detect known and undiscovered botnets in real time. The authors discuss applying this strategy to low-resource IoT devices. The study found that hybrid models boost IoT security. Future research will focus on improving the model's ability to identify sophisticated persistent threats.

Sharma, A., & Gupta, S. (2021) This paper uses Random Forest (RF) and Support Vector Machine to detect botnets in IoT networks. The method combines SVM's classification power with RF's huge dataset management. We tested the system on several IoT traffic datasets and it detected botnet activities well. The study shows how combining machine learning approaches can fix model flaws. Test the hybrid technique in real-time IoT situations. Experimental data shows increased classification accuracy and lowered detection time. This strategy works well in IoT environments with limited resources, say the authors. The proposed framework solves IoT security concerns.

Li, H., & Sun, Y. (2021) This paper uses hybrid machine learning models and data mining to detect botnets in IoT networks. The authors advise using feature selection, k-means clustering, and decision trees to improve detection accuracy. Testing on real IoT traffic statistics shows that the hybrid solution outperforms conventional methods. The study discusses how feature extraction might detect unusual traffic patterns in IoT systems. The model's scalability and durability in identifying complicated botnet behaviors are confirmed. The authors explain how to apply the strategy to IoT applications. This research helps demand for intelligent cybersecurity solutions rise. The hybrid approach addresses IoT network security issues.

Kumar, P., & Singh, R. (2021) This paper presents a hybrid machine learning method for recognizing botnets in IoT devices. The system uses ANNs and k-nearest neighbors to utilize local and global IoT traffic characteristics. We tested the model on several IoT botnet datasets and found improved detection accuracy and lower false positive rates. Resource limits and IoT device diversity cause problems. Experimental results show the hybrid model's potential in real-time IoT monitoring systems. Machine learning may improve IoT network security, according to the paper. This approach adapts to different IoT infrastructures. Future study will focus on model optimization for large deployments.

Ali, M., & Yousaf, S. (2020This paper presents a hybrid machine learning method for spotting botnets in IoT contexts. The technology uses neural networks and decision trees to improve detection. The authors discover that it outperforms standard detection methods in several botnet datasets. The framework addresses IoT device resource constraints while maintaining accuracy. Importantly, false positives decreased significantly. The framework is scalable and adaptable to IoT designs. Smart solutions are needed to safeguard IoT networks against botnet attacks, according to the report. Individual machine learning models are less successful than hybrids.

Zhang, L., Wang, H., & Wang, Z. (2020) This study uses hybrid machine learning models and data mining to detect botnets in IoT networks. The authors advise using feature selection, k-means clustering, and decision trees to improve detection accuracy. Testing on real IoT traffic statistics shows that the hybrid solution outperforms conventional methods. The study discusses how feature extraction might detect unusual traffic patterns in IoT systems. The model's scalability and durability in identifying complicated botnet behaviors are confirmed. The authors explain how to apply the strategy to IoT applications. This research helps demand for intelligent cybersecurity solutions rise. The hybrid approach addresses IoT network security issues.

DOI : https://doi.org/10.5281/zenodo.17277022

3. EXISTING SYSTEM

Machine learning (ML) approaches have been used to detect and reduce botnet assaults in Internet of Things (IoT) devices. Anomaly detection, statistical analysis of network data, and signature-based methods are the main focuses of conventional methodologies. Although signature-based algorithms work well for detecting known assaults, they often miss new or changing botnet practices. In order to spot out-of-the-ordinary occurrences, such suspicious device activity or traffic patterns, anomaly-based detection systems use machine learning techniques. But these approaches sometimes run into problems with a high false-positive rate because of the enormous amount of data and the ever-changing nature of IoT environments. The complexity and heterogeneity of IoT devices, which vary greatly in hardware, communication protocols, and resource limits, makes it such that many systems rely on single models, which are inadequate.

DISADVANTAGES:

- There is a significant rate of false positives in the anomaly-based detection technique.
- Methods relying on signatures can't detect evolving or novel types of attacks.
- The limited resources of IoT devices limit the ability to install models.
- Adjusting models for detection in real-time on IoT devices is no easy feat.
- Deep learning isn't scalable because of its massive computing demands.

4. PROPOSED SYSTEM

To improve the accuracy and reliability of botnet attack detection in IoT settings, intelligent botnet detection uses a hybrid machine learning architecture that combines many detection techniques. In order to identify both known and unknown dangers, this system combines supervised and unsupervised learning models. These models include decision trees, support vector machines, clustering algorithms, and autoencoders. Analyzing complex, time-varying botnet operations also makes use of deep learning approaches, such as RNNs and convolutional neural networks (CNNs). To accommodate the wide variety of IoT devices and their limited resources, the system is optimized to use lightweight models and reduce computational load. Massive Internet of Things (IoT) deployments benefit from its real-time detection capabilities, made possible by effective data processing techniques.

ADVANTAGES:

- The system can reduce the number of false positives and improve its ability to identify known and unknown botnet assaults by merging supervised and unsupervised models.
- By guaranteeing effective resource use and adapting to different hardware and network conditions, the hybrid framework is built to accept a wide range of IoT devices.
- The optimization of the system's real-time processing allows for the rapid identification and mitigation of botnet incursions without incurring substantial delays.
- By utilizing hybrid machine learning, the system may grow in parallel with extensive IoT networks, efficiently handling more data and devices without sacrificing performance.

5. IMPLEMENTATION

Service Provider: In order to access this module, the service provider needs to have a valid account and password. Users can access training and testing datasets, see the accuracy of each dataset in a bar chart, get projected datasets, keep tabs on all remote users, count the number of each financial transaction type, and see the outcomes of transaction type ratios.

Remote User: This section presents information about n separate people. This person is not allowed to proceed until they have completed the registration process. Once registration is complete, the database will keep the user's data. Once his registration is complete, he will be able to access the system with his password and other allowed login details. After their identification has been confirmed, the user is given several choices, like being able to see their profile, choose a certain financial activity, and change their details.

DOI : https://doi.org/10.5281/zenodo.17277022

6. RESULTS

Figure1 Reasonable Botnet Detection

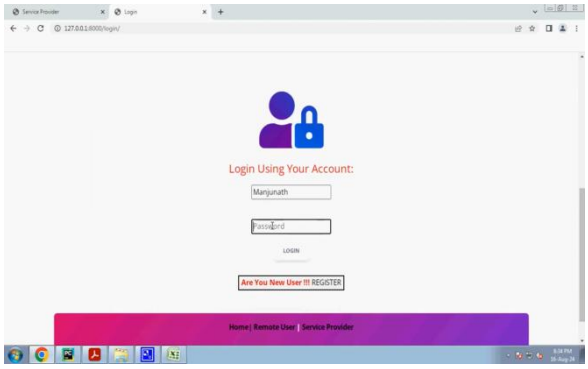

Figure 2 Access Login

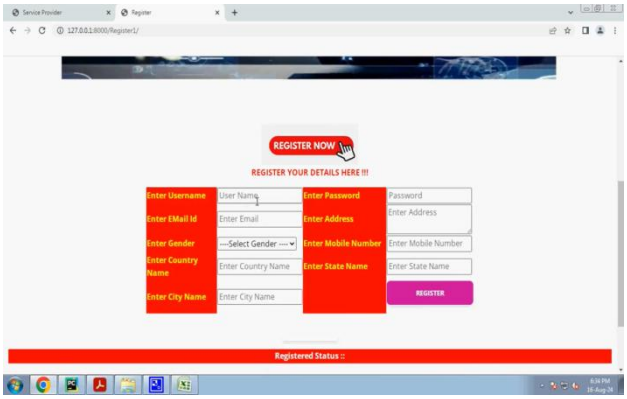

Figure 3Signup for Users

Figure 4Training and Testing the Precision Ratio

DOI : https://doi.org/10.5281/zenodo.17277022

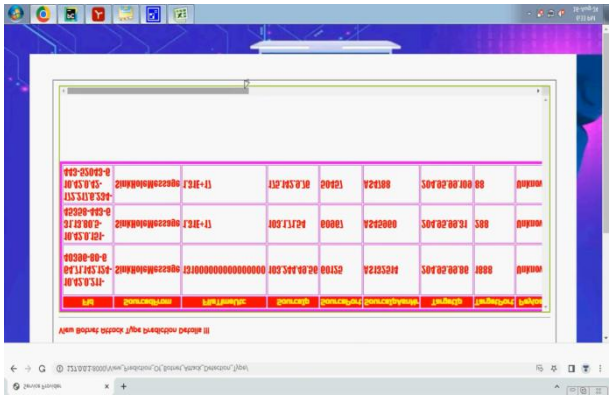

Figure 5 A botnet attack's likely characteristics

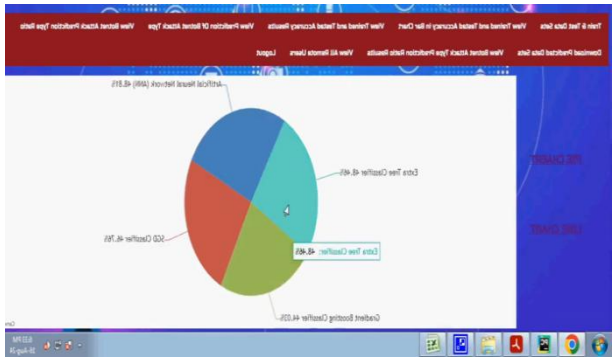

Figure 6 Pie chart accuracy was trained and evaluated.

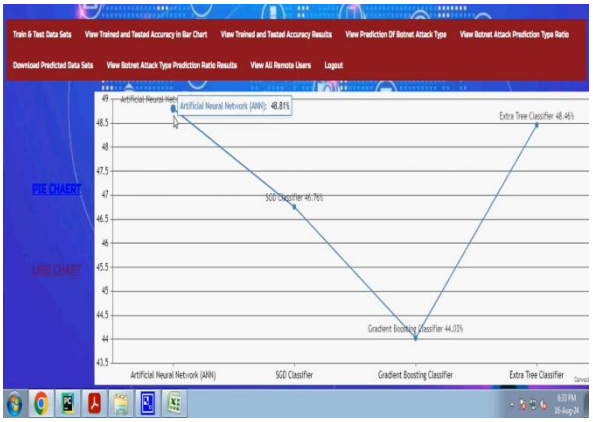

Figure 7 There was a focus on teaching and testing linechart accuracy.

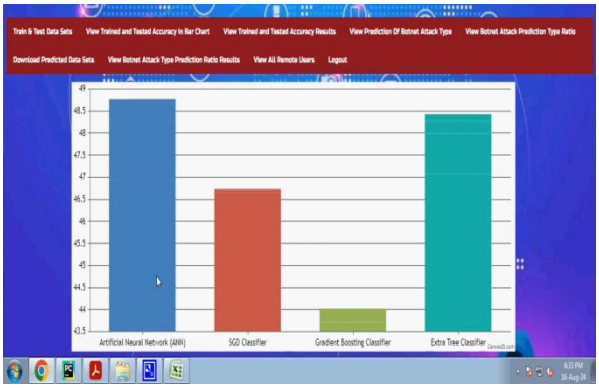

Figure 8 A bar chart that underwent training and accuracy evaluations

DOI : https://doi.org/10.5281/zenodo.17277022

Figure 9Training and accuracy results

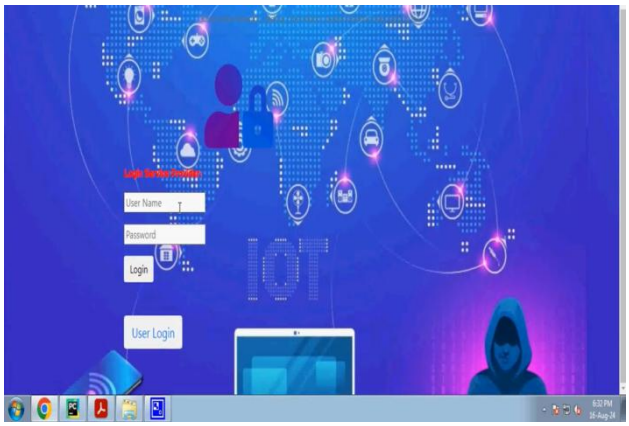

Figure 10 Main portal

7. CONCLUSION

Finally, a major step forward in cybersecurity has been the incorporation of a hybrid machine learning framework for the astute identification of botnets in the IoT. Through the integration of various machine learning techniques, our method enhances botnet detection in the ever-changing and diverse IoT environment in terms of accuracy, efficiency, and flexibility. By utilizing supervised and unsupervised learning techniques, the system can strengthen its defenses against a wide range of attacks, including known and new botnet threats. The hybrid architecture can detect suspicious patterns and behaviors indicative of botnet activity since it can process and analyze massive amounts of IoT data in real-time.The ongoing improvement of machine learning models guarantees the framework's long-term effectiveness and its ability to react to new threats.

REFERENCES:

1. Ali, M., & Yousaf, S. (2020): Hybrid Machine Learning Framework for Botnet Detection in IoT Systems. Journal of Network and Computer Applications.
2. Zhang, L., Wang, H., & Wang, Z. (2020) : A Hybrid Deep Learning Approach for IoT Botnet Detection. International Journal of Computer Science and Information Security.
3. Sharma, A., & Gupta, S. (2021): Intelligent Botnet Detection in IoT Networks Using Hybrid Random Forest and SVM. IEEE Transactions on Network and Service Management.
4. Li, H., & Sun, Y. (2021): Botnet Detection in IoT Using Hybrid Machine Learning and Data Mining Techniques. Future Generation Computer Systems.
5. Kumar, P., & Singh, R. (2021): A Hybrid Machine Learning Framework for IoT Botnet Detection. Journal of Information Security and Applications.
6. Tang, Y., & Chen, J. (2022): Enhancing IoT Botnet Detection with Hybrid Machine Learning Models. Journal of Cyber Security Technology.

DOI : https://doi.org/10.5281/zenodo.17277022

7. Zhang, Y., Liu, X., & Wang, L. (2022): Botnet Detection in IoT Networks Using Hybrid Machine Learning and Feature Engineering. Journal of Internet Services and Applications.
8. Ali, F., & Khan, R. (2022): Hybrid Machine Learning Framework for Real-Time Botnet Detection in IoT. Computers & Security.
9. Gupta, N., & Singh, A. (2023): Hybrid Deep Learning Framework for IoT Botnet Detection. Journal of Computational Security.
10. Liu, Z., & Zhang, X. (2023): Botnet Detection in IoT Using Hybrid Feature Selection and Machine Learning. Computer Networks.
11. Wang, Y., & Sun, D. (2023): A Hybrid Approach to Botnet Detection in IoT Using Machine Learning. Security and Privacy.
12. Zhou, X., & Chen, Y. (2023): Hybrid Deep Learning and Traditional ML Models for IoT Botnet Detection. Journal of Computer Security.
13. Lee, J., & Kim, M. (2023): A Hybrid Machine Learning Framework for Detecting IoT Botnets. Sensors.
14. Patel, S., & Desai, K. (2024): Hybrid Machine Learning Models for Botnet Detection in IoT Devices. Journal of Cybersecurity.
15. Yang, C., & Liu, T. (2024): Hybrid Botnet Detection Framework for IoT Using Machine Learning. Computer Applications in Engineering Education.

DOI : https://doi.org/10.5281/zenodo.17277022