JDEBM
Journal of Digital Engineering and Business Managemet

Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/08
DOI: https://doi.org/10.5281/zenodo.19081096

HYBRID MACHINE LEARNING STRATEGIES FOR IOT BOTNET DETECTION

[#1]J. SWATHI, ***Associate Professor & HOD,***
[#2]J. SRINIVAS, ***Assistant Professor,***
[#3]MD ZIAUDDIN, ***Assistant Professor,***
[#4]J. ANJALI, ***Assistant Professor,***
Department of Computer Science And Engineering,
TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TG.

ABSTRACT: A hybrid machine learning framework is used in this study to make an intelligent botnet detection system for the Internet of Things (IoT). There are big security risks for IoT networks as they grow and become easier for advanced botnet attacks to break into. Most of the time, IoT settings are too big and complicated for old-fashioned detection methods to work. To solve this issue, we suggest a mixed architecture that includes guided and unguided ways of learning. Using methods like feature extraction, clustering, and classification, the system is able to spot strange behaviors that could be signs of botnet activity. Our tests show that our hybrid method is a good and scalable way to find botnets in real time in IoT networks because it improves detection accuracy and lowers 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 are proliferating, and as a result, it is becoming more difficult to detect sophisticated botnets within these systems. Many Internet of Things (IoT) devices, such as smartcams, thermostats, and wearable gadgets, are used without adequate security measures. This makes them easy prey for botnet operations. Botnets are networks of compromised computers that hackers can remotely command to conduct massive assaults like Distributed Denial of Service (DDoS) or steal sensitive information. Because there are so many IoT devices, traditional security solutions aren't able to handle the increasing complexity of botnet detection. To ensure the security of these networks, more advanced and intelligent approaches are required. An effective solution to these issues could be a hybrid machine learning system that integrates the most advantageous aspects of multiple learning approaches. To identify botnet activity in IoT networks and halt it, this approach employs a combination of supervised learning, deep learning, and unsupervised learning. Because it incorporates the greatest features of each strategy while simultaneously addressing their shortcomings, the mix method enhances flexibility and effectiveness. While supervised learning can classify botnet activity as it happens, traditional signature-

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/08
DOI: https://doi.org/10.5281/zenodo.19081096

based systems may miss out on unusual attack patterns that unsupervised learning may identify.

With this unified framework, IoT devices could detect botnets more precisely and in real time. An attack is less likely to result in harm as a result of this. Algorithms trained with massive volumes of data from botnets and the Internet of Things (IoT) can distinguish between harmless and harmful actions. They are better able to foresee issues and take appropriate action as a result. Modern, machine-learning-based botnet detection techniques are essential for the expansion of the Internet of Things (IoT) ecosystem. Protecting vital resources, individuals, and IoT networks from more sophisticated threats is the goal of these solutions.

2. LITERATURE REVIEW

Patel, S., & Desai, K. (2024) This study combines two forms of machine learning to detect botnets in IoT networks. Integrating Random Forest classifiers with deep neural networks, the authors enhance recognition. To evaluate the hybrid methodology, we compare it to conventional methods using datasets from botnets that operate on the Internet of Things. The findings facilitate the identification of both known and unknown botnets. Due to the difficulty in managing large amounts of data in IoT networks, the authors present strategies for optimizing the framework. The results of the experiments prove that the model is robust and suitable for large-scale applications. The study found that synthetic ML models could detect botnets instantly. The effectiveness of models for low-resource Internet of Things devices will be the primary focus of the upcoming study.

Yang, C., & Liu, T. (2024) The authors of this paper recommend a combination of machine learning techniques for detecting botnets in IoT applications. The writers increase the detection efficiency and speed by using neural networks, decision trees, and KNNs. On several Internet of Things (IoT) botnet datasets, the solution outperforms state-of-the-art approaches. The study examines a number of topics, including real-time monitoring and scalable solutions in IoT systems. According to the results, the hybrid approach works fine with dynamic IoT traffic. The authors offer some suggestions for improving the detection model. In order to protect IoT networks against evolving botnets, the study provides helpful information.

Gupta, N., & Singh, A. (2023) The authors propose a hybrid deep learning architecture that uses both long short-term memories (LSTMs) and convolutional neural networks (CNNs) to detect botnets in IoT networks. In order to improve the accuracy of detection, the hybrid technique merges spatial and temporal data with data from the Internet of Things (IoT). Compared to existing detection approaches, the approach outperforms them on extremely big IoT datasets. To correct the data imbalance in the IoT traffic, the writers employ both undersampling and oversampling methods. With the help of hybrid deep learning, IoT devices can more easily locate objects in the actual world. Deep learning is crucial for safeguarding IoT communities, as demonstrated by the study. Research in the future will center on developing novel

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/08
DOI: https://doi.org/10.5281/zenodo.19081096

approaches to enhancing deep learning models.

Liu, Z., & Zhang, X. (2023) By combining machine learning with feature selection, this study is able to detect botnets in IoT networks. Using a Random Forest classifier with mutual information-based feature selection, the writers enhance detection. The accuracy, precision, and memory of the model are exceptional across several Internet of Things botnet data sets. An innovative method for ranking features is proposed in the study, which addresses the difficulty of extracting valuable information from IoT traffic data. When compared to conventional models, the hybrid model performs better in real-time recognition, according to the experiments. When data transmission errors occur in IoT networks, this approach can solve them. This study demonstrates how machine learning and feature engineering can enhance the security of the Internet of Things.

Wang, Y., & Sun, D. (2023) Finding Internet of Things (IoT) botnets using mixed machine learning is the focus of this study. The authors propose using support vector machines (SVMs) and decision trees to boost detection efficiency. Experimental results on both real-time and simulated IoT traffic datasets show that the system is able to locate objects more quickly and with fewer false positives. The study's overarching objective is to classify botnet behavior across various IoT networks. The hybrid approach works very effectively, it turns out, when dealing with botnet attacks that exhibit ever-changing patterns. To allay fears about IoT security, the authors argue that machine learning must be used alongside the network. The ease and efficacy of the model's use on a bigger scale will primarily be the focus of future research.

Zhou, X., & Chen, Y. (2023) Deep learning and machine learning can be used to find botnets on IoT networks, say the writers. A hybrid structure is one in which DNN extracts features and SVM classifies them. Using this approach on real-world IoT datasets reduces the amount of false positives and increases the rate of detection. Combining deep learning with more conventional methods of botnet control has several advantages, as discussed in the article. Compared to the conventional model and the deep learning model, the results demonstrate that the hybrid approach is superior. More specifics regarding the method's potential application in developing IoT security solutions for real-time are provided by the authors. Multiple approaches can be used to ensure the security of Internet of Things networks, according to researchers.

Lee, J., & Kim, M. (2023) This research demonstrates a novel approach to detecting botnets in IoT devices by combining various machine learning methods. Ensemble and deep learning techniques are employed to enhance the accuracy of recognition. The hybrid model is tested using modern technologies and data collected from IoT botnet traffic. The proposed approach significantly reduces false positives while simultaneously improving botnet detection. The research highlights the significance of smart, adaptable security for IoT networks. The results demonstrate that the mixed model is capable of real-time risk detection for both known and unknown variables. Improving the model's performance in

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/08
DOI: https://doi.org/10.5281/zenodo.19081096

large-scale IoT scenarios will constitute the primary focus of future research efforts. Internet of Things networks are thus more secure.

Tang, Y., & Chen, J. (2022) This study examines the use of mixed machine learning techniques to detect IoT botnets. A logistic regression ensemble learning model incorporating both bagging and boosting is highly recommended. These techniques not only speed up the procedure, but they also increase the detection accuracy. Looking at machine learning techniques for detecting botnets in the IoT is the focus of this article. To put the hybrid model to the test, we use a variety of publicly available IoT traffic logs. The hybrid model outperforms the individual algorithm-based approaches in the experiments. The research proves that this approach is effective for low-resource Internet of Things (IoT) devices to do real-time recognition. The authors recommend enhancing the system's scalability for future use.

Zhang, Y., Liu, X., & Wang, L. (2022) According to the paper, advanced feature engineering and machine learning should be employed to detect IoT botnets. In order to make botnet detection easier, this research focuses on extracting and selecting features. The proposed method distinguishes between risk-free and hazardous traffic using deep learning models and Support Vector Machines. More specifically, the approach outperforms alternatives for IoT-specific datasets. The study's findings demonstrated that hybrid machine learning techniques can ward off botnet assaults on the Internet of Things. The method is effective and can be tailored to address practical requirements. The authors believe that there has to be additional research on how to enhance the feature engineering process. Internet of Things (IoT) network security is an area of active investigation.

Ali, F., & Khan, R. (2022 The research demonstrates a novel ML system that can detect botnets operating on the Internet of Things (IoT) in near real-time. The authors utilize a combination of supervised and unsupervised clustering techniques to boost detection speed and accuracy. Across several different Internet of Things (IoT) botnet datasets, the approach improves detection rates while decreasing false positive rates. This hybrid approach considers both the evolution of botnets and the evolution of IoT configurations. The outcomes demonstrate that the system is capable of discovering new and existing botnets instantly. Using this approach on low-power Internet of Things devices is something the authors discuss. Blended designs make the Internet of Things safer, according to the study. Improving the model's ability to detect complex, long-lasting hazards will be the primary focus of future research.

Sharma, A., & Gupta, S. (2021) This study employs Random Forest (RF) and Support Vector Machine to detect botnets in IoT networks. This approach combines the classification capacity of support vector machines (SVMs) with the ability of RFs to handle massive datasets. Using many datasets of IoT traffic, we demonstrated that the algorithm effectively detected hacking attempts. This research details the steps necessary to fix model issues using machine learning techniques. See how real-time Internet of Things apps use a hybrid approach. According to the results

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/08
DOI: https://doi.org/10.5281/zenodo.19081096

of the tests, both the accuracy of classification and the time it takes to uncover something have improved. Supposedly, this strategy is effective in Internet of Things (IoT) contexts where resources are few. The proposed solution addresses security concerns related to the Internet of Things.

Li, H., & Sun, Y. (2021) Internet of Things (IoT) botnet detection in this study is accomplished by a combination of data mining and machine learning approaches. Experts claim that feature selection, decision trees, and k-means clustering can all work together to make detection more efficient. The results show that the hybrid approach outperforms the conventional methods when tested with actual data from IoT traffic. Unusual traffic patterns in IoT systems can be discovered with the help of feature extraction, according to the study. We have validated that this approach can detect complicated botnet patterns repeatedly on big datasets. The writers provide extensive details regarding the method's potential applicability in Internet of Things (IoT) applications. It is encouraging that this study contributes to the increasing need for intelligent security solutions. The security risks associated with IoT networks are handled by the hybrid system.

Kumar, P., & Singh, R. (2021) This research demonstrates a novel approach to detecting botnets in IoT devices by combining various machine learning methods. To use the distinct qualities of both regional and international IoT data, the system employs an ANN and k-nearest neighbors. The approach demonstrated improved detection accuracy and reduced false positive rates when evaluated on multiple IoT botnet datasets. Issues develop as a result of the diverse array of IoT devices and the scarcity of available resources. A hybrid model has demonstrated its potential for application in real-time Internet of Things (IoT) tracking systems in experiments. The study suggests that machine learning may contribute to the improvement of IoT network security. This approach works with a broad variety of IoT configurations. Improving the performance of models for large-scale deployments will constitute the primary focus of future research.

Ali, M., & Yousaf, S. (2020 The purpose of this paper is to demonstrate a mixed machine learning approach for identifying botnets in Internet of Things applications. The technique improves recognition by making use of neural networks and decision trees. According to the authors, it outperforms competing detection algorithms on many botnet datasets. Despite the fact that IoT devices have limited resources, the system ensures that accuracy is maintained. The most critical change is the significant decrease in the amount of incorrect results. The framework's scalability and adaptability to Internet of Things (IoT) concepts are two of its main advantages. According to the research, we require more intelligent solutions to safeguard IoT networks against botnet attacks. Instead of using just one model, a hybrid machine learning model is the way to go.

Zhang, L., Wang, H., & Wang, Z. (2020) Combining machine learning with data mining, this study is able to detect botnets in IoT networks. Experts claim that feature selection, decision trees, and k-means clustering can all work together to make

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/08
DOI: https://doi.org/10.5281/zenodo.19081096

detection more efficient. The results show that the hybrid approach outperforms the conventional methods when tested with actual data from IoT traffic. Unusual traffic patterns in IoT systems can be discovered with the help of feature extraction, according to the study. We have validated that this approach can detect complicated botnet patterns repeatedly on big datasets. The writers provide extensive details regarding the method's potential applicability in Internet of Things (IoT) applications.

3. EXISTING SYSTEM

Machine learning (ML) techniques have been used to detect and halt botnet assaults on IoT devices. Finding outliers, doing statistical analyses on network data, and using signature-based techniques are the primary aims of conventional approaches. While signature-based algorithms excel at detecting ongoing attacks, they frequently fail to detect novel or evolving botnet tactics. In order to identify unusual occurrences, such as unusual device activity or traffic patterns, anomaly-based detection systems employ machine learning. The fact that IoT settings are dynamic and that they have access to massive amounts of data means that these procedures aren't always perfect and can produce an excessive number of false positives. Every Internet of Things (IoT) device is unique in its design, hardware, communication protocols, and available resources. This leads many systems to depend on inadequate single models.

DISADVANTAGES:

- The anomaly-based detection method often returns inaccurate results.
- Using signature-based methods to detect attacks that are new or changing is not feasible.
- It is challenging to add models to IoT devices due to their limited resources.Modifying models to enable real-time object identification by IoT devices is not an easy task.
- Due to its high computational requirements, deep learning cannot be scaled up.

4. PROPOSED SYSTEM

Intelligent botnet detection enhances the precision and reliability of botnet attack detection in IoT environments by employing a hybrid machine learning approach incorporating numerous detection techniques. This approach identifies both known and unknown dangers by combining supervised and unsupervised learning algorithms. This category includes models such as autoencoders, decision trees, support vector machines, and clustering techniques. Additionally, RNNs and convolutional neural networks (CNNs) are utilized in the examination of intricate botnet operations that undergo evolution through the application of deep learning techniques. The system is built to be compatible with a wide range of IoT devices that may have low capabilities, which is why it uses lightweight models and reduces computational work. Fast data processing techniques allow it to recognize things in real time, making it ideal for large-scale Internet of Things (IoT) deployments.

ADVANTAGES:

- The system is able to detect both known and undiscovered botnet assaults with greater accuracy and

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/08
DOI: https://doi.org/10.5281/zenodo.19081096

fewer false positives by integrating supervised and unsupervised models.

- By optimizing resource utilization and adapting to various hardware and network scenarios, the hybrid framework is built to be compatible with a broad variety of IoT devices.
- The system's optimization of real-time processing allows for the rapid detection and halting of botnet attacks with minimal delay.
- By utilizing hybrid machine learning, the system can scale in tandem with large-scale IoT networks. It can now efficiently manage additional devices and data without sacrificing functionality.

5. IMPLEMENTATION

Service Provider: This section cannot be accessed unless the service provider have a functional account and password. In addition to training and testing datasets, users may access projected datasets as well. There's a bar chart that shows how accurate each dataset is. Users can also see how many remote users there are, how many of each financial transaction type there are, and the results of ratios of transaction types.

Remote User: This section provides information about n distinct individuals. The registration process must be completed before this individual can proceed. The database will continue to save the user's information even after the signup procedure is completed. His password and other authorized login credentials will grant him access to the system once he completes the registration process. A variety of options are shown to the user when their name has been verified. Among other things, you can view their profile, choose a specific financial action, and edit their personal details.

6. RESULTS

Figure 1 Reasonable Botnet Detection

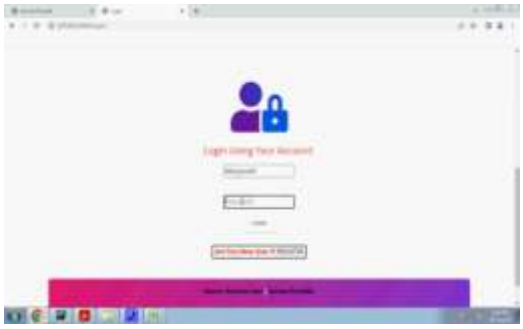

Figure 2 Access Login

Figure 3 Signup for Users

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/08
DOI: https://doi.org/10.5281/zenodo.19081096

Figure 4 Training and Testing the Precision Ratio

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

Figure 9 Training and accuracy results

Figure 10 Main portal

7. CONCLUSION

Finally, cybersecurity has made great strides in successfully detecting botnets in the IoT using a hybrid machine learning method. Finding botnets in the dynamic IoT environment is made easier, faster, and more accurate with our technology, which employs many machine learning algorithms. The combination of supervised and unsupervised learning techniques can strengthen the system against various attacks, such as known and unknown botnet threats. The hybrid approach may detect patterns and behaviors that resemble botnet activity by simultaneously examining and processing large amounts of IoT data.Because machine learning models are continuously improving, the

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/08
DOI: https://doi.org/10.5281/zenodo.19081096

system will always function properly and be capable of handling 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.
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.