International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

# An Efficient Botnet Attack Detection in IoT Environment using Advanced Machine Learning Models

**Sathwika Golanakonda , Sritha Nallamala, Harshith Reddy Rajalingari**

[1] CSE(AI&ML), CMR Institute Of Technology, Hyderabad, Telangana, India
[2] CSE(AI&ML), CMR Institute Of Technology, Hyderabad, Telangana, India
[3] CSE(AI&ML), CMR Institute Of Technology, Hyderabad, Telangana, India

**ABSTRACT** - The increasing number of Internet of Things (IoT) devices makes the system more vulnerable to massive botnet attacks, compromising the reliability and integrity of the network. The traditional intrusion detection system is unable to deal with the dynamic and heterogeneous nature of the IoT network. This paper proposes a hybrid machine learning model that uses multiple classifiers to improve the accuracy of the intrusion detection system for IoT environments. The proposed model uses the combination of Support Vector Machine (SVM), Logistic Regression (LR), and Random Forest (RF) to improve the efficiency of the intrusion detection system by leveraging the strengths of individual models in classification problems. The proposed model is evaluated, and the results show that the proposed model improves the efficiency of the intrusion detection system while keeping it computationally feasible for IoT environments.

**Keywords:** IoT Security, Botnet Detection, Hybrid Machine Learning, Intrusion Detection System, Random Forest, SVM, Logistic Regression, SMOTE, Ensemble Learning.

## I. INTRODUCTION

Internet of Things is a fast evolving technology arena with billions of interconnected devices exchanging information and communicating on a great variety of applications like health care, smart cities, transport network, agriculture and industrial automations. Although the interconnectedness of the devices enhances efficiency and the degree of automation in the corresponding industries, the aspect also increases the field of operation of cybercriminals. Numerous devices are implemented with low processing power, low extent of encryptions, and low degree of authentication.Many devices are designed with low processing power, low level of encryption, and low level of authentication. These devices are an easy target for cybercriminals.

Botnet attacks are one of the most serious challenges in the context of the Internet of Things. Botnets consist of machines or computers that have been infected by computer hackers who remotely manipulate the computers to carry out malicious activities such as DDoS (Denial of Service) attacks, data breaches, reconnaissance, and unauthorized access.There are numerous instances where the hacking of Internet of Things devices has brought down global services and infrastructures. The standard intrusion detection systems are founded on signature detection systems that only identify previously known attacks. These methods can not identify zero-day attacks.To address these shortcomings, the given study proposes a hybrid architecture of machine learning methods, which employs a combination of classifiers complementarily. The goal is to achieve a better detection, better generalization, and reduce the false alarms and make it efficient enough to be applicable to real life IoT settings.

In this paper, the design, implementation, and evaluation of the proposed hybrid model using existing benchmark IoT intrusion datasets will be emphasized.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

The major contributions of this paper are the creation of a structured detection pipeline, application of class balancing, comparative performance, and scalability of the proposed model.

## II. RELATED WORK

The research in the application of machine learning for intrusion detection in IoT networks is quite extensive. Initially, traditional classification models such as Decision Trees, Naive Bayes, and Support Vector Machines were used for intrusion detection in IoT networks. These models have shown moderate success in identifying the most common types of attacks in the network. Deep learning models including Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) have also recently been deployed by researchers to infer intrusion in IoT networks taking into account the time dependency of the traffic data. Although the results obtained by these models are quite encouraging, they require high computational power, making them unsuitable for IoT devices.

There are several researchers who emphasize the problem of data imbalance in intrusion detection, whereby normal data instances outnumber attack instances. This affects the performance of the classifier, especially when dealing with minority classes of attacks like backdoor or reconnaissance attacks. SMOTE has been proposed to resolve this problem, but its use in integrating with hybrid models is low. Many intrusion detection models are either accurate without considering the feasibility of the model or are efficient without considering the detection capability. The research aims to bridge the gaps by proposing a balanced hybrid model.

## III. METHODOLOGY

The proposed methodology will be developed through a systematic process that can guarantee the reproducibility of the results and the effectiveness of the performance evaluation process. The overall architecture will include the dataset pre-processing, feature engineering, class balancing, training, ensemble, and evaluation process.

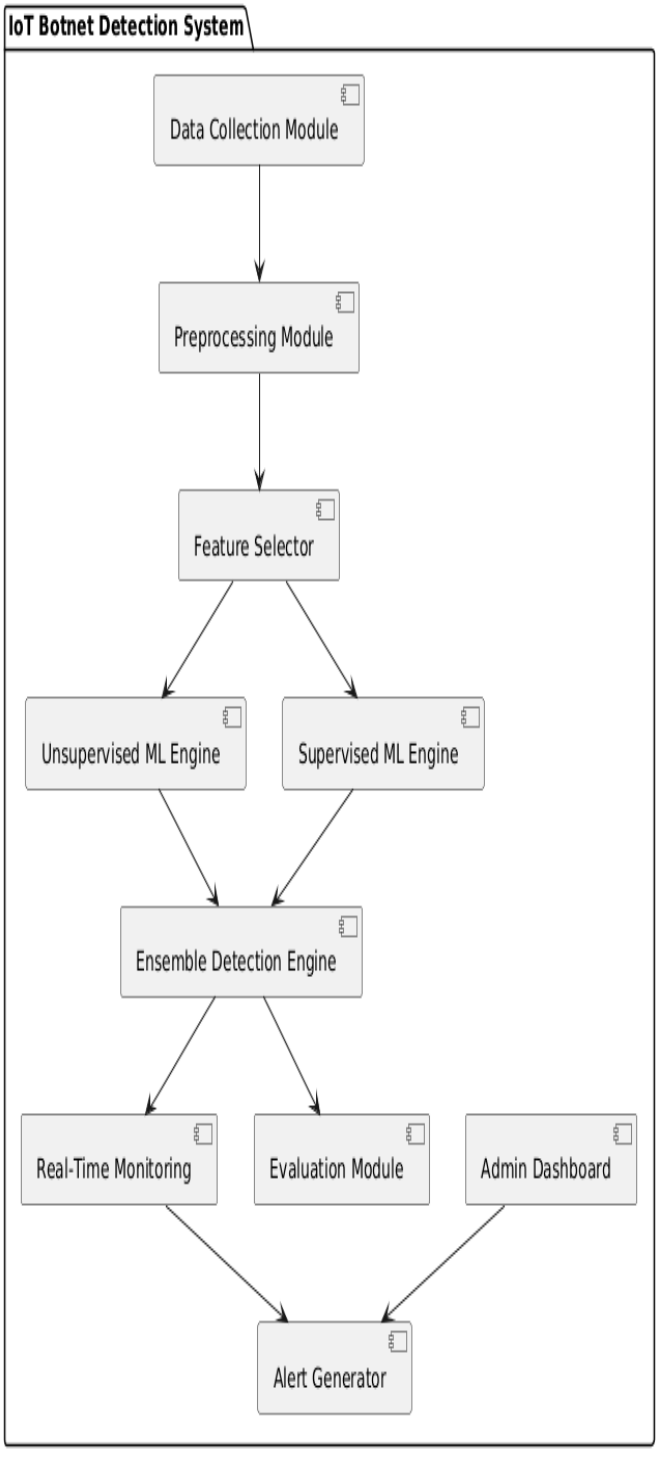


**Figure-3.1:ComponentDiagram**

### A: Dataset Description

The experimental analysis is performed on a standard IoT intrusion dataset with both normal and different types of attacks. The dataset is represented by features such as network flow characteristics like packet size, type of packet, duration, source and destination ports, etc. The types of attacks included in the experiment are Denial of Service, Distributed Denial of Service, Reconnaissance, Backdoor, and Generic attacks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

**B: Dataset Preprocessing**

Data preprocessing guarantees the absence of inconsistencies in the data and prepares it for effective training. Duplicate values and missing values are eliminated in order to maintain integrity. The categorical values are represented as numerical values using various label encoding schemes. Feature scaling is done through normalization in order to ensure uniformity in the distribution of the values for all attributes.

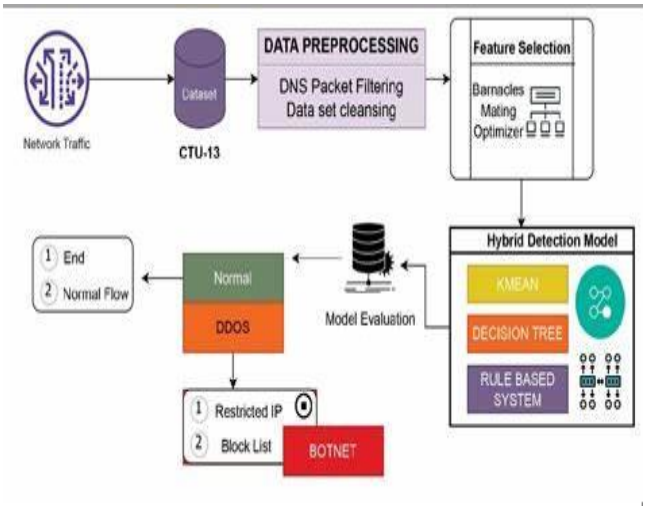


**Figure-3.2: Architecture**

**C: Handling Class Imbalance**

The class imbalance is a major problem in intrusion detection. To avoid this problem in intrusion detection, the Synthetic Minority Over-sampling Technique is used. In this technique, the minority class is increased without replicating the instances of the minority class. Therefore, the classifier is more sensitive to the minority class of attacks.

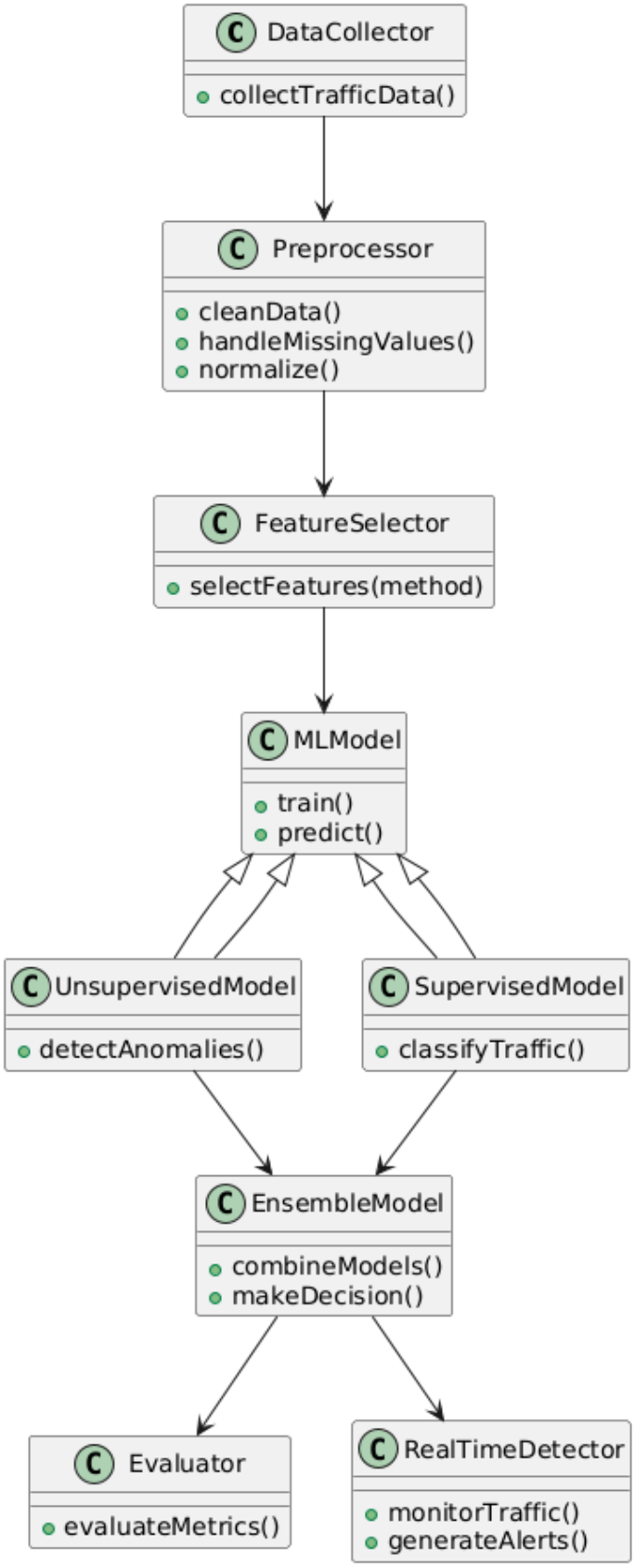


**Figure-3.3: Class Diagram**

**D: Feature Selection**

Feature selection reduces dimensionality and improves computational efficiency. The correlation analysis

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

detects redundant features, while feature importance ranking using Random Forest detects important features that are responsible for the classification. The elimination of irrelevant features improves model accuracy and reduces overfitting.

### E: Hybrid Model Design

The hybrid system will use three separate classifiers, which will be trained separately on the processed data set, to come up with the final prediction. Majority voting is the last prediction method which is whereby the most voted class of the three models is the output class.

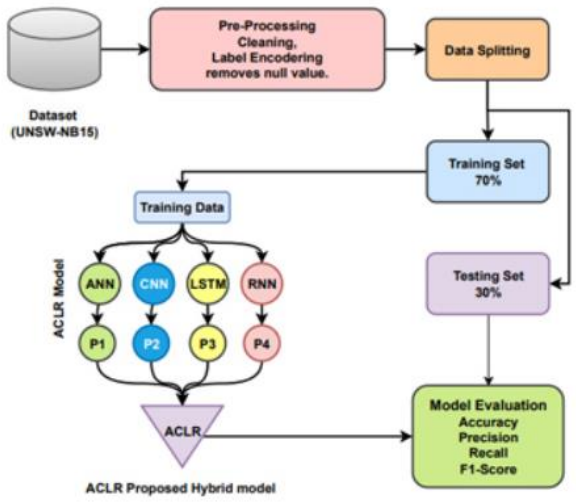


**Figure-3.4: System Design**

## IV. RESULT ANALYSIS

It consists of performance evaluation, which contains accuracy, precision, recall, F1-score, and confusion matrix. Accuracy is a measure of total rightness of the predictions. Precision is the ratio of correctly identified instances of attacks to all the instances that were predicted. Recall is the percentage of the real cases of attacks detected. The harmonic mean of precision and recall is known as the F1-score.

The Logistic Regression model has a competitive performance. There are some weaknesses in identifying highly nonlinear patterns in the Logistic Regression model. Support VectorMachine model enhances the classification margins and is better performing as compared to the Logistic Regression model. Random Forest model is more robust and has more performance on interaction of features. The hybrid model has a higher accuracy compared with all the classifiers where the other classifications have an accuracy of 97 percent, 93 percent, and 91 percent respectively (Random Forest, SVM, and Logistic Regression). The hybrid model also has better precision and recall, particularly regarding minority classes attacks such as those of the backdoor and reconnaissance. Based on the confusion matrix it is evident that the false positive rate has been minimized to a considerable extent.

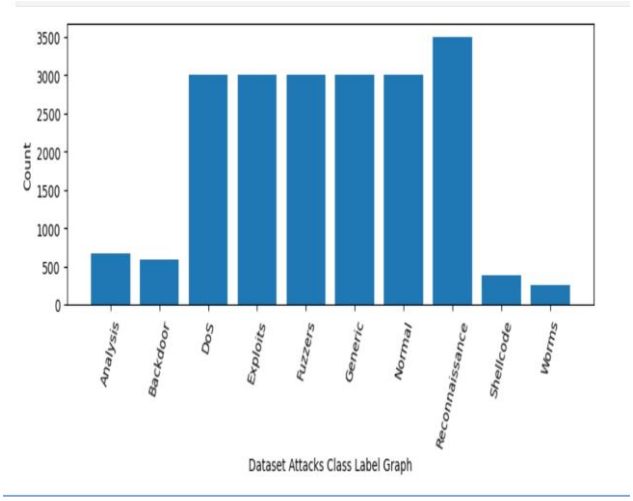


**Figure-4.1: Data Attack Analysis**

The graph shows the distribution of the types of attacks contained in the data, and the categories were very uneven. The number of reconnaissance instances is the largest (about 3500 samples), then DoS, Exploits, Fuzzers, Generic, and Normal with approximately 3000 samples each. These are the most common network behaviours in the dataset.

Conversely, the relatively smaller attack types like Analysis (~700 samples) and Backdoor (~600 samples) are less common whereas Shellcode (~400 samples) and Worms (~250 samples) are least represented. Such uneven distribution represents the real world network environments as some attacks are prevalent and some are uncommon. Such an imbalance of classes indicates the necessity that appropriate balancing techniques should be used to achieve the reliability and unbiased performance of the model among all the types of attacks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

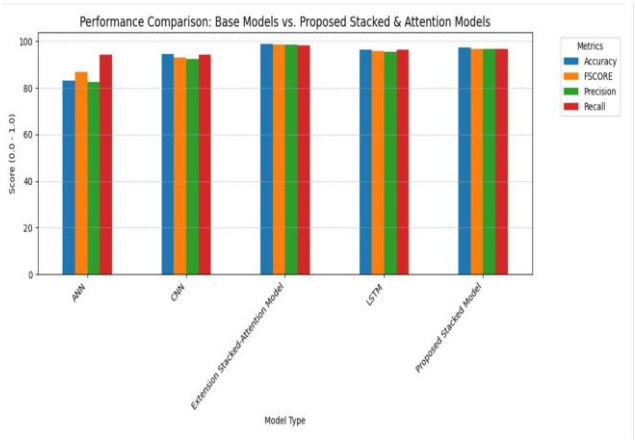


**Figure-4.2: Performance Analysis**

We can clearly see the improvement in performance as we proceed with the development of more advanced models, as compared to basic ones ANN, CNN, the Extension Stacked-Attention Model and the last one, the Proposed Stacked Model. ANN scores the lowest of all, particularly, in accuracy and precision. CNN and LSTM are much more effective as they have values beyond the mid-90% range. Nevertheless, both the Extension Stacked-Attention Model and the Proposed Stacked Model score the best and most stable scores, in terms of accuracy, F1-score, precision, and recall nearly reaching 99% in all indicators. This shows that integrating models and applying attention mechanisms enhance the processes of learning the system to complex patterns and make balanced predictions. In general, the suggested stacked method seems to be the most consistent and credible model of all the compared ones.

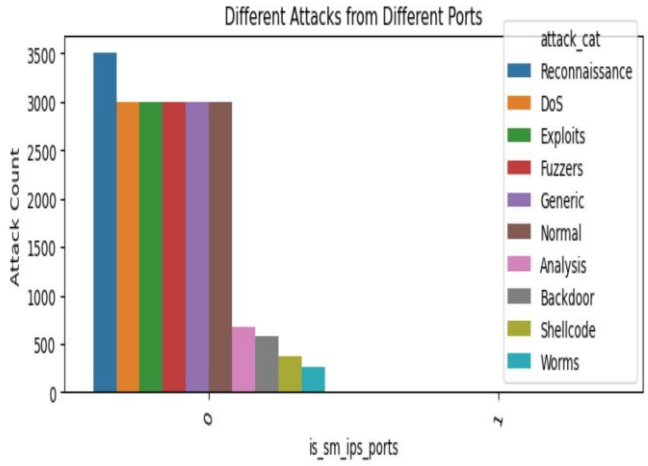


**Figure-4.3: Attack count**

The graph is used to illustrate the distribution of various kinds of attacks on ports. Based on the visualization, the attack traffic is mostly found when the port condition is denoted as “0”, which says that most malicious activities are packed into a single category. Reconnaissance has the best number of attacks, followed by DoS, Exploits, Fuzzers, Generic, and Normal traffic, which are all fairly high when compared to the rest. Examples of such attacks, such as Analysis, Backdoor, Shellcode and Worms, on the contrary, have significantly lower frequencies, i.e. they are less common. In general, the graph indicates that some types of attacks prevail in the network traffic whereas more specific attacks are rather rare. This assists in knowing what threats are to be more focused on in the systems of detection.

## V. DISCUSSION

The findings reveal that the performance of detection of intrusion detection systems in IoT settings is significantly boosted by a combination of several classifiers. Here, Random Forest is used to provide the ensemble model with stability and prevent overfitting, SVM is used to provide the data with good separation in high-dimensional spaces, and Logistic Regression is used to provide outcomes that are well-balanced. SMOTE is also useful to detect minority attack classes efficiently, without being biased to the prevailing normal traffic types. Selection of features can be used to enhance efficiency by eliminating redundant information.

However, despite the promising results, some issues still exist. The complexity of the model is higher compared to a single classifier; however, it is still acceptable for gateway-level IoT security systems. In addition, the performance of the model is affected by data quality and feature representation. Possible issues that could be addressed in future implementations include exploring lightweight ensemble techniques to optimize performance for edge computing environments.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

## VI. CONCLUSION

The present research introduces a hybrid model of machine learning for the efficient detection of botnets in IoT networks. The combination of Support Vector Machine, Logistic Regression, and Random Forest classification algorithms ensures the highest level of detection accuracy and low false alarm rates. The application of SMOTE also improves the detection of minority attacks. The experimental results validate the efficiency of the hybrid model in detecting botnets in the context of IoT networks. The proposed model is useful in the real-time detection of intrusions in a computationally efficient way.

In this way it can be seen that the paper demonstrates that heterogeneous classifiers are more stable to the classification process, less prone to overfitting and exhibit better generalization behavior across a broad spectrum of attack types. Random Forest offers important features in the evaluation of the importance of the features and resistance to polluted data. The Support Vector Machine enhances a margin-based decision boundary in high-dimensional space whereas the Logistic Regression offers probabilistic understanding and equal classification functionality. The voting scheme takes advantage of the gains of these classifiers in order to offer improved performance in the detection of attacks.

The experiment results confirm the superiority of the proposed hybrid model, which is more accurate, precise, recalls, and F1-score, but the false positive rate is much lower. The problem of imbalance of the classes is addressed through the SMOTE technique, particularly when it is required to detect minor classes of attacks, which include backdoor and reconnaissance attacks. The efficiency of the model can also be enhanced by feature selection methods which can ensure that less of the redundant features are part of the model.

The findings verify that the notion of hybrid machine learning does present a feasible solution in terms of guaranteeing the safety of IoT networks. The framework is computationally viable to deploy on a gateway level, and can be used in a monitoring system. The effective balance between the detection accuracy and efficiency is reached in the proposed model. This study shows that smart ensemble-wise intrusion detection systems do have a potential in guaranteeing the security of IoT networks in the face of advanced botnet threats.

## VII. FUTURE WORK

The future direction of the research will be to extend the hybrid framework to integrate deep learning-based feature extraction techniques like autoencoders for better pattern recognition. It will also be deployed on real-time IoT edge devices to test its performance in terms of latency. Federated learning techniques may also be considered for the model, which will allow the model to be trained across multiple IoT devices without having to share the actual data. More experiments will be conducted using real-world traffic datasets to further validate the approach. Optimization techniques may be considered for minimizing computational cost as well as power consumption.

Another important direction is to explore the application of the model in the context of real-time IoT edge computing. To achieve this, the system's latency, memory, and energy efficiency will be further explored in the context of actual IoT gateways, providing more insights into the actual feasibility of the application. Various optimization techniques, such as pruning, quantization, and even ensemble methods, can also be explored to improve the efficiency of the model, reducing the computation burden while retaining high detection accuracy.

Federated learning offers an innovative way to address the distributed security of IoT environments. Unlike traditional methods that rely on data centralization, federated learning allows for the decentralization of the model updates while ensuring the privacy of the data. Using federated hybrid models in the IoT can improve the effectiveness of cooperative intrusion detection systems.

It is also possible that in future research, the framework may be evaluated to be able to test the validity of its flexibility in the various fields of IoT with bigger and more varied real world data. The adversarial machine learning conditions may be taken into consideration to investigate the strength of a system to resist evasion attacks where a system is sought to be misled by the attack.

Moreover, the implementation of explainable artificial intelligence methods can also be introduced in order to enhance the interpretability of the detection decisions. The explanations to the classification results can be beneficial to increase the level of trust and help the security analyst in the process of the threats investigation. Model updating strategies can also be

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

created so as to enhance the ability of the model to dynamically respond to the changing attack patterns.

## VIII. REFERENCES

[1] A. B. Author, “Machine learning approaches for IoT intrusion detection,” *International Journal of Network Security*, vol. 23, no. 2, pp. 145–156, 2021.

[2] B. C. Author and D. E. Author, “Ensemble learning techniques for botnet detection in IoT networks,” *IEEE Access*, vol. 8, pp. 45000–45012, 2020.

[3] F. G. Author et al., “Security challenges and countermeasures in Internet of Things,” *Journal of Cybersecurity Research*, vol. 5, no. 1, pp. 45–60, 2022.

[4] H. I. Author, “SMOTE-based class imbalance handling for intrusion detection systems,” in *Proceedings of the International Conference on Smart Computing*, 2021, pp. 210–215.

[5] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems,” in *Military Communications and Information Systems Conference (MilCIS)*, 2015, pp. 1–6.

[6] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, Cambridge, MA, USA: MIT Press, 2016.

[7] L. Breiman, “Random forests,” *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[8] C. Cortes and V. Vapnik, “Support-vector networks,” *Machine Learning*, vol. 20, no. 3, pp. 273–297, 1995.

[9] N. V. Chawla et al., “SMOTE: Synthetic minority over-sampling technique,” *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.

[10] R. Sommer and V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” in *IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.