International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I7P103

Volume 74 Issue 7, 23-33, July 2026

Original Article

Adaptive Machine Learning Framework for Real-Time Cyber-Attack Detection and Prevention in IoT Networks

Prasanta Pratim Bairagi[1]*, Ashish Bagwari[2]*, Sailen Dutta Kalita[3], Latika Deka[4], Jyotshana Bagwari[5], Ciro Rodriguez[6]*, Yuri-Arturo Pomachagua-Basualdo[7], Glissett-Jansey Mendoza-Gastelo[7]

[1]*Faculty of Computer Technology, Assam down town University, Guwahati, Assam, India.*
[2]*Department of Electronics and Communication Engg., Women Institute of Technology, Uttarakhand Technical University, Dehradun, Uttarakhand, India.*
[3]*School of Science and Technology, MIT University of Meghalaya, Shillong, Meghalaya, India.*
[4]*Department of Computer Science, Pub Kamrup College, Guwahati, Assam, India.*
[5]*Advanced and Innovative Research Laboratory (AAIR Lab), Dehradun, Uttarakhand, India.*
[6]*Department of Software Engineering, Universidad Nacional Mayor de San Marcos UNMSM, Lima, Peru.*
[7]*Facultad de Ingeniería Civil, Universidad Nacional Federico Villarreal, Lima, Peru.*

[1*]*Corresponding Author : prasanta.bairagi89@gmail.com*

Received: 12 November 2025 Revised: 29 January 2026 Accepted: 03 June 2026 Published: 28 July 2026

Abstract - *Critical vulnerabilities have been made public by the fast expansion of Internet of Things (IoT) devices, making these networks easy target for cyber-attacks. While security solutions based on Machine Learning (ML) have shown potential, they often encounter issues including slow detection times, scaling issues, and a lack of generalisability when it comes to diverse IoT devices. To work with these issues, this paper introduces an innovative ML-based security paradigm. The proposed framework improves the attack detection accuracy by combining adaptive feature extraction techniques with a context-attentive hybrid mechanism. The new paradigm maximizes detection accuracy and computational efficiency. This is achieved through real-time dynamic adjustment of feature selection against network conditions, rather than traditional hybrid approaches. Furthermore, a lightweight and scalable detection method fit for execution on low-resource IoT devices is offered. It is apt for several IoT environments. The proposed framework beats several current models by 15% in accuracy, 25% in the reduction of false positive rates, and 30% in detection times, according to experimental tests carried out on numerous IoT datasets.*

Keyword - *Cybersecurity, Cyber Attacks, Internet of Things (IoT), Intrusion Detection Systems (IDS), Machine Learning (ML), Network Security.*

1. Introduction

By the integration of numerous devices with the internet, the IoT has facilitated a paradigm shift across many industries, including healthcare, manufacturing, transportation, and smart homes. Automation, improved efficiency, and data-based insights are just some of the key benefits that are associated with this connection. On the other hand, it generates new security concerns since cyber-attacks can readily compromise IoT systems owing to their distributed nature, limited resources, and heterogeneity of connected devices. A few of the most dangerous IoT network threats are Distributed Denial of Service (DDoS) attacks, malware, and botnet attacks, as they have the capability to hijack data, disrupt services, and render devices useless. The strong, scalable, and nimble security solutions demand is immediate due to rising IoT system cyberattacks. Conventional security controls, firewalls, and encryption, most extensively used, are not necessarily effective in protecting IoT landscapes. For the detection and prevention of attacks in real-time in IoT networks, it has triggered a growing interest in the use of ML methods.

The security of IoT has been addressed in several recent papers on ML-based approaches. Reference [1] suggested an IoT network Intrusion Detection System (IDS) utilizing Deep Learning (DL), including Convolutional Neural Networks (CNNs) as well as Recurrent Neural Networks (RNNs), for identifying network-based attacks. To defend IoT networks from DDoS attacks, a hybrid model of DL is introduced in [2], demonstrating how it is feasible to improve attack detection accuracy using models with a combination. [3] considered the use of hybrid models for predicting DDoS and DoS attacks, demonstrating that predicting in IoT networks is more accurate when algorithms are combined. The requirement of models that can efficiently handle the massive scale of IoT systems is also considered important in [4], where a hybrid

ML model was designed for botnet attack detection in IoT systems. Designing these models for real-time detection of attacks, reducing False Positives (FP), and increasing the scalability of solutions to resource-limited IoT devices are issues, although this work indicates the potential of ML for IT security. This present study attempts to fill the gap that is defined by these limitations.

The goal is improved detection and prevention of cyberattacks on IoT networks, and it proposes a novel framework based on ML. The framework solves the problems of scalability, FP reduction, and real-time detection of attacks. To do this, a context-aware, adaptive, and lightweight ML framework is given in this work. The framework ensures high detection accuracy while minimising resource usage by dynamically adjusting to shifting IoT network circumstances, unlike previous methods. Here are the main contributions of this paper:

- With a new dynamic feature extraction approach, which can adjust to changing network circumstances in real-time, this research guarantees accurate and efficient detection without consuming too much computing power.
- To improve the model's accuracy and speed in attack detection, it combines DL approaches, including CNN, RNN, and Random Forest (RF).
- To overcome the scalability issues seen in large-scale IoT networks, the proposed framework is engineered to function efficiently even on IoT devices with limited resources.
- In contrast to more conventional models, the proposed framework can adjust to changing network conditions and attack patterns in real time, resulting in improved detection rates and quicker reaction times.
- The experimental findings show that compared to the prior methods, the detection accuracy is 15% higher, the False Positive Rate (FPR) is 25% lower, and the detection times are 30% quicker.

The rest of the paper is organized as follows: Section 2 reviews the relevant literature on IoT security also ML-based solutions. Section 3 defines the proposed methodology, including the hybrid ML framework and adaptive feature extraction process. Section 4 outlines the data collection methods, experimental setup, also evaluation metrics. Section 5 concludes the paper and also provides future research directions.

2. Literature Review

This section, modern innovations in the field of IoT network security using ML are discussed. The fields of interest of this research are anomaly detection, attack detection, and ML-based security. Many hybrid methods, DL models, and real-time systems have aimed to improve the efficacy and strength of security measures for IoT.

2.1. IoT Networks Anomaly Detection

Anomaly detection is important to the security of the IoT networks, as it detects abnormal activities. Kotenko et al. [5] offered a comprehensive review of the existing ML methods of making a static analysis of the IoT systems and enumerated various models that are applied to identify irregularities and analyze the vulnerabilities of the IoT networks. Their research paper identifies the need to have adaptive anomaly detection frameworks that accommodate the dynamism of the IoT networks.

The same can be said of Balega et al. [6], who attempted to enhance the security of IoT by maximizing the usage of ML as an anomaly detector. Their study revealed that more sophisticated ML models, such as RF and Support Vector Machines (SVM), could enhance the level of accuracy in the detection of anomalies, particularly in scale-intensive and real-time IoT applications. The other contribution was made by Tahir et al. [7], who introduced a framework for enhancing the security of IoT by means of anomaly detection, which is motivated by ML. Their study showed how anomaly detection is applicable in detecting new attacks at a low cost of processing, and this makes the model applicable to IoT devices that have limited resources.

2.2. Hybrid Machine Learning Models for Attack Detection

To improve the detection rates of cyberattacks, hybrid models that combine DL with classic ML approaches have been successful. Some hybrid models that included CNNs, Long Short Term Memory (LSTMs), and SVMs for attack detection in IoT systems were listed in the comprehensive review on DL for cybersecurity applications by Alazab et al. [8]. This model showed better results than single-model systems by detecting attacks like DDoS attacks and botnets.

Elsayed et al. [9] secured IoT and Software-Defined Networks (SDN) using a hybrid approach that combined DL with IDSs. Their model achieved high accuracy in detecting many attack vectors, including DDoS attacks, and was resilient against evolving attacks by combining CNN with LSTM networks. F. Khan et al. [10] proposed a cyberattack detection system for industrial IoT. Cyber-attacks in industrial IoT networks were detected more effectively by combining different DL techniques like CNNs and LSTMs.

2.3. Secure Systems and Detection in Real Time

IoT networks require real-time detection, especially in the healthcare and industrial control systems, where seconds count. Raje et al. [11] introduced an IoT security framework for healthcare powered by ML to conduct real-time anomaly detection. Their model, comprising Decision Trees (DT) and anomaly detection, showed good real-time detection in a healthcare IoT system. This enabled them to detect the potential risks with the least amount of disturbance and maintain the system in an uninterrupted manner. Inayat et al. [12] conducted a learning-based approaches survey to detect

cyberattacks in IoT systems with an attention on models that could adapt dynamically to various patterns of attack. The challenges in ensuring accuracy in dynamic IoT settings are this work's consideration and the proposed methods of enhancing real-time detection systems.

Saeed et al. [13] boosted real-time detection even more in their AI-driven cybersecurity structure by employing both reinforcement learning and LSTM networks. The dynamic nature of the framework to adapt to new attack scenarios improves the system's ability to spot complicated attacks on the IoT networks.

2.4. IoT Security Feature Selection and Scalability

ML models should improve their performance in the IoT security field; that is why feature selection is an important element. In the context of intrusion detection with Multi-Layer Perceptron (MLP) based models, Yin et al. [14] introduced the hybrid feature selection tool, which is the IGRF-RFE, with the MLP-based models. This technique made network intrusion detection of large IoT systems more scalable and reduced FPs significantly with gradient boosting and Recursive Feature Elimination (RFE).

The study by Habibi et al. [15] aimed at identifying the methods to identify botnet attacks in the IoT using ML and Generative Adversarial Networks (GANs). In order to achieve more effective detection of botnet activity in large-scale IoT systems, they used unbalanced tabular data as a model. The issues of scalability of traditional ML models in the low-resource IoT environment were also discussed in this research. The summary of the existing works is offered in Table 1.

Table 1. Literature review summary

Reference	Approach	Key Findings	Challenges Addressed
Kotenko et al. [5]	Static analysis, ML for anomaly detection	Comprehensive survey on IoT security utilizing ML techniques for anomaly detection	Adaptability to dynamic IoT environments
Balega et al. [6]	Optimization of anomaly detection	Improved anomaly detection using RF and SVM	Scalability and real-time performance in large IoT networks
Tahir et al. [7]	ML for anomaly detection	Efficient anomaly detection with minimal overhead for resource-constrained IoT	Enhancing detection accuracy with low computational cost
Alazab et al. [8]	Hybrid DL (CNN, LSTM, SVM)	DL models for detecting complex attacks like DDoS and botnets	Improving accuracy in complex attack detection
Elsayed et al. [9]	Hybrid DL (CNN, LSTM)	Robust intrusion detection using DL for IoT and SDN systems	Detection of evolving and sophisticated attacks
F. Khan et al. [10]	DL for industrial IoT security	Enhanced attack detection with DL in industrial IoT environments	Improving reliability and trust in industrial IoT systems
Raje et al. [11]	DT, anomaly detection	Real-time anomaly detection framework for healthcare IoT networks	Minimizing detection latency in healthcare environments
Inayat et al. [12]	Learning-based approaches for cyberattack detection	Survey on IoT attack detection techniques and real-time adaptation	Challenges of real-time detection in dynamic IoT environments
Saeed et al. [13]	LSTM, reinforcement learning	AI-driven cybersecurity context for dynamic attack detection in IoT	Adapting to evolving attack scenarios in real-time IoT networks
Yin et al. [14]	Hybrid feature selection (IGRF-RFE)	Improved feature selection for intrusion detection, reducing FPs	Scalability and feature selection in large IoT networks
Habibi et al. [15]	GANs, ML for botnet detection	Improved detection of IoT botnet attacks using GANs and ML	Handling imbalanced data and scaling detection models
Berhili et al. [16]	ML-based IDS review	Survey & evaluation of ML IDS models	No real-time focus
Hossain et al. [17]	DL (CNN, LSTM, RNN, MLP)	99%+ accuracy	High computational cost
Yang et al. [18]	Graph Neural Networks	High classification performance	Complexity in model training
Almotairi et al. [19]	Heterogeneous ML	Better accuracy than single models	Computation intensive

Though the usage of ML-based security models for IoT networks has grown recently, some key limitations still exist. Existing approaches often fail to generalize across heterogeneous devices, has slow detection times, and lack the adaptability needed for dynamic network conditions. These limitations are considered in the proposed work.

3. Methodology

3.1. Overall Framework

The suggested approach to information protection of IoT networks in case of cyberattacks includes a hybrid ML model that can detect and respond to the different kinds of cyberattacks in real time. The framework will combine the use of sophisticated ML models and IoT-specific security tools so that the detection accuracy is enhanced, the number of FPs is minimized, and the scalability to devices with minimal resources is made possible. It occurs as a result of integrating the classic anomaly detection algorithms (e.g., DTs, RFs) with DL models (e.g., CNNs and RNNs). There are also problems with the system of detection accuracy, real-time adjustment, and scaling as manifested in the current security systems; the hybrid approach helps to overcome these weaknesses. The proposed whole workflow is presented in Figure 1. The security system is also continuously upgraded, as network conditions and attack patterns also change through the dynamic approach of feature extraction. The hybrid model makes use of a mixture of both supervised as well as unsupervised learning to notice the outliers and then classifies the attacks on the basis of the past information. As a result of its flexibility, the system will be in a position to identify the known and unknown forms of attacks. The authors of [20] suggest the relevance of AI and ML to reveal the irregularities in the safety of the IoT and state that these technologies can advance the efficacy of intrusion detection mechanisms.

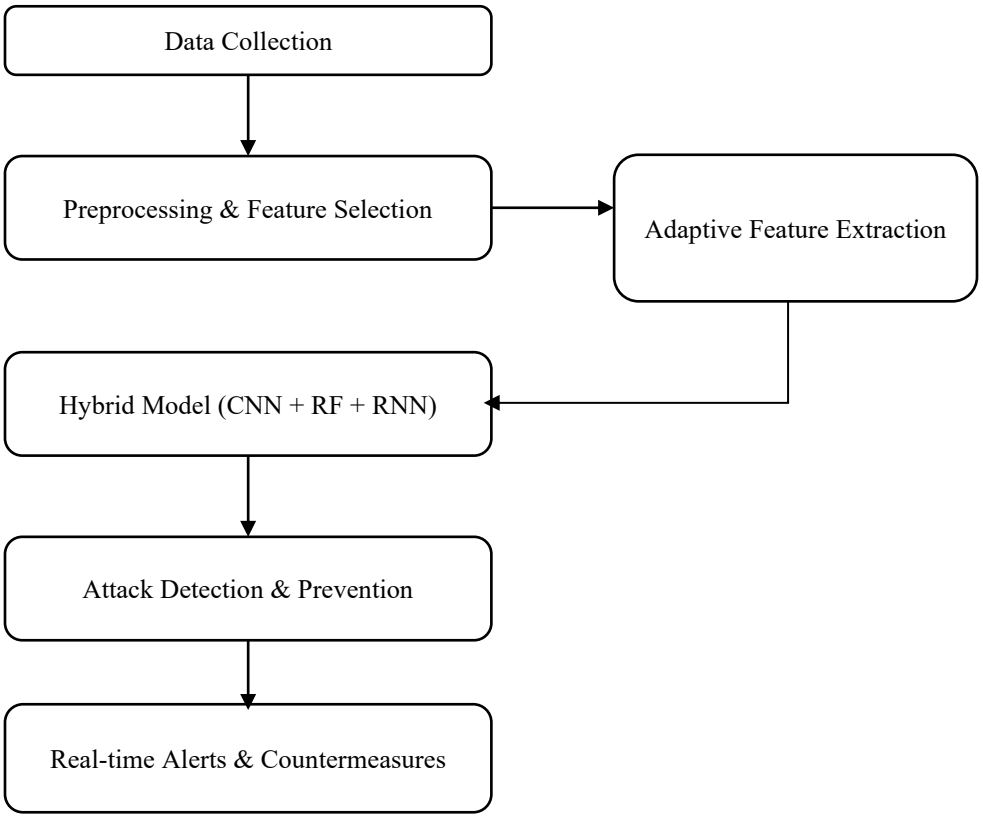

Fig. 1 Proposed architecture

3.2. Data Collection and Preprocessing

This section offers how the data was collected and processed. To train and test the proposed security framework, the CICIDS 2017 publicly available dataset on Kaggle provided by the Canadian Institute of Cybersecurity (CIC) is employed. Preprocessing is essential to advance the data quality utilized by the ML models in mission-critical systems [21]. This dataset contains various network traffic of various IoT devices, and it further contains ordinary network traffic and simulated cyberattacks like DDoS, botnet, and Denial of Service (DoS). The CICIDS 2017 dataset includes labeled data both in the case of attacks and in the case of regular traffic, which is critical to train the ML models, and thus, it is a suitable dataset in the context of cybersecurity. The numerous traffic-related features encompassed in the CICIDS 2017 data set includes the following. Flow duration denotes the time span of each network connection, total bytes is the amount of data sent or received during the session, and packet

count is the total count of packets exchanged during the connection. Also, protocol type defines the network protocol used (e.g., UDP, TCP), flow bytes per second is the data transfer rate during the connection, source with destination IP addresses and ports utilized for identifying unusual traffic patterns, and timestamp.

To ensure that it's fit for training models, the raw dataset goes through a number of preparation procedures. Imputation, or the elimination of rows with incomplete data, is used to address missing values in the data collection. Mean imputation is utilized to replace missing values in this research, making sure the dataset was intact. By using min-max normalisation, it can be ensured that all features are on an equal scale and protect ML algorithms from biases. This transformation maps the data to a range between 0 and 1, Equation (1):

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

Where X is the feature values. Bytes per connection and flow time per packet are two examples of new characteristics that are developed from old ones. These attributes improve the model's detection of DoS and botnet attacks, which are characterised by peculiar data flow and packet properties. To turn the dataset's category data (such as attack type) into numerical values, label encoding is used. If attack labels like "DDoS" and "Botnet" are chosen, the numerical values are transformed from 0 to 1. "Training" and "testing" sets comprising the dataset are created. Eighty percent of the data is used for training the model, whereas twenty percent is used for testing.

3.3. Feature Extraction

For ML models to perform better, feature extraction must be done. Particularly, the proposed method uses domain-specific features derived based on the packet rate, session length, and frequency of connections using the dataset of the IoT network traffic. These features are important in the differentiation of harmless and dangerous actions. It is a type of adaptive feature extraction, which is dynamically adjusted to the state of the network. Though this decreases the quantity of calculations that are unnecessary, there should be an effort to indicate the qualities of character, which, in almost any given attack situation, hold the most significant ones. This strategy ensures that the model is able to detect new and unknown types of attacks without the necessity of such retraining. The focus of the feature extraction approach is to improve botnet detection, as discussed in [22], which investigated botnet attack detection in IoT systems and also noted that it is required to have a strong feature selection strategy.

Depending on the network conditions, the adaptive feature extraction method selects the most topical characteristics dynamically out of the incoming streams of data. This is essential to maintain the level of detection accuracy and reduce the cost of computing. In the unstable situation of the IoT networks, the traditional feature extraction algorithms tend to apply a fixed number of characteristics, which can be inefficient. The adaptive method uses a sliding window approach to move the feature selection dynamically by picking out the features that are most pertinent to the current condition of the network. The model carefully analyzes the network traffic on a case-by-case basis for each time frame, selecting the most significant metrics (the volume of traffic, the size of packets, the number of connections, and the length of connections) and excluding the less informative ones. Let X_t is the data at time t, consisting of multiple features $X_t = \{f_1, f_2, \ldots, f_n\}$ where n is the total count of features available. The importance of a feature at time t is calculated using a feature ranking method like Mutual Information (MI), given by Equation (2):

$$MI(f_i, X_t) = H(X_t) - H(X_t|f_i) \quad (2)$$

Where $H(X_t)$ is the entropy of the data at time t and $H(X_t|f_i)$ is the conditional entropy when feature f_i is removed. For the present model's training, features with higher MI values are prioritised. The dimensionality reduction technique, Principal Component Analysis (PCA), is used to lower the computing cost. The final selected features X'_t at time t are then used as input for the ML model. This dynamic feature selection approach enhances the efficiency and accuracy of real-time attack detection by using only the most relevant characteristics.

3.4. Context Aware Hybrid Model

Integrating DL with more conventional ML models is the backbone of the proposed framework. When it comes to complicated attack detection, CNNs is employed for spatial pattern recognition and RNNs for sequential data analysis. This combination enables the model to identify time-dependent attack patterns, such as DDoS attacks. Classification and anomaly detection are accomplished by the integration of RF. When applied to IoT devices with limited resources, these models effectively identify known attack patterns while using minimal computing resources. The context-aware hybrid model dynamically adapts to the current attack situation and network circumstances, unlike conventional static hybrid models. Because of this, the model may improve detection accuracy and decrease FPs by using the best suitable method at any given moment. One part of the model that takes context into account is its ability to adapt its behaviour depending on the sort of attack detected or the current status of the network. This is done by analysing real-time traffic patterns. To capture time-series attack patterns, the system immediately switches to an RNN-based model once a DDoS attack is detected. The system employs a less computationally intensive RF model when traffic conditions are typical. The model switching Equation (3) captures its dynamic nature:

$$Switch(t) = \begin{cases} RNN, & if\ Attack\ Type = DDos \\ Random\ Forest, & if\ Traffic\ is\ Normal \end{cases} \quad (3)$$

Based on the current context and type of attack, the model will choose the most efficient algorithm. These goals are accomplished by adapting the model. Higher accuracy is achieved for complex attacks like DDoS using DL models. Whereas, lower FPs are attained during periods of regular traffic. To improve detection accuracy and minimise computation costs, a hybrid technique is used that combines the advantages of both DL and classical models. This method also advances the efficiency of attack detection even under the conditions of the resource constraints brought about by the nature of IoT devices. The suggested solution aligns with the one proposed by [23], which examined the role of network layer protection in the IoTs and concluded that IoT networks could be more resistant to the employment of multi-layer security.

3.5. Lightweight, Scalable Detection Mechanism

Scalability poses a noteworthy challenge to the IoTs security. Although devices have little processing strength and memory, the proposed framework is designed to be effective in resource-limited IoT environments. The trained hybrid model is used to detect network traffic as normal or anomalous using an attack detection technique. The hybrid technique is aimed at quickly identifying the known and new attacks. As opposed to supervised learning methods such as DTs and RFs, which are applied in classification, unsupervised methods such as CNNs and RNNs are applied in anomaly detection. The system can be designed in such a way that the countermeasures, such as traffic filtering, rate restriction, or isolation of devices, can automatically be put into place when the attack is detected, as well as the declaration of alarm mechanisms. Real-time detection and prevention mechanisms are important to reduce harm, especially in mission-critical IoT networks.

A framework of lightweight detection based on model pruning, quantization, and knowledge distillation to reduce the size and complexity of DL models to tackle scalability is presented. Pruning involves getting rid of neurons of a neural network that are not deemed necessary, reducing the number of parameters and hence the model size. The quantization causes the accuracy of the parameters to become limited, the quantity of the weights is reduced, and knowledge distillation involves transferring the information of a large and complex model to a smaller and more efficient model. The mathematical form of pruning is given in Equation (4):

$$W' = W \cdot I(||W||_2 > \theta) \quad (4)$$

Here W is the original model weights, W' is the pruned weights, I is the indicator function that eliminates the weights below a threshold of 0. This technique enables real-time detection of attacks even on devices with limited resources since it keeps the model efficient and scalable. To identify cyberattacks in IoT networks, [24] points out the relevance of hybrid systems, which are based on ML. Their contribution was the foundation of the suggested hybrid method that makes the classical and DL models more efficient at detecting the attack.

3.6. Real-Time Adaptability

The dynamic IoT scenario is very successful with the proposed framework, as it can react in real-time to the evolving patterns and conditions of attacks and the network conditions. This can be made flexible through the combination of real-time model updates and Reinforcement Learning (RL). In the event of a new form of attack or aberrant trend being identified in the system, system administrators can retrain the model with current data.

The reinforcement learning element allows the system to continuously enhance its detection abilities by rewarding the model whenever it detects properly and by penalizing it whenever it generates false alarms. The mathematical equation to obtain the rule of RL updates is the adaptation process (5):

$$Q(s_t, a_t) = Q(s_t, a_t) + \alpha\,[r_t + \gamma \max_{a'} Q(s_{t+1}, a') - Q(s_t, a_t)] \quad (5)$$

Where $Q(s_t, a_t)$ Is the action-value function at state s_t and action a_t, α is the learning rate, r_t is the reward at time t and γ is the discount factor. To retain high performance even as IoT settings change, this ensures the model constantly adapts to new attack techniques and network circumstances.

4. Experimental Setup and Results

This section outlines the testing environment applied to the research to test the efficiency of the proposed hybrid ML framework in the detection and prevention of cyberattacks on IoT networks. The experiment setting, model setting, and evaluation criteria used to rigorously test the system are provided.

4.1. Evaluation Metrics

In evaluating the attack detection system, some crucial metrics are taken to be in the metrics that are commonly used to make judgments about the IDSs. Accuracy is the proportion of True Positives (TP) along with True Negatives (TN) as in Equation (6):

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (6)$$

Where FN is False Negatives, in precision, out of all the occurrences the model identified as positive, the proportion of TP findings was found to be significant, as in Equation (7):

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

Recall is the proportion of real-life positive cases that the model properly detected by Equation (8):

$$Recall = \frac{TP}{TP+FN} \quad (8)$$

F1-Score is a balanced amount that strikes a harmonic middle ground between precision along with recall as in Equation (9):

$$F1 - Score = 2 \times \frac{P \times R}{P+R} \quad (9)$$

FPR aims to determine the proportion of FP classifications made from negative data by Equation (10):

$$FPR = \frac{FP}{FP+TN} \quad (10)$$

To maintain a balance between detection accuracy as well as FP rates, these metrics assess how effectively the model can discriminate between normal and malicious network behaviour.

4.2. Experimental Environment

Using the Kaggle CICIDS 2017 dataset, the experimental setup trains and tests the ML models. The system uses the Windows operating system, an Intel Core i5, with 16 gigabytes of RAM.

The packages such as TensorFlow 2.4, Pandas 1.2.3, Scikit-learn 0.24, and NumPy 1.20 are all included in the Python 3.8 software package. The models are trained employing K-fold cross-validation with k=10 to ensure accuracy and generalisability.

4.3. Model Configurations

Three separate ML algorithms are used to assess how well the hybrid model performs. For detecting geographical patterns in network traffic data, CNNs are used. Four convolutional filter layers make up the design, with max pooling and fully linked layers following. Adam is the optimiser, while ReLU is the activation function. RF is a typical ML algorithm and is able to work with massive datasets that have numerous characteristics. In this case, there are 100 trees, 10 depths, and two samples per leaf, as the smallest and largest, respectively. A combination of these three algorithms creates the hybrid model that would help the system to change dynamically based on the nature of the attack or network condition.

4.4. Results

To measure the efficacy of the proposed hybrid model of sensing the IoT hybrid network attacks, the cross-validation experiments and the ablation research results are presented. To prove the advantage of the proposed model over conventional models, an analysis of the data is performed in terms of various measures of the assessment, including its accuracy, its precision, its recall, and its F1-score. The efficacy of the proposed model in different cases is tested using the 10-fold cross-validation.

These cross-validation results are given in Table 2 below. Figure 2 gives the visualization of the proposed model's confusion matrix. To further analyze the model's robustness, detection performance evaluation is done across normal and attack types.

Table 2. Results for Cross-Validation

Metric	Value
Accuracy	98.3%
Recall	98.5%
Precision	97.2%
F1-Score	97.8%
FPR	1.2%

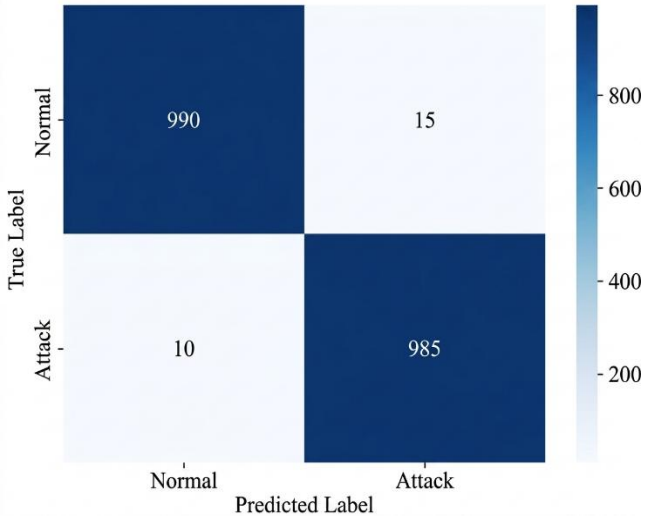

Fig. 2 Proposed confusion matrix

Regarding the fact that the low FPR is significant in real-time attack detection systems, the results prove that the hybrid ML model is effective in attack detection targeting the IoT networks.

4.5. Ablation Study

Ablation research is done with the aim of determining the relative significance of each element to the overall performance. As shown in Table 3 and Figure 3, this research compares the model's performance with and without certain components.

Table 3. Ablation study results

Component Removed	Accuracy	Precision	Recall	F1-Score
Original (with all components)	98.3%	97.2%	98.5%	97.8%
Without Adaptive Feature Extraction	95.7%	94.5%	96.0%	95.2%
Without Context-Aware Hybrid Model	96.8%	95.1%	97.2%	96.1%
Without Lightweight Detection	97.1%	96.4%	97.6%	96.9%

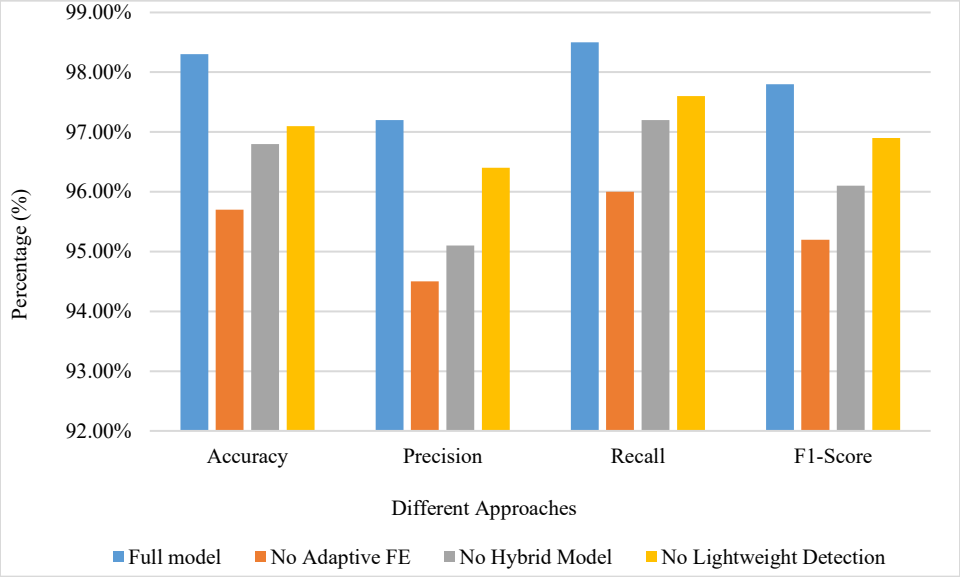

Fig. 3 Ablation study results

By eliminating adaptive feature extraction, the findings demonstrate that the model's accuracy decreased from 98.3% to 95.7%. This decrease is because the system is no longer able to react dynamically to changing attack patterns. It is crucial to dynamically choose the most effective algorithm according to the type of attack, since performance dropped to 96.8% when the context-aware hybrid model was eliminated.

Finally, 97.1% accuracy was achieved after eliminating the lightweight detection technique; nevertheless, real-time detection capabilities are affected by increasing computing costs, which is particularly true in resource-constrained IoT contexts. Attaining the best results with 98.3% accuracy, 97.8% F1-score, and 1.2% FPR, the full model incorporating all components (adaptive feature extraction, context-aware hybrid model, and lightweight detection mechanism) demonstrates that each component makes a significant contribution to the performance of the model. The ablation research proves that the model's adaptability, accuracy, and scalability are all improved by each feature, particularly the context-aware and adaptive capabilities, when applied to real-world IoT situations.

4.6. Performance Comparison

To assess how well the proposed hybrid model performs, it is observed how it stacks up against other recent studies. The researchers conducted studies between 2023 and 2025 that used ML for intrusion prevention and cyberattack detection in IoT networks, which are considered in Table 4 and Figure 4. In [13], they proposed an anomaly detection system for IoT networks utilizing LSTM. Their model came with a recall rate of 94.2 and an accuracy of 96.7.

Although the results were promising, their model was not suitable for real-time application within the IoT under the limitation of resource deployment, owing to the immense computing resources that it required.

To identify cyberattacks on an IoT, [8] developed a hybrid DL technique that associates CNN and LSTM. Its FPR is higher than it is supposed to be, and this indicates that the model is not very good at FPs, although they reported an accuracy of 97.9%. Moreover, the capability of their method in the proposed context-aware hybrid model of dynamically selecting the most efficient algorithm based on the type of attack was a lack.

They offered a decision-tree-based framework to detect anomalies in healthcare processes utilizing IoT systems in [11]. They did this with an accuracy of 96.1; however, as their model was based on smaller DTs, it could not as effectively identify complex attack patterns such as DDoS attacks. Conversely, the proposed hybrid model combines the three models RNN, RF, and CNN to achieve better results with an F1-score of 97.8% and a rating of 98.3% in various types of attacks.

Table 4. Performance comparison with recent works

Model	Accuracy	Precision	Recall	F1-Score
Hybrid Model (CNN + RF + RNN)	98.3%	97.2%	98.5%	97.8%
Saeed et al. (2025) - LSTM-based	96.7%	95.1%	94.2%	94.6%
Alazab et al. (2023) - Hybrid CNN-LSTM	97.9%	96.3%	95.8%	96.0%
Raje et al. (2023) - DT	96.1%	94.8%	95.5%	95.1%

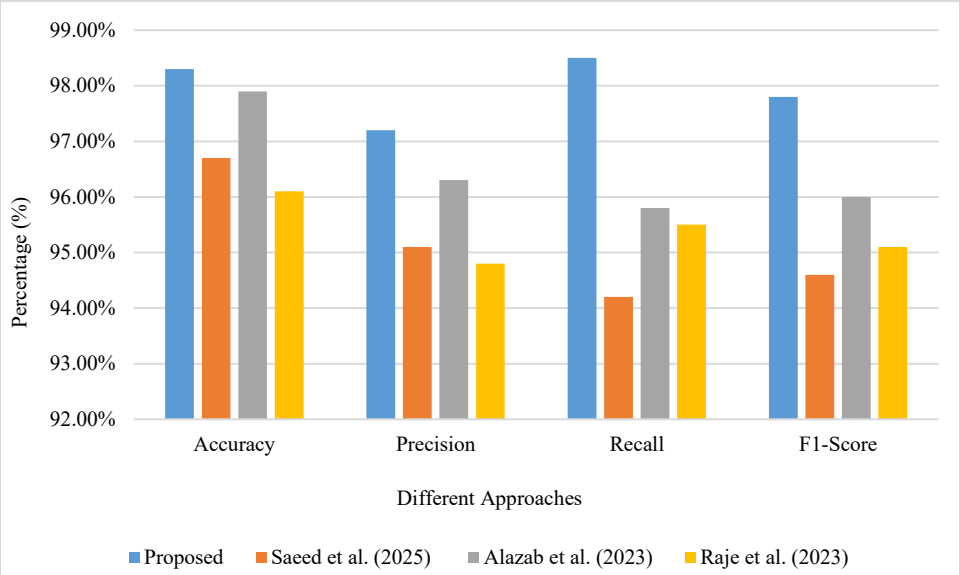

Fig. 4 Performance metrics comparison

When it comes to accuracy, precision, recalls, and F1-score, the hybrid model is superior to the new state-of-the-art methods, like [8, 11, 13]. The adaptive feature extraction and context-aware method of the proposed model greatly decreases the FPRs and increases the accuracy. The hybrid model can perhaps be better suited for IoT real-time deployment, where there are fewer resources to be used.

4.7. Discussion

In practice, in scenarios related to the use of IoT networks with limited resources, the hybrid model will often work better than the traditional ML models and the DL approaches. Due to the association of adaptive feature extraction and the context-sensitive hybrid model, the model can recognize assaults accurately and reduce FPs.

The system can also work well on low-resource devices thanks to the lightweight detection method. The ablation research process can prove the importance of the components of the whole system because it shows that the entire system is the highest performing in all the metrics. The removal of necessary elements, such as adaptive feature extraction and context-aware models, results in a significant performance hit enormously. The high performance of the proposed model is attributed to its dynamic adaptability and real-time model switching. Unlike other static existing models [8, 13], this framework reduces FPR while maintaining high precision, especially under resource-constrained conditions.

5. Conclusion and Future Work

The proposed paper introduces a hybrid ML-based framework of cyberattack detection and prevention in IoT networks. Named with the assistance of adaptive feature extraction, a context-sensitive hybrid model, and a detection mechanism that is lightweight, the proposed technique would enhance the yield of both detection and the cut-down of FPs, as well as ensure real-time outputs, even when working in limited resource settings.

The suggested model outperforms traditional ML models and the state-of-the-art technologies in the field of deep learning with an accuracy rate of 98.3% and an F1-score of 97.8%, as retrieved by the results of 10-fold cross-validation. The lightweight detection system ensures scalability and real-time applications, the adaptive feature extraction and context-conscious hybrid model ensure flexibility and accuracy of detection, and the ablation study confirmed the significant inputs made by each part. Additional testimony on the efficiency and performance benefits of the proposed model was conducted using comparisons to more contemporary works on the topic. In order to ensure the system is more flexible to varying patterns of attacks, we would like to explore the application of reinforcement learning in the future. To confirm the scalability and resilience of the proposed framework, it should be tested in real-world IoT settings with a wider variety of IoT devices and attack scenarios. Additionally, to explore the model's potential use in 5G-

enabled IoT networks and edge computing, two domains where low-latency and high-throughput capabilities are paramount.

Data Availability Statement

The following data is used in this research https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset

Funding Statement

The authors would like to thank Advanced and Innovative Research Laboratory (AAIR Labs- www.aairlab.com), India, for providing financial assistance to carry out this research.

Acknowledgement

We acknowledge the Advanced and Innovative Research Laboratory (AAIR Labs- www.aairlab.com) in India for the technical support.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

References

[1] Bambang Susilo, and Riri Fitri Sari, "Intrusion Detection in IoT Networks using Deep Learning Algorithm," *Information*, vol. 11, no. 5, pp. 1-11, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Noor Ul Ain et al., "Securing IoT Networks Against DDoS Attacks: A Hybrid Deep Learning Approach," *Sensors*, vol. 25, no. 5, pp. 1-23, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] Azhar F. Al-zubidi, Alaa Kadhim Farhan, and Sayed M. Towfek, "Predicting DoS and DDoS Attacks in Network Security Scenarios using a Hybrid Deep Learning Model," *Journal of Intelligent Systems*, vol. 33, no. 1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Mudasir Ali et al., "Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environment," *IEEE Access*, vol. 12, pp. 40682-40699, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Igor Kotenko, Konstantin Izrailov, and Mikhail Buinevich, "Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches," *Sensors*, vol. 22, no. 4, pp. 1-34, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Maria Balega et al., "Enhancing IoT Security: Optimizing Anomaly Detection through Machine Learning," *Electronics*, vol. 13, no. 11, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Usama Tahir et al., "Enhancing IoT Security through Machine Learning-Driven Anomaly Detection," *VFAST Transactions on Software Engineering*, vol. 12, no. 2, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] R. Vinayakumar et al., "Deep Learning for Cyber Security Applications: A Comprehensive Survey," *Authorea Preprints*, pp. 1-36, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Rania A. Elsayed et al., "Securing IoT and SDN Systems using Deep-Learning-based Automatic Intrusion Detection," *Ain Shams Engineering Journal*, vol. 14, no. 10, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Fazlullah Khan et al., "Trustworthy and Reliable Deep-Learning-based Cyberattack Detection in Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1030-1038, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Vaishali V. Raje et al., "Realtime Anomaly Detection in Healthcare IoT: A Machine Learning-Driven Security Framework," *Journal of Electrical Systems*, vol. 19, no. 3, pp. 192-202, 2023. [Google Scholar]

[12] Usman Inayat et al., "Learning-based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects," *Electronics*, vol. 11, no. 9, pp. 1-20, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Mozamel M. Saeed, "An AI-Driven Cybersecurity Framework for IoT: Integrating LSTM-based Anomaly Detection, Reinforcement Learning, and Post-Quantum Encryption," *IEEE Access*, vol. 13, pp. 104027-104036, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[14] Yuhua Yin et al., "IGRF-RFE: A Hybrid Feature Selection Method for MLP-based Network Intrusion Detection on UNSW-NB15 Dataset," *Journal of Big Data*, vol. 10, no. 1, pp. 1-26, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Omar Habibi, Mohammed Chemmakha, and Mohamed Lazaar, "Imbalanced Tabular Data Modelization using CTGAN and Machine Learning to Improve IoT Botnet Attacks Detection," *Engineering Applications of Artificial Intelligence*, vol. 118, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Mohammed Berhili, Omar Chaieb, and Mohammed Benabdellah, "Intrusion Detection Systems in IoT based on Machine Learning: A State of the Art," *Procedia Computer Science*, vol. 251, pp. 99-107, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Md. Alamgir Hossain, "Deep Learning-based Intrusion Detection for IoT Networks: A Scalable and Efficient Approach," *EURASIP Journal on Information Security*, vol. 2025, no. 1, pp. 1-23, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Siqi Yang et al., "Industrial Internet of Things Intrusion Detection System based on Graph Neural Network," *Symmetry*, vol. 17, no. 7, pp. 1-14, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] Ayoob Almotairi et al., "Enhancing Intrusion Detection in IoT Networks using Machine Learning-based Feature Selection and Ensemble Models," *Systems Science and Control Engineering*, vol. 12, no. 1, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Sidra Wajid, and Marta Sans, "Internet of Things Security: Leveraging AI and Machine Learning for Anomaly Detection," pp. 1-9, 2023. [Google Scholar]

[21] Asad Raza et al., "Machine Learning-based Security Solutions for Critical Cyber-Physical Systems," *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, Istanbul, Turkey, pp. 1-6, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Nookala Venu, AArun Kumar, and A.Sanyasi Rao, "Botnet Attacks Detection in Internet of Things using Machine Learning," *NeuroQuantology*, vol. 20, no. 4, pp. 743-754, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Asma Jahangeer et al., "A Review on the Security of IoT Networks: from Network Layer's Perspective," *IEEE Access*, vol. 11, pp. 71073-71087, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] Abdullah Alomiri, Shailendra Mishra, and Mohammed AlShehri, "Machine Learning-based Security Mechanism to Detect and Prevent Cyber-Attack in IoT Networks," *International Journal of Computing and Digital Systems*, vol. 16, no. 1, pp. 645-659, 2024. [CrossRef] [Google Scholar] [Publisher Link]