



## RECURSIVE VOTING FUSION: AN RFE-BASED ENSEMBLE MODEL FOR CATEGORIZING IOT DDOS ATTACKS

Piyush M. Prajapati<sup>\*1</sup>, Priyesh P. Gandhi<sup>2</sup>, Sheshang Degadwala<sup>3</sup>,  
Keyur Brahmhatt<sup>4</sup>, Swapnil M Parikh<sup>5</sup>

<sup>1</sup>Computer Engineering, Gujarat Technological University, Ahmedabad, Gujarat, India.

<sup>2</sup>Provost, Sigma University, Vadodara, Gujarat, India.

<sup>3</sup>Department of Computer Engineering, Sigma University, Vadodara, Gujarat, India.

<sup>4</sup>Department of Computer Engineering, Sigma University, Vadodara, Gujarat, India.

<sup>5</sup>Computer Science and Engineering, Parul Institute of Technology, Parul University, Vadodara, Gujarat, India.

<sup>1</sup><https://orcid.org/0009-0000-8148-0410>, <sup>2</sup><https://orcid.org/0000-0001-5338-3111>, <sup>3</sup><https://orcid.org/0000-0002-2385-7790>,

<sup>4</sup><https://orcid.org/0000-0001-7478-3173>, <sup>5</sup><https://orcid.org/0009-0005-8816-5508>

Email: \*[piyush.prj@gmail.com](mailto:piyush.prj@gmail.com), [priyeshgandhi@gmail.com](mailto:priyeshgandhi@gmail.com), [sheshang13@gmail.com](mailto:sheshang13@gmail.com), [keyur.brahmbhatt@bvmengineering.ac.in](mailto:keyur.brahmbhatt@bvmengineering.ac.in),  
[swapnil.parikh17761@paruluniversity.ac.in](mailto:swapnil.parikh17761@paruluniversity.ac.in)

### ARTICLE INFO

#### Article History

Received: March 13, 2026

Reviewed: April 15, 2026

Accepted: July 15, 2026

Published: August 31, 2026

#### Keywords:

Distributed Denial of Service,  
Internet of Things,  
Recursive Feature Elimination,  
Ensemble Machine Learning,  
Intrusion Detection Systems.

### ABSTRACT

The rise of the Internet of Things (IoT) devices has led to an enormous vulnerability to multiple DDoS attacks, including low-rate traffic disruption and high-rate SYN Floods. This increasing menace underscores the importance of proper multi-classification methods that can detect various DDoS attack patterns. Nonetheless, most of the current machine learning models cannot provide a generalization between various DDoS types that include DDoS-ACK Fragmentation, DDoS-HTTP Flood, DoS-TCP Flood, and DDoS-SYN Flood. Non-linear Support Vector Machines (SVM) which are traditional classifiers tend to have poor performance when trying to differentiate subtle differences between these types of attacks. To overcome this drawback, this paper suggests a Recursive Voting Fusion model, which involves Recursive Feature Elimination (RFE) as the method of optimum feature selection and an ensemble approach to the robust classification. The framework is a hybrid of Decision Tree, Random Forest, and Extra tree classifiers where soft voting is used. It is experimentally demonstrated that the proposed approach has 99 per cent accuracy, precision, recall, and F1-score, and 99 per cent MCC and AUC-ROC, which is significantly higher than the baseline models. It implies that the model is highly robust and scalable to be used in real-time IoT intrusion detection and efficient mitigation of the developing DDoS threats.



Copyright ©2026 by authors and Galileo Institute of Technology and Education of the Amazon (ITEGAM). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

### I. INTRODUCTION

The fast growth of the Internet of Things (IoT) has introduced new standards of connectivity, autonomous automation, and efficiency in business fields like healthcare, smart cities, agriculture, transportation, and manufacturing [1-3]. Nevertheless, this enhanced interconnectedness has expanded the area of attack by cyber threats. Distributed Denial of Service (DDoS) attacks are among these and currently one of the most unsettling and mostly launched cyberattacks on IoT infrastructures [4-6]. The IoT devices are relatively resource-limited and oftentimes have the bare-minimum security protocols installed, which makes them the best targets of botnet infection which can then be utilized to execute massive, multi-vector DDoS attack [7], [8]. An example of such an attack that caused havoc on the global internet is the 2016 Mirai botnet attack that used insecure IoT devices to flood the DNS provider Dyn [9], [10]. The all-purpose classification of DDoS attacks may be done by the attacker by the type of the network stack and the point of entry into the victim network [11-13]. Attacks that can occur at the network layer are TCP SYN Flood, UDP Flood, and ICMP Flood, which aim to either consume bandwidth or connection queues with a flood of packets. Fragmentation vulnerabilities can be used at the transport layer by means of ACK Fragmentation and UDP Fragmentation [14-16].

Applications layer is prone to advanced attacks such as the HTTP Flood and DNS Amplification that are harder to detect since they imitate the normal user actions. These attacks vary in frequency, packet size and protocol exploitation and multi-classification is essential to identify and mitigate them more accurately [17], [18]. Although the intrusion detection systems (IDS) research field has been researched extensively, machine learning-based IoT DDoS detection solutions are associated with three major limitations [19-21]. To begin with, they demonstrate low generalization abilities with different classes of DDoS, often classifying less common or more intricate attacks [22-24]. Second, most models are not very robust at feature selection that may lead to incorporation of redundant or noisy features that multiply computational requirements and poor performance [25-27]. Third, the presence of imbalance in classes in datasets distorts the learning process, as it leads to biased prediction on the most prevalent types of attacks and ignoring rare but essential threats [28], [29]. As an example, traditional models, e.g. Support Vector Machines (SVM) and Naive Bayes, provide poor macro-average F1-scores and are unable to detect attacks, such as DDoS-ICMP Flood or UDP Fragmentation [30], [31]. To overcome them, the paper will suggest Recursive Voting Fusion, a new framework of ensemble classifications, which aims to precisely and effectively identify various types of IoT-based DDoS attacks. The framework combines Recursive Feature Elimination (RFE) to discover the most discriminative set of features, in other words, noise reduction and improved classification accuracy. The fundamental classifier consists of a hard voting set of Decision Tree, Random Forest and Extra Tree models which are combined to exploit multiple learning biases to enhance detection strength. The key aim of this study is to work on a lightweight, scalable, and high-accuracy multi-class DDoS detecting system that can be used in the real-time IoT security system. The study intends to: (i) identify 15 different IoT DDoS and DoS attack types with high accuracy, (ii) optimize the performance of the model based on feature selection (iii) compare the system to the principles of the traditional classifier to prove its excellence. An experimental analysis of the labeled IoT DDoS data indicates that the proposed model has 99% accuracy, precision, recall, and F1-score, and MCC and AUC-ROC of 0.99. Recursive Voting Fusion is much more effective on all the measures compared to baseline classifiers like SVM (25%), KNN (97%), and Naive Bayes (54%). Additionally, the model is highly recalled in complex subcategories like HTTP Flood, DNS Amplification, and Smurf and, therefore, it shows effectiveness in detecting threat subtly. The suggested system is a resource-saving, practical proposal of the IoT networks in the contemporary era, which have been added to not only academic development but also the implementation of the solution and solution to the proposed-system in proactive DDoS prevention models.

## II. THEORETICAL REFERENCE

The exponentially accelerated development of Internet of Things (IoT) technologies has increased connectivity and smart automation in the industrial sector. Nevertheless, the very resource-limited character of the IoT devices and their massive deployment has predisposed them to the DDoS attacks. This has made effective and smart systems of detection instrumental in detecting and categorizing and curtailing such threats. The given literature review discusses the recent trends in machine learning (ML) and deep learning (DL) systems to identify multi-class DDoS attacks in IoT setups, particularly ensemble models, feature selection algorithms, and class imbalance. By [1] suggested a hybrid learning model to identify cyberattacks using IoT-based detection that takes advantage of feature transformation and a collection of classifiers to identify advanced threats. In turn [2] have made a comparative analysis of anomaly detection techniques and highlighted the trade of between unsupervised and supervised techniques in IoT networks. The strength of sequence-based models of dynamic traffic analysis is demonstrated with the help of LSTM networks applied to the CIC-IoT2023 dataset by [3], who identified the temporal patterns of attacks. An intrusion detection system was introduced by [4] that employs convolutional layers and autoencoders to identify DDoS traffic using deep learning. According to [5] took the idea a step further and suggested a hybrid CNN-BiLSTM system to also address low-rate DDoS attacks that are especially difficult to detect because of their insidious traffic signature. In turn [6] scaled recurrent neural architectures to real-life IoT settings, with an emphasis on scalability and accuracy. In healthcare systems that rely on the IoT, which are critical regarding security, [7] used machine learning to detect anomalies. Their work represented better performance in case of engineered features based on domain knowledge. By [8] suggested CKAN model (Convolutional Kolmogorov-Arnold Networks) that was able to identify non-linear relationships within IoT traffic to be able to classify them effectively. In a similar way, [9] proposed a deep ensemble learning method with pruning, which maximizes the accuracy of detection and efficiency of computing DDoS detection. By [10] also applied Principal Component Analysis (PCA), which increases the accuracy and efficiency of computation in the detection of DDoS. In order to address the issue of detection robustness, [11] developed a hybrid system which combines feature selection based on filters with ensemble classifiers.

In turn [12] extended their model by using SMOTE-ENN to balance the data and effective feature selection so that the model can be better at minority classes. By [13] concentrated on detecting DDoS in the IoT applications based on supervised machine learning models and showed significant enhancement with random forest and SVM. By [14] created a hybrid intrusion detection framework of the cyber-physical systems with the best feature selection based on correlation and mutual information parameters. A hybrid feature selection algorithm, LightGBM with a modified slap swarm algorithm, was proposed by [15], and it demonstrated significant performance in the context of big data IoT. [16] have suggested a multi-class intrusion detection system based on transformers and CIC-IoT-2023 dataset, demonstrating great versatility to complicated traffic patterns. In turn [17] compared different deep learning models in the context of the IoT intrusion classification and have demonstrated that ensemble deep learning models were more effective in multiclass configurations in comparison with single architectures. According to [18] reused their previous methodology and critically analyzed some machine learning algorithms on the CIC-IoT2023 dataset. By [19] boosted the intrusion detection by using a twostep clustering method, which makes the system more sensitive to detect low level DDoS activities. VGGIncepNet developed by [20] involved non-image-to-image conversion methods and CNN architecture in intrusion detection, and it achieved better spatial feature extraction. By [21] have created an agent-based system that automates the process of feature extraction and selection in detecting DDoS, minimizing preprocessing costs by hand and enhancing the real-time results. According to [22] offered a smart architecture that combines various levels of detection in order to identify threats, which is optimized in terms of IoT scale throughput and latency. By [23] made the CICIoT2023 dataset available and made it a reference on how to measure large-scale IoT attacks. In turn [24] proposed the attention mechanism-enhanced CNN-BiLSTM model and it was found to be of great significance in the classification of DDoS variants such as TCP SYN and ICMP floods.

By [25] gave a broad overview of the ML methods to detect DDoS in IoT and proposed the future research opportunities in adaptive and self-healing detection systems. In turn [26] introduced a hybrid DDoS detector based on CNN and GRU, with high accuracy results and robustness. The work by [27] compared the performance of the common ML classifiers to the CIC-IDS2017 dataset, indicating the ensemble learning as the future direction. By [28] developed IoT-specific intrusion detection system based on standard ML algorithms and emphasize the relevance of features to achieve high classification performance using the CICIoT dataset. In turn [29] trained the Random Forest models with the purpose of DDoS detection in the IoT and verified its functionality using the CICIoT dataset. According to [30] maximized the performance of AdaBoost through undersampling and hyperparameter optimization, which shown that pre-processing of data has a significant impact on model accuracy. Finally, Avc\u0131 and by [31] used supervised learning-based method of predicting DDoS in building management systems and stated that such models can be generalized to all smart infrastructure. As noted in the reviewed literature, use of deep learning architectures such as LSTM, CNN-BiLSTM, transformers; ensemble techniques involving multiple classifiers; and feature selection techniques including PCA, SMOTE-ENN, and swarm algorithms have several promising trends. Nonetheless, the majority of studies are related to binary classification or definite types of DDoS without multiclass categorization. In addition, features selection is also understudied or uses heuristic methods. Also, the datasets do not possess the appropriate class balance, which is poorly addressed in most of the models, limiting the performance on minor types of DDoS.

### III. MATERIALS AND METHODS

Figure 1 indicates a very elaborate and methodically formatted pipeline that is to be used in the detection of Distributed Denial of Service (DDoS) attacks in Internet of Things (IoT) systems by using a powerful voting-based ensemble machine learning framework. This all-encompassing flowchart summarizes six sequential stages and interdependent ones, which represent the essential part of the entire data analytics and cybersecurity workflow starting with the first data acquisition and preprocess, feature extraction, model training, and eventual decision-making. The basis of this framework is the CICIoT2023 dataset [23] a balanced and well-curated dataset consisting of fifteen types of DDoS attacks, with one hundred samples each or a total of 1,500 rows and 47 columns. The variety and realism of the dataset is closely related to the real-world situation of IoT network, which contributes to the higher generalizability and effectiveness of the approach proposed to detect intrusion.

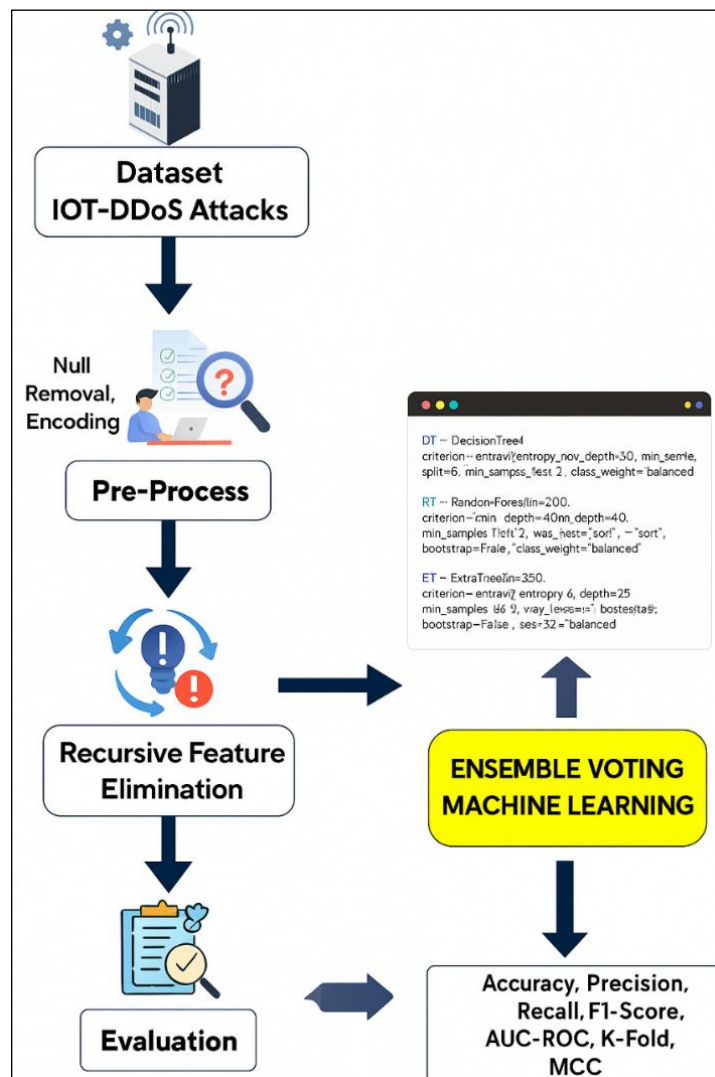


Figure 1: Flow Diagram of Recursive Voting Fusion.  
Source: Authors, (2026).

### III.1 PSEUDO CODE

```

1: D ← load_dataset()
2: D ← preprocess(D) // null removal, encoding
3: F ← RFE(D, k=30)
4: X_train, X_val, y_train, y_val ← train_test_split(F)
5: DT ← DecisionTree(criterion='entropy', max_depth=30, min_samples_split=4,
    min_samples_leaf=2, class_weight='balanced')
6: RF ← RandomForest(n=200, criterion='gini', max_depth=40, min_samples_split=3,
    min_samples_leaf=2, max_feat='sqrt', bootstrap=True,
    class_weight='balanced', seed=42)
7: ET ← ExtraTrees(n=250, criterion='entropy', max_depth=35, min_samples_split=3,
    min_samples_leaf=1, max_feat='log2', bootstrap=False,
    class_weight='balanced', seed=42)
8: VC ← VotingClassifier([('DT', DT), ('RF', RF), ('ET', ET)], voting='hard')
9: VC.fit(X_train, y_train)
10: y_pred ← VC.predict(X_val)
11: acc ← Accuracy(y_val, y_pred)
12: prec ← Precision(y_val, y_pred)
13: rec ← Recall(y_val, y_pred)
14: f1 ← F1(y_val, y_pred)
15: auc ← AUC_ROC(y_val, VC, multi_class='ovr')
16: mcc ← MCC(y_val, y_pred)
17: KF ← KFold(n_splits=5)
18: scores ← cross_val_score(VC, F, y, cv=KF)

```

### III.2 DATASET: CICIOT2023 (1500 SAMPLES, 15 CLASSES)

At the core of this pipeline is the CICIOT2023 dataset [23], a benchmark dataset designed to reflect real-time and large-scale attacks specifically tailored for IoT networks. Table 1. encompasses 47 columns or features and 15 types of cyberattack classes including botnets, brute-force, infiltration, and various types of DDoS patterns each represented by 100 samples. The dataset includes high-resolution telemetry such as:

- Network traffic features (e.g., source IP, destination IP, protocol, packet count, byte count)
- Flow behavior metrics (e.g., flow duration, flow bytes per second, inter-arrival time)
- Attack signatures relevant to multi-vector DDoS scenarios

Using a uniform class distribution (100 samples/class) helps in mitigating class imbalance, a major challenge in supervised classification tasks. The dataset ensures diversity in attack vectors, making the model generalizable and robust for real-world intrusion detection systems (IDS) in IoT ecosystems.

Table 1: Dataset Columns Description.

| Column Name     | Description                                                           |
|-----------------|-----------------------------------------------------------------------|
| flow_duration   | Total duration of the network flow (in microseconds or milliseconds). |
| Header_Length   | Length of the packet headers.                                         |
| Protocol Type   | Type of transport protocol used (e.g., TCP, UDP, ICMP).               |
| Duration        | Duration of the specific activity/connection.                         |
| Rate            | Average transmission rate of packets or bytes.                        |
| Srate           | Source-to-destination packet transmission rate.                       |
| Drate           | Destination-to-source packet transmission rate.                       |
| fin_flag_number | Number of FIN flags observed (connection termination signal).         |
| syn_flag_number | Number of SYN flags (used to initiate a TCP connection).              |
| rst_flag_number | Number of RST flags (used to reset a TCP connection).                 |
| psh_flag_number | Number of PSH flags (push data to receiving app).                     |
| ack_flag_number | Number of ACK flags (acknowledge receipt).                            |
| ece_flag_number | Number of ECE flags (Explicit Congestion Notification Echo).          |
| cwr_flag_number | Number of CWR flags (Congestion Window Reduced).                      |
| ack_count       | Count of packets with ACK flag set.                                   |
| syn_count       | Count of packets with SYN flag set.                                   |
| fin_count       | Count of packets with FIN flag set.                                   |

|            |                                                       |
|------------|-------------------------------------------------------|
| urg_count  | Count of packets with URG (urgent) flag set.          |
| rst_count  | Count of packets with RST flag set.                   |
| HTTP       | Indicator/count for HTTP protocol usage.              |
| HTTPS      | Indicator/count for HTTPS protocol usage.             |
| DNS        | Indicator/count for DNS protocol usage.               |
| Telnet     | Indicator/count for Telnet protocol usage.            |
| SMTP       | Indicator/count for SMTP protocol usage.              |
| SSH        | Indicator/count for SSH protocol usage.               |
| IRC        | Indicator/count for IRC protocol usage.               |
| TCP        | Indicator/count for TCP protocol usage.               |
| UDP        | Indicator/count for UDP protocol usage.               |
| DHCP       | Indicator/count for DHCP protocol usage.              |
| ARP        | Indicator/count for ARP protocol usage.               |
| ICMP       | Indicator/count for ICMP protocol usage.              |
| IPv        | IP version indicator (IPv4 or IPv6).                  |
| LLC        | Indicator/count for LLC (Logical Link Control) usage. |
| Tot sum    | Total sum of packet sizes in the flow.                |
| Min        | Minimum packet size in the flow.                      |
| Max        | Maximum packet size in the flow.                      |
| AVG        | Average packet size in the flow.                      |
| Std        | Standard deviation of packet sizes.                   |
| Tot size   | Total size of the data transferred in the flow.       |
| IAT        | Inter-arrival time between packets.                   |
| Number     | Total number of packets in the flow.                  |
| Magnitude  | Magnitude of packet payloads or statistical metric    |
| Radius     | Statistical feature showing distance in feature space |
| Covariance | Covariance between selected flow parameters.          |
| Variance   | Variance of packet sizes or times in the flow.        |
| Weight     | Weight assigned to the flow                           |
| label      | Class label                                           |

Source: Authors, (2026).

### III.3 PRE-PROCESSING: NULL VALUE HANDLING AND ENCODING

Once the dataset is acquired, the first critical step is data pre-processing, which ensures the dataset is clean and suitable for machine learning algorithms. The dataset, derived from [23], includes multiple features that may contain null or missing values and categorical fields that are not directly interpretable by machine learning models.

- Null Value Handling: Missing values in the dataset can degrade the performance of classifiers. Let the dataset be represented as a matrix  $X \in \mathbb{R}^{n \times m}$ , where  $n = 1500$  samples and  $m$  features. A missing value in element  $x_{ij}$  (i.e., the value at the  $i$ th row and  $j$ th column) is either removed if the percentage of missingness is negligible, or imputed using statistical methods such as: Mean imputation:

$$x_{ij} = (1/N) \sum_{k=1}^N x_{kj} \quad (1)$$

K-Nearest Neighbors imputation (KNN):

$$x_{ij} = \text{mean}(\{x_{pj} \mid x_p \in N_k(x_i)\}) \quad (2)$$

- Encoding: Categorical variables such as protocol or flag type are transformed into numerical format using encoding schemes. For nominal variables  $C = \{c_1, c_2, \dots, c_k\}$ , One-Hot Encoding creates binary vectors for each class label:

$$\text{Encoded}(c_j) = [0, 0, \dots, 1, \dots, 0] \quad (3)$$

### III.4 RECURSIVE FEATURE ELIMINATION (RFE)

After the data is cleaned and numerically encoded, the next step is Recursive Feature Elimination (RFE). This is a feature selection technique that aims to reduce the dimensionality of the feature space while preserving the most predictive attributes.

$$X = [x_1, x_2, \dots, x_m] \quad (4)$$

$$\text{Feature Set}_{t+1} = \text{Feature Set}_t \setminus \{\arg\min_{x_j \in \text{Feature Set}_t} I(x_j)\} \quad (5)$$

### III.5 ENSEMBLE VOTING-BASED MACHINE LEARNING

The core of the detection framework is a Voting-Based Ensemble Model, which integrates predictions from multiple classifiers to improve robustness and accuracy. The ensemble here consists of Decision Tree (DT), Random Forest (RF), and Extra Trees (ET) classifiers each tuned with specific hyperparameters to maximize performance and diversity.

**Decision Tree (DT):** The Decision Tree is built using the Entropy-based Information Gain criterion. The entropy  $H(S)$  of a dataset  $S$  is calculated as:

$$H(S) = -\sum_{i=1}^k p_i \log_2(p_i) \quad (6)$$

Where  $p_i$  is the proportion of samples belonging to class  $i$ . A split at node  $N$  aims to maximize the Information Gain (IG):

$$IG(S,A) = H(S) - \sum_{v \in \text{Values}(A)} (|S_v| / |S|) H(S_v) \quad (7)$$

The tree's growth is constrained by maximum depth  $d = 30$ , minimum samples to split  $s = 4$ , and minimum leaf size  $l = 2$ . Class weights are balanced to counteract skewed class distributions. **Random Forest (RF):** The Random Forest is an ensemble of decision trees trained using bootstrap aggregation (bagging) and random feature selection. Let  $T = \{t_1, t_2, \dots, t_n\}$  denote the set of  $n = 200$  decision trees, each trained on a bootstrap sample from the dataset. The Gini index is used to determine optimal splits:

$$\text{Gini}(S) = 1 - \sum_{i=1}^k p_i^2 \quad (8)$$

Each tree considers a random subset of features (square root of total features) at each split, increasing diversity among trees. The output class is determined by majority vote:

$$\hat{y} = \text{mode}(\{t_i(x) \mid i = 1, \dots, n\}) \quad (9)$$

**Extra Trees (ET):** The Extra Trees classifier is like Random Forest but introduces additional randomness by selecting split thresholds at random, rather than choosing the best threshold. Here,  $n = 250$  trees are grown without bootstrapping (entire dataset used), and split criterion is entropy. The maximum number of features at each split is set to  $\log_2(m)$ , where  $m$  is the total number of features.

$$\text{max features} = \log_2(m) \quad (10)$$

### III.6 EVALUATION METRICS

After model training, the ensemble classifier is evaluated using a comprehensive set of metrics that capture different dimensions of performance.

- **Accuracy:** Measures overall correctness:

$$\text{Accuracy} = (TP + TN) / (TP + TN + FP + FN) \quad (11)$$

- **Precision and Recall:** Precision measures the correctness of positive predictions, and recall measures completeness:

$$\text{Precision} = TP / (TP + FP) \quad (12)$$

$$\text{Recall} = TP / (TP + FN) \quad (13)$$

- **F1-Score:** The harmonic means of precision and recall:

$$F1 = 2 * (\text{Precision} * \text{Recall}) / (\text{Precision} + \text{Recall}) \quad (14)$$

- **K-Fold Cross Validation:** The dataset is split into  $K$  equal parts. For each iteration,  $K - 1$  parts are used for training and 1 for testing. This is repeated  $K$  times, and the results are averaged:

$$\text{Cross-validation Accuracy} = (1/K) \sum_{i=1}^K \text{Accuracy}_i \quad (15)$$

- **Matthews Correlation Coefficient (MCC):** A balanced measure for classification performance:

$$\text{MCC} = (TP * TN - FP * FN) / \sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)} \quad (16)$$

This metric is particularly useful in multi-class problems or where class imbalance exists, as it takes all four confusion matrix categories into account. In summary, sub section 1.2 through 1.6 form the core computational and analytical backbone of proposed system pipeline. Each step from data cleansing and transformation, through intelligent feature reduction, to the highly optimized ensemble model contributes to a robust and interpretable system for IoT DDoS attack detection, validated by rich evaluation strategies.

#### IV. RESULTS AND DISCUSSIONS

To provide an efficient training and evaluation of the proposed ensemble intrusion detection model, the result analysis was performed in the Google Colab environment with a T4 GPU setting. The data used in the CICIoT2023 consist of 15 classes with 1500 samples per class, which was split into an 80:20 train-test to ensure a balanced evaluation environment was obtained. In order to test the strength of the model, a cross-validation strategy (5 folds) was applied and gave coherent performance forecasts across various data subsets. The proposed ensemble model, a combination of Decision Tree, Random Forest, and Extra Trees classifiers with optimized hyperparameters, was compared to each other in terms of comparative effectiveness. The accuracy, the precision, the recall, the F1-score, and the ROC-AUC, which are the evaluation metrics, had better performance of the ensemble framework especially in the class imbalance and complicated patterns. The ability of the model to discriminate was also demonstrated by Receiver Operating Characteristic (ROC) curves that demonstrated high true positive rates across classes. Such extensive experimentation highlights the generalization capability and usefulness of the system in the IoT-based intrusion detection. Figure 2. represents the loaded dataset of 1500 rows and 47 columns. It contains such attributes as flow duration, Header length, Protocol type and other measures of traffic rates, which is probably intended to perform DDoS detection work.

|      | flow_duration | Header_Length | Protocol Type | Duration | Rate       | Srate      | Draft |
|------|---------------|---------------|---------------|----------|------------|------------|-------|
| 0    | 0.000000      | 0.00          | 1.00          | 64.00    | 4.475459   | 4.475459   | 0     |
| 1    | 0.000000      | 0.00          | 1.00          | 64.00    | 3.053283   | 3.053283   | 0     |
| 2    | 0.015796      | 8.21          | 1.21          | 64.53    | 59.344342  | 59.344342  | 0     |
| 3    | 0.010202      | 17.78         | 1.10          | 64.00    | 36.765677  | 36.765677  | 0     |
| 4    | 0.000000      | 0.00          | 1.00          | 64.00    | 3.005904   | 3.005904   | 0     |
| ...  | ...           | ...           | ...           | ...      | ...        | ...        | ...   |
| 1495 | 158.952476    | 37496.78      | 6.83          | 92.13    | 52.782361  | 52.782361  | 0     |
| 1496 | 45.475748     | 4584.10       | 6.48          | 61.12    | 0.479950   | 0.479950   | 0     |
| 1497 | 7.095029      | 415266.79     | 5.96          | 84.52    | 129.443848 | 129.443848 | 0     |
| 1498 | 20.909274     | 445858.82     | 6.22          | 88.81    | 38.287177  | 38.287177  | 0     |
| 1499 | 1.584323      | 1301.07       | 5.88          | 62.64    | 2.913833   | 2.913833   | 0     |

1500 rows x 47 columns

Figure 2: Dataset Load.

Source: Authors, (2026).

Figure 3. compares the performance of five dimensionality reduction methods (SPCA, SRP, GRP, KB, RFE) over 10, 20, and 30 features. RFE (Recursive Feature Elimination) shows the highest accuracy at all feature levels, peaking at 30 features with 0.8483.

|    | SPCA     | SRP      | GRP      | KB       | RFE      |
|----|----------|----------|----------|----------|----------|
| 10 | 0.797500 | 0.785000 | 0.817500 | 0.666667 | 0.815000 |
| 20 | 0.820833 | 0.815833 | 0.816667 | 0.792500 | 0.836667 |
| 30 | 0.827500 | 0.821667 | 0.818333 | 0.842500 | 0.848333 |

Figure 3: Feature Selection Methods.

Source: Authors, (2026).

Figure 4. bar chart displays the RFE feature ranking. Lower scores indicate more important features. The red line marks the top 30 selected features, with flow\_duration, Header\_Length, and Protocol\_Type ranked highest (best features).

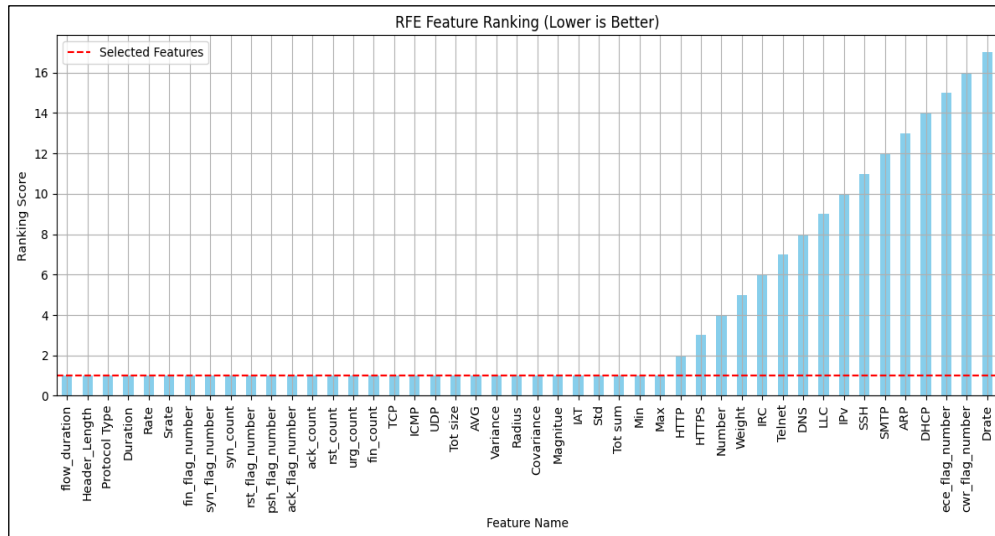


Figure 4: RFE 30-Features Selected.

Source: Authors, (2026).

Figure 5. shows confusion matrices and classification metrics for K-Nearest Neighbors and SVM classifiers. KNN performs very well (accuracy: 0.97, MCC: 0.9679), while SVM struggles significantly (accuracy: 0.25, MCC: 0.2379), indicating poor performance on this dataset.

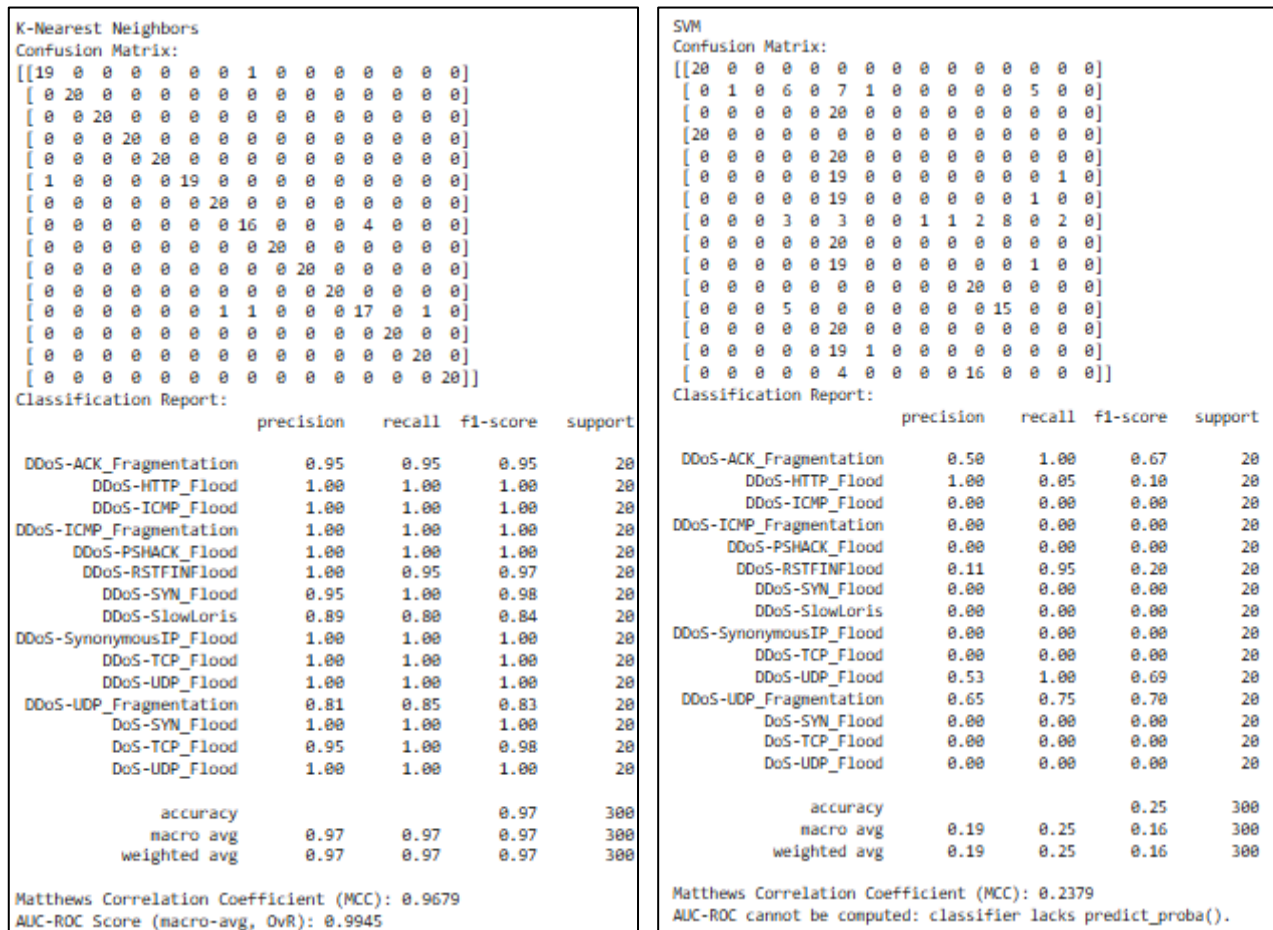


Figure 5: KNN and SVM Model Evaluation.

Source: Authors, (2026).

Figure 6, The confusion matrices and reports show that both Decision Tree and Random Forest classifiers perform excellently, with macro and weighted F1-scores above 0.98. Random Forest slightly outperforms with an MCC of 0.9822.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |           |        |          |         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |           |        |          |         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------|----------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------|----------|---------|
| <b>Decision Tree</b><br>Confusion Matrix:<br><pre>[[19 0 0 0 0 0 0 1 0 0 0 0 0 0 0]  [ 0 19 0 1 0 0 0 0 0 0 0 0 0 0 0]  [ 0 0 20 0 0 0 0 0 0 0 0 0 0 0 0]  [ 0 0 0 20 0 0 0 0 0 0 0 0 0 0 0]  [ 0 0 0 0 20 0 0 0 0 0 0 0 0 0 0]  [ 0 0 0 0 0 20 0 0 0 0 0 0 0 0 0]  [ 0 0 0 0 0 0 20 0 0 0 0 0 0 0 0]  [ 0 0 0 0 0 0 0 20 0 0 0 0 0 0 0]  [ 0 0 0 0 0 0 0 0 20 0 0 0 0 0 0]  [ 0 0 0 0 0 0 0 0 0 20 0 0 0 0 0]  [ 0 0 0 0 0 0 0 0 0 0 20 0 0 0 0]  [ 0 0 0 0 0 0 0 0 0 0 0 20 0 0 0]  [ 0 0 0 0 0 0 0 0 0 0 0 0 20 0 0]  [ 0 0 0 0 0 0 0 0 0 0 0 0 0 20 0]  [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 20]]</pre> Classification Report: |           |        |          |         | <b>Random Forest</b><br>Confusion Matrix:<br><pre>[[18 2 0 0 0 0 0 0 0 0 0 0 0 0 0]  [ 0 17 0 0 0 0 0 0 1 2 0 0 0 0 0]  [ 0 0 20 0 0 0 0 0 0 0 0 0 0 0 0]  [ 0 0 0 20 0 0 0 0 0 0 0 0 0 0 0]  [ 0 0 0 0 20 0 0 0 0 0 0 0 0 0 0]  [ 0 0 0 0 0 20 0 0 0 0 0 0 0 0 0]  [ 0 0 0 0 0 0 20 0 0 0 0 0 0 0 0]  [ 0 0 0 0 0 0 0 20 0 0 0 0 0 0 0]  [ 0 0 0 0 0 0 0 0 20 0 0 0 0 0 0]  [ 0 0 0 0 0 0 0 0 0 20 0 0 0 0 0]  [ 0 0 0 0 0 0 0 0 0 0 20 0 0 0 0]  [ 0 0 0 0 0 0 0 0 0 0 0 20 0 0 0]  [ 0 0 0 0 0 0 0 0 0 0 0 0 20 0 0]  [ 0 0 0 0 0 0 0 0 0 0 0 0 0 20 0]  [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 20]]</pre> Classification Report: |           |        |          |         |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | precision | recall | f1-score | support |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | precision | recall | f1-score | support |
| DDoS-ACK_Fragmentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 0.95      | 0.95   | 0.95     | 20      | DDoS-ACK_Fragmentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 1.00      | 0.90   | 0.95     | 20      |
| DDoS-HTTP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 1.00      | 0.95   | 0.97     | 20      | DDoS-HTTP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 0.89      | 0.85   | 0.87     | 20      |
| DDoS-ICMP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 1.00      | 1.00   | 1.00     | 20      | DDoS-ICMP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 1.00      | 1.00   | 1.00     | 20      |
| DDoS-ICMP_Fragmentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 0.95      | 1.00   | 0.98     | 20      | DDoS-ICMP_Fragmentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 1.00      | 1.00   | 1.00     | 20      |
| DDoS-PSHACK_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 1.00      | 1.00   | 1.00     | 20      | DDoS-PSHACK_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 1.00      | 1.00   | 1.00     | 20      |
| DDoS-RSTFINFlood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 1.00      | 1.00   | 1.00     | 20      | DDoS-RSTFINFlood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 1.00      | 1.00   | 1.00     | 20      |
| DDoS-SYN_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 1.00      | 1.00   | 1.00     | 20      | DDoS-SYN_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 1.00      | 1.00   | 1.00     | 20      |
| DDoS-SlowLoris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 0.95      | 0.95   | 0.95     | 20      | DDoS-SlowLoris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 0.95      | 1.00   | 0.98     | 20      |
| DDoS-SynonymousIP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 1.00      | 1.00   | 1.00     | 20      | DDoS-SynonymousIP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 0.91      | 1.00   | 0.95     | 20      |
| DDoS-TCP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 1.00      | 1.00   | 1.00     | 20      | DDoS-TCP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 1.00      | 1.00   | 1.00     | 20      |
| DDoS-UDP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 1.00      | 1.00   | 1.00     | 20      | DDoS-UDP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 1.00      | 1.00   | 1.00     | 20      |
| DDoS-UDP_Fragmentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 1.00      | 1.00   | 1.00     | 20      | DDoS-UDP_Fragmentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 1.00      | 1.00   | 1.00     | 20      |
| DoS-SYN_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 1.00      | 1.00   | 1.00     | 20      | DoS-SYN_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 1.00      | 1.00   | 1.00     | 20      |
| DoS-TCP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 1.00      | 1.00   | 1.00     | 20      | DoS-TCP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 1.00      | 1.00   | 1.00     | 20      |
| DoS-UDP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 1.00      | 1.00   | 1.00     | 20      | DoS-UDP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 1.00      | 1.00   | 1.00     | 20      |
| accuracy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |        | 0.99     | 300     | accuracy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |        | 0.98     | 300     |
| macro avg                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 0.99      | 0.99   | 0.99     | 300     | macro avg                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 0.98      | 0.98   | 0.98     | 300     |
| weighted avg                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 0.99      | 0.99   | 0.99     | 300     | weighted avg                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 0.98      | 0.98   | 0.98     | 300     |
| Matthews Correlation Coefficient (MCC): 0.9893<br>AUC-ROC Score (macro-avg, OvR): 0.9946                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |        |          |         | Matthews Correlation Coefficient (MCC): 0.9822<br>AUC-ROC Score (macro-avg, OvR): 0.9983                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |        |          |         |

Figure 6: Decision Tree and Random Forest Model Evaluation.

Source: Authors, (2026).

Figure 7, Naïve Bayes yields moderate performance (MCC: 0.5268), struggling with class precision. In contrast, Extra Trees Classifier performs excellently with high scores across all metrics (accuracy: 0.96, MCC: 0.9608).

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |           |        |          |         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |        |          |         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------|----------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------|----------|---------|
| <b>Naive Bayes</b><br>Confusion Matrix:<br><pre>[[17 2 0 0 0 0 0 0 0 0 0 1 0 0 0]  [ 0 11 2 0 0 0 0 0 0 0 0 0 0 0 0]  [ 0 0 20 0 0 0 0 0 0 0 0 0 0 0 0]  [19 0 0 0 0 0 0 0 0 0 0 0 1 0 0]  [ 0 0 0 20 0 0 0 0 0 0 0 0 0 0 0]  [ 0 0 0 0 18 2 0 0 0 0 0 0 0 0 0]  [ 0 0 18 0 0 0 1 0 0 1 0 0 0 0 0]  [ 0 4 0 0 0 0 2 0 0 0 0 5 1 0 0]  [ 0 0 0 0 0 0 0 20 0 0 0 0 0 0 0]  [ 0 0 0 0 0 0 1 0 0 19 0 0 0 0 0]  [ 0 0 0 0 0 0 0 0 0 0 20 0 0 0 0]  [ 0 0 0 2 0 0 0 0 0 0 0 18 0 0 0]  [ 0 0 19 0 0 0 0 0 0 0 0 0 1 0 0]  [ 0 0 19 0 0 0 0 1 0 0 0 0 0 0 0]  [ 0 1 0 0 0 0 0 0 0 0 14 0 0 0 5]]</pre> Classification Report: |           |        |          |         | <b>ExtraTreesClassifier</b><br>Confusion Matrix:<br><pre>[[18 2 0 0 0 0 0 0 0 0 0 0 0 0 0]  [ 0 17 0 0 0 0 0 0 0 0 0 0 0 0 0]  [ 0 0 20 0 0 0 0 0 0 0 0 0 0 0 0]  [ 0 0 0 20 0 0 0 0 0 0 0 0 0 0 0]  [ 0 0 0 0 19 0 0 0 0 0 1 0 0 0 0]  [ 0 0 0 0 0 20 0 0 0 0 0 0 0 0 0]  [ 0 1 0 0 0 0 18 0 1 0 0 0 0 0 0]  [ 0 2 0 0 0 0 0 18 0 0 0 0 0 0 0]  [ 0 0 0 0 0 0 0 0 20 0 0 0 0 0 0]  [ 0 0 0 0 0 0 0 0 0 20 0 0 0 0 0]  [ 0 0 0 0 0 0 0 0 0 0 20 0 0 0 0]  [ 0 0 0 0 0 0 0 0 0 0 0 20 0 0 0]  [ 0 1 0 0 0 0 0 0 0 0 0 0 19 0 0]  [ 0 0 0 0 0 0 0 0 0 0 0 0 0 20 0]  [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 20]]</pre> Classification Report: |           |        |          |         |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | precision | recall | f1-score | support |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | precision | recall | f1-score | support |
| DDoS-ACK_Fragmentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 0.47      | 0.85   | 0.61     | 20      | DDoS-ACK_Fragmentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 1.00      | 0.90   | 0.95     | 20      |
| DDoS-HTTP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 0.61      | 0.55   | 0.58     | 20      | DDoS-HTTP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 0.74      | 0.85   | 0.79     | 20      |
| DDoS-ICMP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 0.26      | 1.00   | 0.41     | 20      | DDoS-ICMP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 1.00      | 1.00   | 1.00     | 20      |
| DDoS-ICMP_Fragmentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 0.00      | 0.00   | 0.00     | 20      | DDoS-ICMP_Fragmentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 1.00      | 1.00   | 1.00     | 20      |
| DDoS-PSHACK_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 0.53      | 1.00   | 0.69     | 20      | DDoS-PSHACK_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 1.00      | 0.95   | 0.97     | 20      |
| DDoS-RSTFINFlood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 1.00      | 0.10   | 0.18     | 20      | DDoS-RSTFINFlood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 1.00      | 1.00   | 1.00     | 20      |
| DDoS-SYN_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 0.09      | 0.05   | 0.06     | 20      | DDoS-SYN_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 0.86      | 0.90   | 0.88     | 20      |
| DDoS-SlowLoris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 0.89      | 0.40   | 0.55     | 20      | DDoS-SlowLoris                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 1.00      | 0.90   | 0.95     | 20      |
| DDoS-SynonymousIP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 1.00      | 1.00   | 1.00     | 20      | DDoS-SynonymousIP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 0.95      | 1.00   | 0.98     | 20      |
| DDoS-TCP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 0.95      | 0.95   | 0.95     | 20      | DDoS-TCP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 0.95      | 1.00   | 0.98     | 20      |
| DDoS-UDP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 0.51      | 1.00   | 0.68     | 20      | DDoS-UDP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 1.00      | 1.00   | 1.00     | 20      |
| DDoS-UDP_Fragmentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 0.86      | 0.90   | 0.88     | 20      | DDoS-UDP_Fragmentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 1.00      | 1.00   | 1.00     | 20      |
| DoS-SYN_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 1.00      | 0.05   | 0.10     | 20      | DoS-SYN_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 1.00      | 0.95   | 0.97     | 20      |
| DoS-TCP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 0.00      | 0.00   | 0.00     | 20      | DoS-TCP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 1.00      | 1.00   | 1.00     | 20      |
| DoS-UDP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 1.00      | 0.25   | 0.40     | 20      | DoS-UDP_Flood                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 1.00      | 1.00   | 1.00     | 20      |
| accuracy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |        | 0.54     | 300     | accuracy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |           |        | 0.96     | 300     |
| macro avg                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 0.61      | 0.54   | 0.47     | 300     | macro avg                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 0.97      | 0.96   | 0.96     | 300     |
| weighted avg                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 0.61      | 0.54   | 0.47     | 300     | weighted avg                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 0.97      | 0.96   | 0.96     | 300     |
| Matthews Correlation Coefficient (MCC): 0.5268<br>AUC-ROC Score (macro-avg, OvR): 0.9671                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |        |          |         | Matthews Correlation Coefficient (MCC): 0.9608<br>AUC-ROC Score (macro-avg, OvR): 0.9958                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |           |        |          |         |

Figure 7: Naïve Bayes and Extra Tree Model Evaluation.

Source: Authors, (2026).

Figure 8, The ensemble VotingClassifier achieves perfect or near-perfect scores across all DDoS attack types with accuracy, recall, and F1-score close to 0.99. It shows the strongest performance among all models.

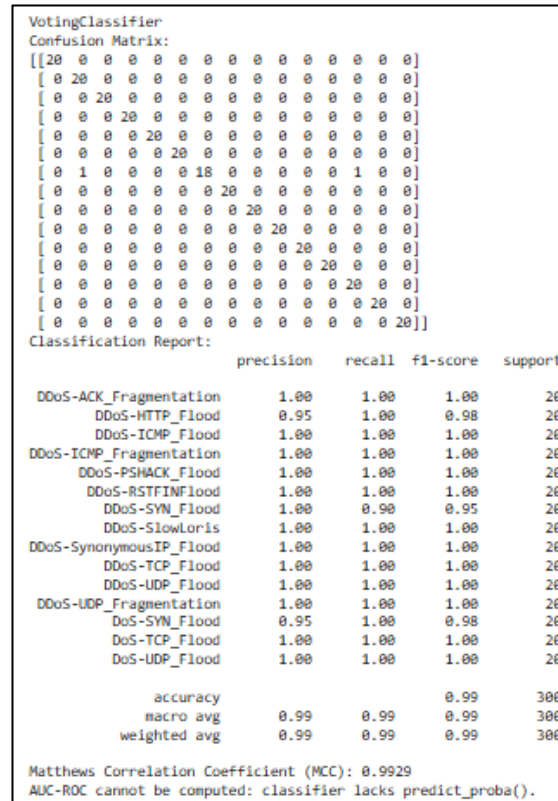


Figure 8: Proposed Ensemble Voting Model Evaluation.  
Source: Authors, (2026).

Figure 9. ROC curve for the Extra Trees Classifier indicates near-perfect classification for each DDoS class, with AUC values ranging from 0.99 to 1.00, demonstrating the model's strong discriminatory ability.

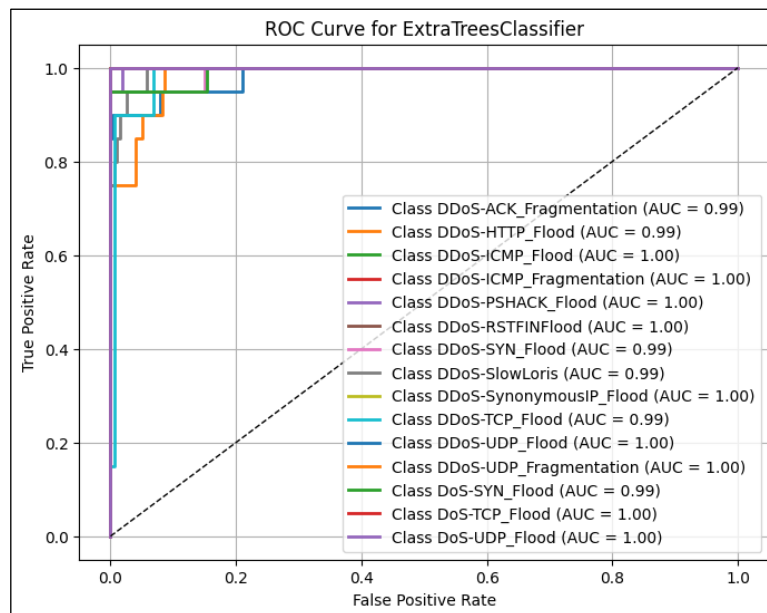


Figure 9: Proposed Ensemble Voting Model ROC Curve.  
Source: Authors, (2026).

Table 2: Proposed Ensemble Voting Model K-Fold Validation.

| Fold | Accuracy | Precision | Recall | F1-Score | MCC    |
|------|----------|-----------|--------|----------|--------|
| 1    | 0.9833   | 0.9857    | 0.9833 | 0.9836   | 0.9823 |
| 2    | 0.9900   | 0.9908    | 0.9900 | 0.9900   | 0.9893 |
| 3    | 0.9933   | 0.9937    | 0.9933 | 0.9933   | 0.9929 |
| 4    | 0.9867   | 0.9873    | 0.9867 | 0.9867   | 0.9858 |
| 5    | 0.9833   | 0.9840    | 0.9833 | 0.9834   | 0.9822 |

Source: Authors, (2026).

Table 2 presents the 5-fold cross-validation results of the proposed ensemble voting model, demonstrating consistent and robust performance across all folds. Accuracy ranges from 98.33% to 99.33%, with precision, recall, and F1-score values consistently above 98%, and MCC scores ranging between 0.9822 and 0.9929, indicating high model reliability and balanced classification capability.

Table 3: Comparative Analysis.

| Model                          | ACC(%) | P(%) | R(%) | F1-Score(%) | MCC  | AUC-ROC |
|--------------------------------|--------|------|------|-------------|------|---------|
| K-Nearest Neighbor             | 97%    | 97%  | 97%  | 97%         | 0.96 | 0.99    |
| Support Vector Machine         | 25%    | 19%  | 25%  | 16%         | 0.23 | 0.23    |
| Decision Tree                  | 98%    | 98%  | 98%  | 98%         | 0.98 | 0.99    |
| Random Forest                  | 98%    | 98%  | 98%  | 98%         | 0.98 | 0.99    |
| Navier Bayer's                 | 54%    | 61%  | 54%  | 47%         | 0.52 | 0.96    |
| Extra Tree                     | 96%    | 97%  | 96%  | 96%         | 0.96 | 0.99    |
| Proposed Ensemble Voting Model | 99%    | 99%  | 99%  | 99%         | 0.99 | 0.99    |

Source: Authors, (2026).

Table 3 provides a comparative analysis of various classifiers, where traditional models like K-Nearest Neighbor, Decision Tree, Random Forest, and Extra Trees show strong results with accuracies around 96–98%, while Support Vector Machine and Naïve Bayes significantly underperform due to limitations in handling feature space and class imbalance. The proposed ensemble voting model outperforms all other methods, achieving 99% across all key performance metrics accuracy, precision, recall, F1-score, MCC, and AUC-ROC highlighting its superiority and effectiveness in intrusion detection tasks.

## V. CONCLUSIONS

This research presents an effective ensemble intrusion detection system that can be used in detecting Distributed Denial-of-Service (DDoS) attacks in Internet of Things (IoT) systems. In a voting ensemble model, the system uses a Decision Tree, Random Forest, and Extra Trees classifier, with the best hyperparameters to optimize the detection performance. The high-quality feature sets were also guaranteed by preprocessing steps, such as KNN-based imputation, categorical variables encoding, and Recursive Feature Elimination (RFE), which boosted the accuracy of the models. The proposed model was shown to have a good classification ability across various types of attacks using the CICIoT2023 dataset comprising of 15 diverse classes of attacks with 1500 samples per attack category. The ensemble approach had better precision, recall, and F1-score values compared to base models and supports its usefulness in dynamic and complex IoT ecosystems. The following research should look into the possibility of combining adaptive learning mechanisms which would enable the system to adapt or change with new attack patterns. Lightweight deep learning models can be incorporated as a trade-off between performance and computational efficiency to deploy in edge devices in real time. Second, it is possible to incorporate real-time streaming data into the framework and implement it in a Software Defined Network (SDN) infrastructure to achieve even greater responsiveness and scalability. Federated learning methods would also deal with the issue of privacy in distributed IoT settings and provide strong security. It is important to keep benchmarking of the model and various types of datasets and environments in order to be able to extrapolate the effectiveness of the model to heterogeneous IoT applications.

## VI. AUTHOR'S CONTRIBUTION

**Conceptualization:** Piyush M. Prajapati, Priyesh P. Gandhi, Sheshang Degadwala, Keyur Brahmabhatt, Swapnil M Parikh.

**Methodology:** Piyush M. Prajapati, Priyesh P. Gandhi, Sheshang Degadwala, Keyur Brahmabhatt, Swapnil M Parikh.

**Investigation:** Piyush M. Prajapati, Priyesh P. Gandhi, Sheshang Degadwala, Keyur Brahmabhatt, Swapnil M Parikh.

**Discussion of results:** Piyush M. Prajapati, Priyesh P. Gandhi, Sheshang Degadwala, Keyur Brahmabhatt, Swapnil M Parikh.

**Writing – Original Draft:** Piyush M. Prajapati, Priyesh P. Gandhi, Sheshang Degadwala, Keyur Brahmabhatt, Swapnil M Parikh.

**Writing – Review and Editing:** Piyush M. Prajapati, Priyesh P. Gandhi, Sheshang Degadwala, Keyur Brahmabhatt, Swapnil M Parikh.

**Resources:** Piyush M. Prajapati, Priyesh P. Gandhi, Sheshang Degadwala, Keyur Brahmabhatt, Swapnil M Parikh.

**Supervision:** Piyush M. Prajapati, Priyesh P. Gandhi, Sheshang Degadwala, Keyur Brahmabhatt, Swapnil M Parikh.

**Approval of the final text:** Piyush M. Prajapati, Priyesh P. Gandhi, Sheshang Degadwala, Keyur Brahmabhatt, Swapnil M Parikh.

## VII. REFERENCES

- [1]. A. Behera, K. S. Sahoo, T. K. Mishra, and M. Bhuyan, "A combination learning framework to uncover cyber attacks in IoT networks," *Internet of Things (The Netherlands)*, vol. 28, no. July, p. 101395, 2024, doi: 10.1016/j.iot.2024.101395.
- [2]. E. Krzysztoń, I. Rojek, and D. Mikołajewski, "A Comparative Analysis of Anomaly Detection Methods in IoT Networks: An Experimental Study," *Applied Sciences (Switzerland)*, vol. 14, no. 24, 2024, doi: 10.3390/app142411545.
- [3]. A. I. Jony and A. K. B. Arnob, "A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset," *Journal of Edge Computing*, vol. 3, no. 1, pp. 28–42, 2024, doi: 10.55056/jec.648.
- [4]. S. Hizal, U. Cavusoglu, and D. Akgun, "A novel deep learning-based intrusion detection system for IoT DDoS security," *Internet of Things (Netherlands)*, vol. 28, no. April, p. 101336, 2024, doi: 10.1016/j.iot.2024.101336.
- [5]. X. Yin, W. Fang, Z. Liu, and D. Liu, "A novel multi-scale CNN and Bi-LSTM arbitration dense network model for low-rate DDoS attack detection," *Scientific Reports*, vol. 14, no. 1, pp. 1–15, 2024, doi: 10.1038/s41598-024-55814-y.

- [6]. S. Abbas et al., "An efficient deep recurrent neural network for detection of cyberattacks in realistic IoT environment," *Journal of Supercomputing*, vol. 80, no. 10, pp. 13557–13575, 2024, doi: 10.1007/s11227-024-05993-2.
- [7]. M. M. Khan and M. Alkhathami, "Anomaly detection in IoT-based healthcare: machine learning for enhanced security," *Scientific Reports*, vol. 14, no. 1, pp. 1–16, 2024, doi: 10.1038/s41598-024-56126-x.
- [8]. M. A. Elaziz, I. A. Fares, and A. O. Aseeri, "CKAN: Convolutional Kolmogorov-Arnold Networks Model for Intrusion Detection In IoT environment," *IEEE Access*, no. July, 2024, doi: 10.1109/ACCESS.2024.3462297.
- [9]. M. F. Saiyedand and I. Al-Anbagi, "Deep Ensemble Learning With Pruning for DDoS Attack Detection in IoT Networks," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 2, no. March, pp. 596–616, 2024, doi: 10.1109/tmlcn.2024.3395419.
- [10]. S. K. Dash et al., "Enhancing DDoS attack detection in IoT using PCA," *Egyptian Informatics Journal*, vol. 25, no. August 2023, p. 100450, 2024, doi: 10.1016/j.eij.2024.100450.
- [11]. M. A. Hossain and M. S. Islam, "Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity," *Measurement: Sensors*, vol. 32, no. October 2023, p. 101037, 2024, doi: 10.1016/j.measen.2024.101037.
- [12]. A. Behera, K. S. Sahoo, T. K. Mishra, A. Nayyar, and M. Bilal, "Enhancing DDoS detection in SDIoT through effective feature selection with SMOTE-ENN," *PLoS ONE*, vol. 19, no. 10, pp. 1–29, 2024, doi: 10.1371/journal.pone.0309682.
- [13]. A. M. Salama, M. A. Mohamed, and E. Abdelhalim, "Enhancing Network Security in IoT Applications through DDoS Attack Detection Using ML," *Mansoura Engineering Journal*, vol. 49, no. 3, 2024, doi: 10.58491/2735-4202.3181.
- [14]. R. Ji, N. Kumar, and D. Padha, "Hybrid Enhanced Intrusion Detection Frameworks for Cyber-Physical Systems via Optimal Features Selection," *Indian Journal Of Science And Technology*, vol. 17, no. 30, pp. 3069–3079, 2024, doi: 10.17485/ijst/v17i30.1794.
- [15]. W. Chen, H. Yang, L. Yin, and X. Luo, "Large-scale IoT attack detection scheme based on LightGBM and feature selection using an improved salp swarm algorithm," *Scientific Reports*, vol. 14, no. 1, pp. 1–25, 2024, doi: 10.1038/s41598-024-69968-2.
- [16]. S. M. Tseng, Y. Q. Wang, and Y. C. Wang, "Multi-Class Intrusion Detection Based on Transformer for IoT Networks Using CIC-IoT-2023 Dataset," *Future Internet*, vol. 16, no. 8, 2024, doi: 10.3390/fi16080284.
- [17]. F. L. Becerra-Suarez, V. A. Tuesta-Monteza, H. I. Mejia-Cabrera, and J. Arcila-Diaz, "Performance Evaluation of Deep Learning Models for Classifying Cybersecurity Attacks in IoT Networks," *Informatics*, vol. 11, no. 2, 2024, doi: 10.3390/informatics11020032.
- [18]. A. I. Jony and A. K. B. Arnob, "Securing the Internet of Things: Evaluating Machine Learning Algorithms for Detecting IoT Cyberattacks Using CIC-IoT2023 Dataset," *International Journal of Information Technology and Computer Science*, vol. 16, no. 4, pp. 56–65, 2024, doi: 10.5815/ijitcs.2024.04.04.
- [19]. H. Q. Gheni and W. L. Al-Yaseen, "Two-step data clustering for improved intrusion detection system using CICIoT2023 dataset," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 9, no. March, p. 100673, 2024, doi: 10.1016/j.prime.2024.100673.
- [20]. J. Chen, J. Xiao, and J. Xu, "VGGIncepNet: Enhancing Network Intrusion Detection and Network Security through Non-Image-to-Image Conversion and Deep Learning," *Electronics*, vol. 13, no. 18, p. 3639, Sep. 2024, doi: 10.3390/electronics13183639.
- [21]. R. Abu Bakar, X. Huang, M. S. Javed, S. Hussain, and M. F. Majeed, "An Intelligent Agent-Based Detection System for DDoS Attacks Using Automatic Feature Extraction and Selection," *Sensors*, vol. 23, no. 6, 2023, doi: 10.3390/s23063333.
- [22]. N. T. Cam and N. G. Trung, "An Intelligent Approach to Improving the Performance of Threat Detection in IoT," *IEEE Access*, vol. 11, no. April, pp. 44319–44334, 2023, doi: 10.1109/ACCESS.2023.3273160.
- [23]. E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, 2023, doi: 10.3390/s23135941.
- [24]. J. Zhao, Y. Liu, Q. Zhang, and X. Zheng, "CNN-AttBiLSTM Mechanism: A DDoS Attack Detection Method Based on Attention Mechanism and CNN-BiLSTM," *IEEE Access*, vol. 11, no. November, pp. 136308–136317, 2023, doi: 10.1109/ACCESS.2023.3334916.
- [25]. A. A. Alahmadi et al., "DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions," *Electronics (Switzerland)*, vol. 12, no. 14, pp. 1–24, 2023, doi: 10.3390/electronics12143103.
- [26]. A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. Ben Dhaou, "Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model," *IEEE Access*, vol. 11, no. August, pp. 119862–119875, 2023, doi: 10.1109/ACCESS.2023.3327620.
- [27]. S. Farhat, M. Abdelkader, A. Meddeb-Makhlouf, and F. Zarai, "Evaluation of DoS/DDoS Attack Detection with ML Techniques on CIC-IDS2017 Dataset," *International Conference on Information Systems Security and Privacy*, no. Icissp, pp. 287–295, 2023, doi: 10.5220/0011605700003405.
- [28]. B. Xu, L. Sun, X. Mao, R. Ding, and C. Liu, "IoT Intrusion Detection System Based on Machine Learning," *Electronics (Switzerland)*, vol. 12, no. 20, 2023, doi: 10.3390/electronics12204289.
- [29]. P. Prashanthi, M. M. Reddy, and A. Lavanya, "Machine Learning for IoT Security: Random Forest Model for DDoS Attack Detection," *Turkish Journal of Computer and Mathematics Education*, vol. 14, no. 03, pp. 1029–1038, 2023.
- [30]. S. Y. Fahrezi, A. Nugraha, A. Luthfiarta, and N. Dwi, "Optimizing Performance of AdaBoost Algorithm through Undersampling and Hyperparameter Tuning on CICIoT 2023 Dataset," pp. 175–184, 2023.
- [31]. İ. Avcı and M. Koca, "Predicting DDoS Attacks Using Machine Learning Algorithms in Building Management Systems," *Electronics (Switzerland)*, vol. 12, no. 19, pp. 1–13, 2023, doi: 10.3390/electronics12194142.