# *Machine Learning Framework for DDoS Detection in IoT*

R. Pradeep[#1], J. Jegadesh[#2], Mr. S. Manoj[*3]
[#1, #2]Student, Department of Computer Science with Cognitive Systems,

Sri Ramakrishna College of Arts and Science,

Coimbatore, Tamil nadu, India.

[*3]Assistant Professor, Department of Computer Science with Cognitive Systems,

Sri Ramakrishna College of Arts and Science,

Coimbatore, Tamil nadu, India.

[1]pradeep2005ravi@gmail.com, [2]jegadesh145@gmail.com , [3]Manoj@srcas.srcas.ac.in

***ABSTRACT: With the rapid advancement of technology, the use of Internet of Things (IoT) devices continues to increase in daily life. These devices provide convenience and efficiency for ordinary users, even without advanced technical knowledge. IoT technology is commonly used in home security systems, smart refrigerators, smart televisions, and many other connected appliances. While these internet-enabled devices offer several advantages, they also create serious security concerns. Cyber attackers constantly search for new ways to exploit weaknesses in digital systems, and IoT devices are particularly vulnerable due to their large numbers and limited protection. This makes them ideal targets for large-scale cyberattacks, including Distributed Denial of Service (DDoS) attacks, where compromised devices are used Bots to overwhelm networks and services. services, ultimately disrupting their availability. In order to determine whether an attack has taken place within a network, a dependable and efficient detection mechanism is required. One of the most widely used approaches for this purpose is artificial intelligence, specifically Machine Learning (ML) and Deep Learning (DL), which assist in identifying and analysing cyber threats. ML models utilize structured data and algorithms to recognize patterns, make predictions, and detect abnormal behaviour within network traffic. The primary objective of this paper is to review selected research studies and publications related to DDoS detection in IoT-based networks using machine learning techniques. This work provides a comprehensive reference base for researchers seeking to define or expand their studies in this field.***

***Keywords: DDoS Attacks, Artificial Intelligence in Cybersecurity, Artificial Neural Networks (ANN), AdaBoost Algorithm, Support Vector Classifier (SVC), Random Forest Classifier***

## 1. INTRODUCTION

The Internet of Things (IoT) is a revolutionary technology that has become increasingly beneficial in recent years. In modern society, IoT plays a vital role in everyday activities. It is widely applied in numerous areas such as smart homes, smart cities, smart grids, autonomous transportation systems, healthcare facilities, industrial plants, and many more. The primary objective of IoT technology is to make human life easier and more intelligent by integrating physical systems with digital capabilities [1]. IoT-enabled devices are able to collect data and transmit it at any time and from any location through internet connectivity. This information is then processed and analyzed within a centralized platform, where it becomes accessible to other connected devices. Reports indicate that approximately 10.07 billion IoT devices were connected to the Internet in 2021, and this number is expected to increase to nearly 24.1 billion by the year 2030 [2]. As a result, an enormous volume of information is exchanged between these interconnected devices, making it extremely important to ensure the secure flow of data and protect it from potential cyber threats [1]. Security risks associated with IoT devices and their networks can be classified into six main categories: Denial of Service (DoS), false data injection, unauthorized monitoring, identity spoofing, hardware tampering, and message interruption [2]. Among these threats, DoS and… Distributed DoS (DDoS) attacks, which are the more advanced version of Dos and they are more complicated to detect or mitigate, are the most dangerous and destructive method to take over IoT. In this type of attack, the attacker's purpose is to …overburden the target service by sending massive amounts of data traffic, making it incapable of handling the load. As a result, legitimate users and connected devices experience interruptions and are unable to access the required services due to the generated disruption [3]. There are several forms of DDoS attacks, each with unique features and attack behaviors. The most common types include TCP Flood, SYN Flood, UDP Flood, ICMP Flood, HTTP Flood, Ping of Death, NTP Amplification, DNS Flood, and Zero-Day DDoS attacks.

The structure of the proposed study is illustrated in Figure 1, and the primary contributions of this work are summarized as follow

- Introducing a new approach for feature selection and dimensionality reduction using the CICDDoS2019 dataset.
- Presenting a detection model capable of classifying DDoS attacks with higher accuracy and greater speed when compared to existing state-of-the-art models.
- Identifying the most suitable machine learning technique for DoS/DDoS detection based on performance and efficiency analysis within the model.

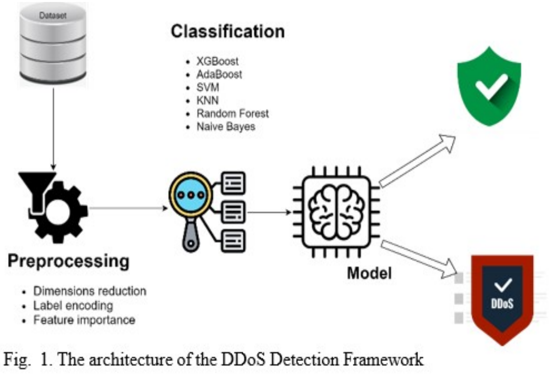

**Fig. 1:** The architecture of the DDos Detection Framework

## 2. BACKGROUND AND RELATED WORKS

### 2.1 DoS and DDoS Attacks

Traditional ML models have been widely attempted to detect network intrusions. One of the earliest study found in literature that employed Bayesian algorithm as classifier, which has advantages of simplicity, easy to implement, and applicability to binary and multi-class classification [5]. K-nearest neighbor algorithm was also applied for detecting DDoS attack in wireless sensor network, but it is difficult to determine the optimal K value for large datasets. Ambusaidi et al. [6] employed SVM model and developed a mutual An information-driven feature selection method is used to enhance the performance of the detection system. However, as the size and dimensionality of the dataset continue to increase, the overall accuracy of the classifier may decline. Doshi et a. [7] evaluated five different machine learning–based detection techniques on a dataset consisting of both normal and DDoS attack traffic obtained from an experimental IoT-based environment. Since conventional machine learning approaches rely heavily on manual feature engineering, identifying correlations among features often becomes a complex and time-consuming task. As a result, applying traditional ML algorithms for real-time attack detection is generally impractical. The most common types of DoS/DDoS attacks are described below. TCP Flood: In this type of attack, the attacker exploits a part of TCP's three-way handshake to consume target resources and render it unresponsive [8].

- **TCP Flood:** In this attack, the adversary takes advantage of the TCP three-way handshake process to exhaust system resources and make the target system unresponsive
- . **SYN Flood:** In a SYN Flood attack, the attacker continuously sends SYN requests to the target’s ports using spoofed IP addresses, leaving the connection incomplete and consuming resources.
- **ICMP Flood:** Also known as a attack uses Internet Control Message Protocol (ICMP) packets to bombard the target system, attempting to exhaust its resources and make it unreachable to legitimate network traffic.Ping Flood, this
- **HTTP Flood:** In this type of attack, the adversary overloads the targeted web server by sending a large number of HTTP GET or POST requests.
- **Ping of Death:** In this attack, the attacker sends malformed or oversized ping packets to disrupt the normal functioning of the target system, potentially causing it to freeze or crash..
- **NTP Amplification:** This DDoS attack exploits publicly accessible Network Time Protocol (NTP) servers to generate and direct an amplified volume of UDP traffic toward the target.
- **DNS Flood:** A Domain Name System (DNS) flood is a form of DDoS attack in which the attacker overwhelms one or more DNS servers of a specific domain, thereby preventing the proper resolution of domain records.

## 2.2 Machine Learning Classifiers for DDoS Detection

A variety of techniques have been developed for detecting DDoS attacks. However, many traditional approaches are becoming less effective due to the increasing complexity and sophistication of modern attack methods. As a As a result, the application of data mining and machine learning techniques has become one of the most effective and reliable methods for detecting and mitigating such threats within network environments. Researchers first utilize machine learning algorithms to train a detection model and subsequently evaluate its performance in order to determine whether it is suitable for identifying DDoS attacks. A list of widely used machine learning algorithms for DDoS detection is presented in the following paragraph.

- **Decision Tree (DT)**

The Decision Tree is a supervised learning algorithm structured in a hierarchical manner, where internal nodes represent dataset features, branches correspond to decision rules, and leaf nodes indicate the final outcome. This structure is illustrated in Figure 2. The classification process begins at the root node and continues down the tree until a leaf node is reached. Decision Trees are capable of handling inconsistent data, as instances within the same class share similar conditional probabilities, and they require less data preprocessing compared to other approaches. Furthermore, the logical structure of DT is easy to interpret and closely resembles human reasoning in the decision-making process [9].

- **Random Forest (RF)**

RF is an ensemble-based supervised learning technique that merges multiple classifiers to tackle a challenging problem and improves the performance of models. RF takes less training time and maintains a high prediction accuracy even for large datasets and large missing proportions of the data [10]. Figure 4 illustrates the breakdown of RF that contains multiple decision trees for each subset of a dataset. To improve its predictive accuracy, RF aggregates the prediction outcomes of each tree to predict the outcome based on the most votes. Furthermore, to predict an accurate result, there must be some actual values in the dataset's feature variable, as well as a greater number of trees.

- **K-Nearest Neighbors (KNN)**

K-Nearest Neighbors is a simple and commonly used supervised machine learning algorithm. Unlike many other algorithms, KNN does not directly learn a model from the training data. Instead, it stores the dataset and determines the class of a new data point by comparing its similarity to existing instances, assigning it to the category of its closest neighbors. KNN is relatively robust to noisy data. However, it involves a high computational cost, as predictions are made based on distance calculations using advanced distance metrics [11].

- **XGBoost (eXtreme Gradient Boosting)**

XGBoost is an advanced implementation of gradient-boosted decision trees that is based on sequential learning. The term "gradient" refers to the optimization of the objective (loss) function, allowing the algorithm to achieve high performance while efficiently utilizing computational resources.

- **Artificial Neural Network (ANN)**

Artificial Neural Networks (ANNs), also known as neural networks (NNs), are designed to emulate the structure and functioning of biological neural systems, replicating aspects of the human brain to enable computers to recognize patterns and make decisions in a human-like manner. As shown in Figure 5, ANNs generally consist of three layers: an input layer, one or more hidden layers, and an output layer. The hidden layers perform essential computations to identify underlying patterns and extract important features from the input data. ANNs offer several advantages, including parallel processing capabilities, robustness to incomplete information, and fault tolerance. However, they are heavily dependent on hardware resources and require careful design and proper configuration to ensure optimal performance [13].

- **Support Vector Machine (SVM)**

Support Vector Machine (SVM) is a supervised learning algorithm commonly used for classification tasks. The SVM algorithm aims to identify an optimal decision boundary, known as a hyperplane, that separates two classes within an N-dimensional feature space (where N represents the number of features). SVMs are memory-efficient because they rely only on a subset of critical data points, called support vectors, which define the decision function. As illustrated in Figure 6, SVMs can be categorized into two types: linear SVMs, which separate data using a straight hyperplane, and non-linear SVMs, which employ kernel functions to handle complex, non-linearly separable data [14].

**(A) Linear SVM:** This type of SVM is used for datasets that are linearly separable, meaning that the data can be divided into two distinct classes using a single straight line (or hyperplane in higher dimensions). When the classification can be achieved with such a linear boundary, the algorithm is referred to as a Linear SVM..

**(B) Non-linear SVM:** This type of SVM is used for datasets that are not linearly separable. In cases where the data cannot be divided into classes using a single straight line, it is considered non-linear data, and the classifier used to handle such datasets is referred to as a Non-linear SVM..

- **Adaptive Boosting (AdaBoost)**

AdaBoost is a supervised learning technique that employs an iterative ensemble-based approach. It combines multiple weak classifiers, each with relatively low accuracy, to create a single strong classifier with high predictive performance. [15].

## 3. METHODOLOGY

### 3.1 Proposed Study

Initially, we reviewed the existing literature to identify the most widely used machine learning algorithms for detecting DoS and DDoS attacks. Based on this review, we proposed a model to evaluate and compare these algorithms in terms of both accuracy and processing speed. The study utilized the most recent dataset available, the "CICDDoS2019," as input for the experiments. After performing data preprocessing, we applied the selected machine learning algorithms and recorded the resulting performance metrics. Finally, we identified the key features of the "CICDDoS2019" dataset that have the greatest influence on DDoS attack prediction, providing new insights into feature importance for this dataset.

### 3.2 Dataset

In this study, we used the "CICDDoS2019" Dataset, which is the latest available Dataset in the context of DDoS attacks and has improved most of the shortcomings of the previous Dataset. This Dataset contains both Reflection-based and Exploitation-based DDoS attacks using TCP/UDP-based protocols at the application layer. The main benefit of using this Dataset is that it has proposed a new taxonomy, including new attack types. As a result, there are different categories of DDoS attack types which are labelled as 'PortMap,' 'NetBIOS,' 'LDAP,' 'MSSQL,' 'UDP,' 'UDP-Lag,' 'NTP,' 'DNS,' 'SNMP,' 'SSDP,' 'WebDDoS' and 'TFTP' and normal traffic which is labeled as 'BENIGN.' Network traffic data with their respective labels and traffic features which are extracted by CICFlowMeter-V3, are saved in a CSV file and available for free.

### 3.3 Machine Learning Algorithms

We reviewed existing literature to identify the machine learning algorithms most frequently applied for DDoS attack detection. Among these, Naïve Bayes, SVM, KNN, Random Forest, XGBoost, and AdaBoost were the most commonly used and demonstrated strong performance in previous DDoS detection studies. These algorithms were incorporated into our experimental model, and their performance was systematically evaluated to determine the most effective approaches. The following sections provide a detailed description of the evaluation metrics used and present the results of our experiments.

### 3.4 Evaluation Metrics

To compare the performance of the tested algorithms, we utilized Accuracy Score, F1-Score, ROC Curve, and Training Time. Additionally, to identify the most influential features, we employed Feature Importance analysis.

- **Accuracy Score**:This metric calculates the proportion of correctly predicted labels out of the total number of labels. However, because the dataset may be imbalanced, relying exclusively on Accuracy Score may not provide a complete assessment of model performance. The formula for Accuracy Score is given below:

ISSN: 3107-6513

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

- **F1-Score:** The F1-Score represents the harmonic mean of Precision and Recall. It is a complementary metric to Accuracy, particularly useful for imbalanced datasets, as it takes into account both False Positives and False Negatives. The formulas for Precision, Recall, and F1-Score are as follows::

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

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

$$\text{F1 Score} = \frac{2 * \text{Precision} * \text{Recall}}{(\text{precision} + \text{recall})}$$

- **ROC Curve (Receiver Operating Characteristic Curve):** This metric assesses the performance of the model by taking into account both the False Positive Rate and the False Negative Rate.
- **Training Time:** This metric measures the computational efficiency of the model, indicating how quickly it can learn from the training
- **Feature Importance:** This metric evaluates the impact of each feature on the predicted output by estimating the correlation between individual features and the target label.

## 4. RESULTS AND ANALYSIS

This section presents the results of the comparative evaluation of the selected machine learning algorithms using our experimental model and the CICDDoS2019 dataset, followed by an analysis of these results. As shown in Table I and Figure 2, SVM and Random Forest achieved the highest performance, with an accuracy of 100% and an F1-Score of 1.0. Additionally, SVM demonstrated slightly faster training times compared to Decision Tree and AdaBoost. XGBoost, KNN, and ANN also achieved good performance, with accuracies of 98.5%, 98.75%, and 99.0%, and F1-Scores of 0.9850, 0.9875, and 0.9306, respectively.

Naïve Bayes performed well in terms of efficiency and effectiveness. The main reason that ANN and Naïve Bayes didn't have acceptable performance was that this algorithm is based on Bayes Theorem, which assumes the feature as being independent and, in our Dataset, features were not wholly independent.

**Table 1: Evaluation Results**

| Algorithms | Evaluation Method | |
|---|---|---|
| | **Accuracy** | **F1-Score** |
| Decision Tree | 98.50% | 0.985 |
| Random Forest | 100% | 1 |
| K-Nearest Neighbors | 98.75% | 0.9875 |
| XGBoost | 99% | 0.9363 |
| Artificial Neural Network | 96.21% | 0.7098 |
| Support Vector Machine | 100% | 1 |
| Naïve Bayes | 95.67% | 0.7134 |

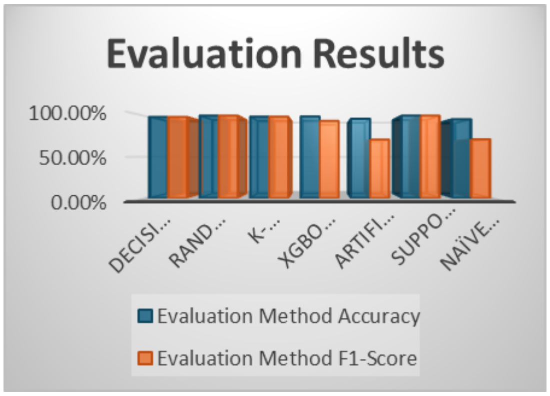

**Fig.2:** DDoS Detection Results

## 5. CONCLUSION

This study proposed a DDoS detection framework and evaluated several widely used machine learning algorithms, including ANN, Naïve Bayes, SVM, AdaBoost, XGBoost, KNN, and Random Forest, for the binary classification of CICDDoS2019 network traffic into `Benign` and `Attack` categories. All tested algorithms, with the exception of Naïve Bayes, effectively distinguished between benign and attack traffic. Among them, Random Forest and SVM achieved outstanding performance, both attaining an Accuracy Score of 100% and an F1-Score of 1.0. Moreover, SVM demonstrated slightly faster training and detection times compared to AdaBoost. The study also identified the top ten most influential features within the dataset that have the greatest impact on accurate DDoS attack prediction, providing valuable insights for future research and model optimization. This represents a significant advancement in…work since selecting the most pivotal features and removing nonsignificant ones would help the detection model to be trained better and have higher accuracy and speed and also would prevent the overfitting of the model.

ISSN: **3107-6513**

# REFERENCES:

[1] A. Aljuhani, "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments," IEEE Access, vol. 9, pp. 42236-42264, 2021.

[2] N. Jyoti and S. Behal, "A Meta-evaluation of Machine Learning Techniques for Detection of DDoS Attacks."

[3] S. Mishra, C. Mahanty, S. Dash, and B. K. Mishra, "Implementation of bfs-nb hybrid model in intrusion detection system," in Recent Developments in Machine Learning and Data Analytics. Springer, 2019.

[4] D. Papamartzivanos, F. G. Marmol, and G. Kambourakis, "Dendron: ´ Genetic trees driven rule induction for network intrusion detection systems," Future Generation Computer Systems, vol. 79, pp. 558–574, 2018.

[5] T. Kawamura, M. Fukushi, Y. Hirano, Y. Fujita and Y. Hamamoto, "An NTP-based detection module for DDoS attacks on IoT", 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), 2017

[6] W. N. H. Ibrahim et al., "Multilayer framework for botnet detection using machine learning algorithms," IEEE Access, vol. 9, pp. 48753- 48768, 2021.

[7] Amrish, R.; Bavapriyan, K.; Gopinaath, V.; Jawahar, A.; Vinoth, C.K. DDoS Detection using Machine Learning Techniques. J. IoT Soc. Mob. Anal. Cloud 2022, 4, 24–32.

[8] A. Rezaei, "Using Ensemble Learning Technique for Detecting Botnet on IoT," SN Computer Science, vol. 2, no. 3, pp. 1-14, 2021.

[9] Alkasassbeh, M.; Al-Naymat, G.; Hassanat, A.B.; Almseidin, M. Detecting Distributed Denial of Service Attacks Using Data Mining Techniques. Int. J. Adv. Comput. Sci. Appl. (IJACSA) 2016.

[10] S. Wankhede and D. Kshirsagar, "DoS attack detection using machine learning and neural network," in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018: IEE.