STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **13**, January 2025, pp 409–433.
Published online in International Academic Press (www.IAPress.org)

A Prevalent Model-based on Machine Learning for Identifying DRDoS Attacks through Features Optimization Technique

Pabon Shaha[1], Md. Saikat Islam Khan[1], Anichur Rahman[1,2,*], Mohammad Minoar Hossain[1], Golam Mahamood Mammun[1], Mostofa Kamal Nasir[1]

[1]*Department of CSE, Mawlana Bhashani Science and Technology Department, Tangail-1902, Dhaka, Bangladesh*
[2]*Department of CSE, National Institute of Textile Engineering and Research (NITER), Constituent Institute of the University of Dhaka, Savar, Dhaka-1350, Bangladesh*

Abstract Growing apprehension among internet users regarding cyber-security threats, particularly Distributed Reflective Denial of Service (DRDoS) attacks, underscores a pressing issue. Despite considerable research endeavors, the efficacy of detecting DRDoS attacks remains unsatisfactory. This deficiency calls for the development of pioneering solutions to enhance detection capabilities and fortify cyber defenses against this sophisticated subtype of Distributed Denial of Service (DDoS) attacks. Our study addresses this challenge by utilizing four distinct machine learning algorithms: SVM, DT, RF, and LR, supplemented by PCA. Leveraging the "CIC Bell DNS 2021" dataset, our experiments produce compelling results. Specifically, both DT and RF algorithms exhibit exceptional performance with 100% accuracy and perfect F1 scores. This remarkable performance holds true with or without PCA-based feature reduction, except for dataset 4. Consequently, our research highlights the potential of machine learning in detecting and mitigating DRDoS attacks, offering valuable insights for bolstering cybersecurity measures against evolving threats.

Keywords DRDoS Attack, Attack Analysis, Cyber Security Attack, PCA, Machine Learning, DNS, UDP, NetBIOS, NTP

AMS 2010 subject classifications 97P40, 97P60, 97R40

DOI: 10.19139/soic-2310-5070-2042

1. Introduction

In this era, cyber-attacks have emerged as a widespread concern for a substantial portion of internet users. Among the array of cyber threats, Denial of Service (DoS), Distributed Denial of Service (DDoS), and the newer Distributed Reflection Denial of Service (DRDoS) attacks hold particular prominence. The DRDoS attack, a variant of DDoS, has gained increasing attention due to its distinct characteristics and assault methodology, posing formidable challenges for mitigation. These attacks exploit reflection techniques to magnify their impact, complicating efforts to counteract them effectively. Consequently, defending against DRDoS attacks necessitates the implementation of advanced strategies and technologies to mitigate their disruptive potential [1]. In a DRDoS attack, the perpetrator utilizes a falsified source IP address belonging to the victim to instigate outdated requests toward numerous servers. Subsequently, these servers respond by dispatching messages to the targeted PC. Importantly, these responses often surpass the size of the victim's original requests, a phenomenon recognized as amplification attacks. This method furnishes two key advantages to the attacker: anonymity and amplification. By leveraging the victim's IP address, the attacker obfuscates the victim's true location, complicating efforts to

[*]Correspondence to: Anichur Rahman (Email: anis_cse@niter.edu.bd). Department of CSE, National Institute of Textile Engineering and Research (NITER), Constituent Institute of the University of Dhaka, Savar, Dhaka-1350, Bangladesh.

ISSN 2310-5070 (online) ISSN 2311-004X (print)

trace the origin of the assault. Moreover, amplification enables the attacker to dramatically escalate the volume of traffic directed at the victim, thereby intensifying the impact of the attack [2].

The amplification factor of Distributed Denial of Service (DDoS) attacks can cause an exponential increase in the amount of traffic directed towards the victim, making them especially harmful. This makes managing and mitigating it challenging, particularly for businesses without strong cybersecurity safeguards. If the attack serves as a distraction from other malicious activities, the repercussions may include downtime, lost revenue, reputational harm, and possible breaches. Furthermore, since the legitimate servers are frequently ignorant of their involvement in the attack, using them to amplify attacks further complicates the process of tracking down and stopping the source[3]. In the landscape of DDoS attacks, the DRDoS tactic has been utilized by 39 percent of attackers, marking its prominence in the realm of cyber assaults. Over the span of more than a decade, DRDoS attacks have maintained their status as a dependable and potent form of DDoS attack. Despite efforts to mitigate them, these attacks seem resilient and difficult to thwart. Their enduring effectiveness and increasing popularity suggest that they remain a formidable threat in the cybersecurity domain, posing ongoing challenges to defenders [4, 5]. To execute devastating attacks aimed at inundating networks, incapacitating websites, and disrupting corporate targets, DRDoS attackers have resorted to exploiting various protocols on Internet-connected devices and servers. These protocols, including DNS (Domain Name System), NTP (Network Time Protocol), SNMP (Simple Network Management Protocol), and SSDP (Simple Service Discovery Protocol), among others, have been manipulated by attackers to amplify their assault capabilities significantly. By exploiting vulnerabilities in these widely used protocols, DRDoS attackers can amplify the volume of traffic directed towards their targets, intensifying the impact of their attacks and maximizing the disruption caused to their victims [6].

The Domain Name Service (DNS) plays a crucial role in the functioning of the internet by translating numerical IP addresses into domain names, facilitating user-friendly access to websites. When users input web addresses into their browsers, DNS resolvers resolve these addresses by querying DNS servers, which then respond with the corresponding IP addresses. However, in a DRDoS DNS attack scenario, attackers manipulate this process by first spoofing the user's IP address. Subsequently, they initiate DNS queries to DNS servers using the spoofed IP address. As a result, the legitimate user receives unwanted responses from the DNS server, leading to a flood of traffic directed towards the victim, thereby disrupting their online services [7]. NetBIOS, originally developed by IBM and later adopted by Microsoft, serves as a network system facilitating various network services and enabling communication between computers on a LAN network. It operates by establishing connections between computers and allowing software applications to interact. Communication within this system relies on specific protocols known as NetBIOS frames for transmitting data between network devices. NetBIOS, which stands for Network Basic Input/Output System, is typically used over TCP/IP but functions at the Session layer (Layer 5) of the OSI model. [8]. The 16-character NetBIOS names are used by software applications as identifiers. The initiation and termination of NetBIOS Sessions are controlled by commands sent by clients. In the context of cyber-attacks, attackers initiate the assault by sending NetBIOS queries or commands to the victim's devices. Through spoofing techniques, attackers manipulate the victim devices to appear legitimate and induce them to send a high volume of requests to target devices, thereby disrupting their functionality [9, 10].

In a DRDoS NTP attack, the Network Time Protocol (NTP) serves as a conduit for attackers to synchronize time across Internet servers. The attack begins with the attacker identifying the IP address of the victim machine. Subsequently, the attacker inundates the NTP server with a substantial volume of UDP packets. These packets are designed to support the MONLIST command, a feature of the NTP protocol that provides a list of the most recent IP addresses querying the NTP server. Upon receiving the MONLIST command, the NTP server compiles the list and forwards it to the source IP address, which has been spoofed by the attacker. This manipulation of the NTP server's functionality results in a flood of responses being directed towards the victim, overwhelming its resources and causing disruption to its operations [11]. The User Datagram Protocol (UDP) operates as a connectionless protocol, eliminating the need for a host-to-host connection. Working at the transport layer, UDP transmits Datagrams across the network. Unlike some other protocols, UDP does not inspect source IP addresses, making it an attractive choice for attackers. Exploiting this characteristic, attackers forge IP packet Datagrams, allowing them to include a falsified source IP address. In a typical scenario, the attacker duplicates the victim's IP address across a vast number of UDP packets. Consequently, when the target machine responds, it does so to the victim machine, unwittingly facilitating the attacker's malicious intentions [12, 13].

This paper explores the effectiveness of various machine learning algorithms, including (SVM), (DT),(RT), and (LR), in detecting DRDoS attacks. It examines both scenarios: detecting these attacks without feature reduction and with feature reduction using PCA. By employing these algorithms, the study aims to develop robust detection mechanisms to safeguard internet users against DRDoS attacks. Through comparative analysis, the paper evaluates the performance of each algorithm in accurately identifying and mitigating these malicious activities, thereby contributing to the enhancement of cybersecurity measures in the digital landscape. The key contributions of this paper include:

- We propose a machine learning-based model for identifying Distributed Reflection Denial of Service (DRDoS) attacks using a technique for optimizing features.
- Four machine learning algorithms, namely SVM, LR, RF, and DT, were employed for detecting DRDoS attacks.
- Initially, these four algorithms apply without considering the feature reduction technique. Then, the feature reduction technique was taken into account when applying these four algorithms.
- Additionally, We assess the performance of the proposed algorithm using recall, F1-score, accuracy, and precision efficiently.

The paper proceeds with Section 2, providing an in-depth exploration of related research on DRDoS attacks. Section 3 outlines the methodology utilized for DRDoS attack detection. In Section 4, experimental results are showcased, supported by pertinent tables for clarity and analysis. Section 5 encapsulates conclusive findings and insights drawn from the study. Finally, Section 6 includes references for further exploration and validation of the presented findings.

2. Literature Reviews

The author's study [14] involved a thorough analysis of administered reflection denial of service attacks, with a focus on distinguishing between DRDoS attacks that are based on TCP and UDP. Through rigorous analysis, the author elucidated and described the distinctions in the methodologies and impacts inherent to these two variants of attacks. This examination provided valuable insights into the unique characteristics and strategies employed by TCP and UDP-based DRDoS attacks, shedding light on their respective strengths and weaknesses. Overall, the study contributed to a deeper understanding of the nuanced dynamics within the realm of DRDoS attacks, informing more targeted and effective mitigation strategies. In their paper [1], the authors introduced a novel proactive feature selection model aimed at detecting DRDoS assaults, leveraging improved optimization techniques. Their model is based on proactive feature selection (PFS) and integrated machine learning methods, including KNN, RF, and SVM, for predicting DRDoS assaults. Through this approach, they achieved an accuracy rate of 89.59 percent, demonstrating the efficacy of their methodology in identifying such cyber threats. An enhanced method for validating source IP addresses is suggested in the paper [15] to stop DDoS attacks in 5G networks. This strategy involves enhancing the User Plane Function (UPF) within the 5G core network. The study demonstrates that increasing the Packet Inspection Rate (PIR) through this method effectively deters DRDoS attacks.

According to Xu et al. [16], the authors presented a DRDoS Detection based on Deep Forest and Defense Method in order to integrate Deep Forest, IoT, Big Data, and other techniques within a Big Data environment. By achieving a greater detection rate and a lower false alarm rate in comparison to current techniques, their research proved the effectiveness of their technology for DRDoS defense and detection. This comprehensive approach underscores the potential of leveraging diverse techniques to enhance cybersecurity against DRDoS attacks. In order to prevent DRDoS attacks, the authors of the paper [17] proposed a cloud-based defense that uses cloud infrastructure. Their strategy makes use of cloud resources to efficiently lessen the effects of DRDoS attacks. In the paper [18], The authors suggested "Visualization of Actionable Knowledge to Mitigate DRDoS Attacks", a technology and strategy that gives Internet service providers (ISPs) ways to effectively defend against such attacks.A machine learning-based approach for detecting and evaluating DDoS attacks was presented by the author of the paper [19]. This method computed metrics such as the overall success rate, detection rate, and false positive rate. In their paper [20], To counteract DDoS attacks, the authors presented the Protocol Independent Detection and Classification. Effectively detecting and classifying DDoS attacks, this system uses machine learning and data mining algorithms, like the C4.5 classification algorithm. At 99% true positive and less than 1% false positive, their method worked wonderfully. The response packet confirmation system that the authors of the paper [21] developed is a model for DRDoS attack detection. This system presents a straightforward and cost-effective approach to detection within the research context.

In their study [22], the authors introduced a method for detecting Reflection Amplification (RA) attacks targeting the UDP Protocol, utilizing classification and analysis techniques specific to RA attacks. Additionally, they employed a detection algorithm and assessed its reliability in identifying and mitigating such attacks. The authors of the paper [23] introduced a mechanism titled “DRDoS attacks within Mobile Ad Hoc Networks (MANETs) are addressed by CARD (Continuous and Random Dropping) based DRDoS Attack Detection and Prevention Techniques in MANET”. Their proposal entails leveraging CARD technology for detecting and preventing such attacks, offering a specialized solution tailored to the challenges of MANET environments. A model for DRDoS attack detection was created by the authors of the paper [21], using a response packet confirmation system. Their approach achieved a high true positive rate of 99 percent and a low false positive rate of 1 percent, while also demonstrating a 98 percent accuracy in categorizing attacks.

In order to counter advanced SIP-DRDoS attacks that take advantage of SIP feature vulnerabilities, the study [24] presents a novel defense mechanism. The defense mechanism comprises statistics, inspection, and action modules to mitigate such attacks effectively. Through experimentation in a simulated VoIP/SIP environment, the proposed defense mechanism successfully detects and mitigates SIP flood attacks, significantly reducing CPU usage on the SIP server. Overall, this approach represents a substantial improvement over existing defense mechanisms, offering effective protection against SIP-based DRDoS attacks in VoIP systems. WSN play a crucial role in data collection and transmission, with small sensor nodes being the primary components vulnerable to intrusion due to their disorganized layout. The increasing digitization of human activities, accelerated by the COVID-19 pandemic, has led to a surge in cyberattacks like DDoS and DRDoS, posing significant threats to Internet-based systems. Because of the shortcomings of existing detection techniques and the growing danger associated with the proliferation of IoT devices, this study offers a thorough overview of the related work for DDoS and DRDoS attack detection on deep learning .[25, 26, 27, 28, 29].

In summary, a considerable body of research has focused on introducing various models for detecting cyber attacks, including DoS, DDoS, and DRDoS. Yet, these models often reveal limitations within their proposed frameworks. In response, our research aims to devise a novel approach precisely designed to detect DRDoS attacks while mitigating the deficiencies observed in prior models. By tackling these limitations head-on, our proposed model seeks to bolster the effectiveness and precision of cyber attack detection mechanisms, particularly in the realm of DRDoS incidents.

3. Proposed Methodology for DRDoS Attack Detection

In our study, we introduce a machine learning model designed for identifying DRDoS attacks, employing a Features Optimization Technique. Initially, we load the dataset and execute various data preprocessing techniques. Subsequently, we apply two methods: one without feature reduction and the other utilizing PCA for feature reduction. The dataset is then split into two portions: 70% for training and 30% for testing. We utilize machine learning algorithms such as SVM, LR, DT, and RF to construct optimal models. Following this, we assess all models using performance evaluation metrics, including accuracy, precision, and f1-score, and apply cross-validation to validate their efficacy. Finally, we select the best-performing model for further analysis. Figure 5 represents the DRDoS Attack Detection Methodology.

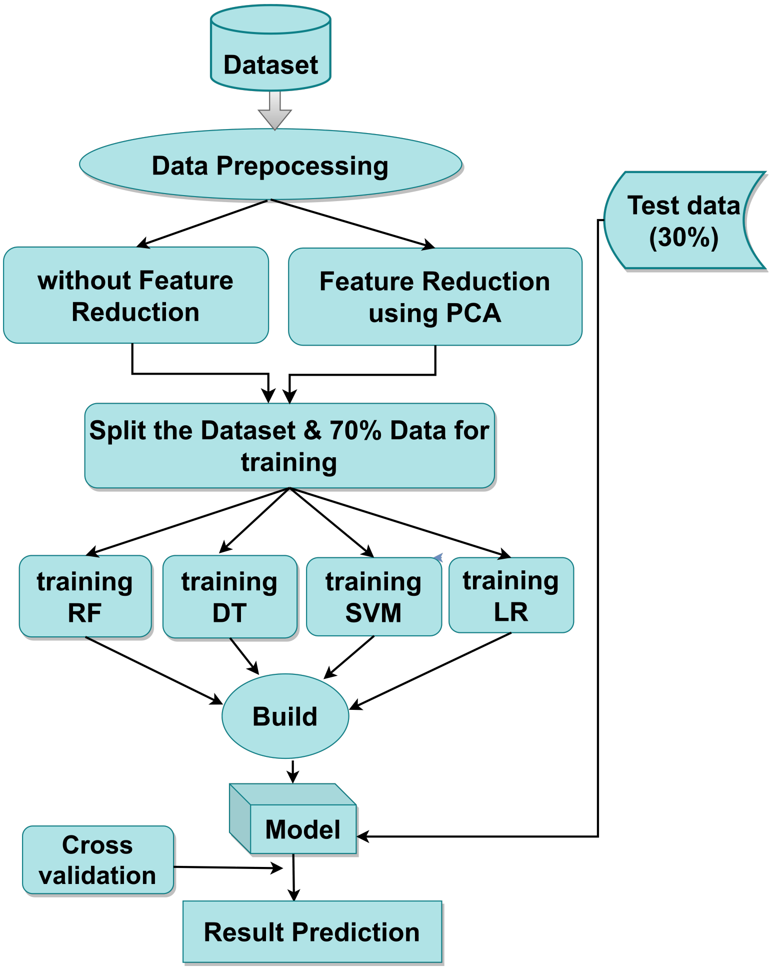


Figure 1. Proposed Architecture for DRDoS Attack Detection

3.1. Dataset

The study utilizes datasets openly accessible through the Canadian Institute for Cybersecurity (CIC). These datasets consist of four sets, each containing 100,000 data points. They form the basis for the analysis and evaluation conducted in the research.The ”Benin” or ”DRDoS Attack” class is present in all four datasets’ label columns. Table 1 shows the information about datasets.

Table 1. Dataset Description

Dataset	Dataset Name	No. of Features	Class
Dataset-1	DRDoS-DNS	88	Benin/DRDoS
Dataset-2	DRDoS-NetBIOS	88	Benin/DRDoS
Dataset-3	DRDoS-UDP	89	Benin/DRDoS
Dataset-4	DRDoS-NTP	89	Benin/DRDoS

3.2. Methods

In this study, multiple datasets were employed to facilitate the detection of DRDoS attacks. Prior to analysis, preprocessing of the datasets was conducted, wherein a label encoding technique was utilized to convert string data into numerical data. The research methodology encompassed two distinct approaches: Method-1 involved detecting DRDoS attacks without employing feature reduction techniques, while Method-2 incorporated feature reduction through Principal Component Analysis (PCA). By comparing the outcomes of these two methods, the effectiveness of feature reduction in enhancing DRDoS attack detection performance could be evaluated.

Method-1:The dataset was split into training and testing sets after the pre-processing stage was finished, with 70% of the data going toward training and the remaining 30% going toward testing. Subsequently, each of the four machine learning algorithms (SVM, LR, RF, DT) was trained using the training data to develop individual models. The performance of each model was then assessed using the test data to evaluate their effectiveness in detecting DRDoS attacks. Notably, this approach did not incorporate feature reduction techniques.

Method-2: After applying the PCA technique for feature reduction, features that contribute to 95% of the dataset's variance were selected to inform decision-making. Following this feature reduction step, 70% of the data was utilized to train individual machine learning algorithms (SVM, LR, RF, DT) and develop respective models. Subsequently, the performance of each model was evaluated using the remaining test data to assess their effectiveness in detecting DRDoS attacks. This approach integrated PCA for feature reduction to enhance the efficiency and efficacy of the detection process.

3.3. Algorithm of DRDoS attack Detection:

A step-by-step process or collection of guidelines for resolving a specific issue or completing a given task is called an algorithm. It is essentially a finite sequence of well-defined instructions that can be executed to achieve a desired outcome. Fundamental to computer science, algorithms are widely employed in a variety of disciplines, such as engineering, data science, AI and mathematics. Algorithms are central to the development of software and are used in a wide range of applications, including search engines, recommendation systems, image processing, cryptography, and machine learning. Understanding algorithms and their properties is essential for computer scientists, software engineers, and anyone working in the field of computing.

The **"Algorithm 1"** begins with loading the dataset into memory, which serves as the initial step preceding any data processing or modeling efforts.Following the dataset loading, it undergoes preparation for modeling, involving tasks such as handling missing values, outliers, encoding categorical variables if needed, and normalizing/standardizing numerical features to ensure consistency and enhance model performance.The preprocessed dataset undergoes two distinct approaches. One method entails modeling without feature reduction, while the other employs Principal Component Analysis (PCA) for dimensionality reduction, preserving the dataset's variance. Subsequently, the dataset is partitioned into training and testing subsets, with a standard allocation of 70% for training to enable pattern learning and 30% for evaluating model performance on unseen data.During the training phase, a variety of machine learning algorithms (e.g., SVM, Random Forest, Logistic Regression, Decision Trees) are trained on the training data. Subsequently, the trained models undergo evaluation using cross-validation techniques (e.g., k-fold cross-validation) on the testing data to estimate performance metrics such as accuracy, precision, recall, and F1 score. Furthermore, the obtained performance metrics from each model are compared to identify the best-performing algorithms. Additionally, the impact of feature reduction using PCA on model performance is analyzed. Based on the evaluation metrics, the best-performing model(s) are selected for deployment, with an expectation of good generalization to new/unseen data. These selected model(s) are then deployed to make predictions on new data in real-world scenarios.After selecting the best-performing model(s), deploy them to make predictions on new or unseen data. Periodically monitor and evaluate the deployed model(s) to ensure continued performance. Make necessary adjustments as needed based on the evaluation results. This ensures that the deployed model(s) maintain their effectiveness over time and adapt to any changes in the data or environment.

Algorithm 1 Data Processing and Model Evaluation

```
procedure STEP-1: LOAD DATASET
end procedure
procedure STEP-2: PREPROCESS DATASET
    a. Handle missing values.
    b. Handle outliers.
    c. Encode categorical variables if necessary.
    d. Normalize/standardize numerical features.
end procedure
procedure STEP-3: APPLY TWO APPROACHES
    a. Approach 1: Without feature reduction.
    b. Approach 2: With feature reduction using PCA.
end procedure
procedure STEP-4: SPLIT DATASET
    a. Training data: 70% of the dataset.
    b. Testing data: 30% of the dataset.
end procedure
procedure STEP-5: FOR EACH APPROACH
    a. Use the training data to build AI models:
        i. Train different machine learning algorithms (e.g., SVM, Random Forest, Logistic Regression, Decision Trees) on the training data.
    b. Test the models using cross-validation on the testing data:
        i. Perform k-fold cross-validation (e.g., k=5) on each model.
        ii. Evaluate the performance metrics (e.g., accuracy, precision, recall, F1 score) for each model.
end procedure
procedure STEP-6: COMPARE MODEL PERFORMANCE
    a. Compare the mean performance metrics across different algorithms.
    b. Analyze the impact of feature reduction using PCA on model performance.
end procedure
Step-7: Select the best-performing model(s) based on the evaluation metrics.
Step-8: Deploy the selected model(s) for making predictions on new/unseen data.
Step-9: Monitor and evaluate the deployed model(s) periodically to ensure continued performance and make necessary adjustments as needed.
```

3.4. Machine Learning Algorithm

Machine learning algorithms such as SVM, DT, RF, and LR play a pivotal role in detecting DRDoS attacks efficiently. Each algorithm offers distinct features and capabilities, contributing to the effectiveness of detection methodologies. Through individual examination, researchers can gain insights into the strengths and limitations of SVM, DT, RF, and LR in the context of DRDoS attack detection.

3.4.1. ***Decision Tree Algorithm(DT):*** The decision tree algorithm finds extensive application in data classification across various domains. It establishes a hierarchical structure wherein nodes correspond to dataset features, while branches represent decision rules derived from these features. At each node, the algorithm optimizes classification accuracy by selecting the best split, progressing recursively until reaching leaf nodes that determine final outcomes. This iterative evaluation of features enables decision trees to proficiently organize and classify data, accommodating both categorical and numerical data types. Additionally, their interpretability aids in elucidating underlying data patterns and justifying classification decisions. [30]. The Random Forest algorithm follows this operational procedure:

- Selecting the target attribute.

- Compute Information Gain with respect to the desired attribute.
- Applying the following formula to find the entropy of the other characteristics:

$$Entropy(s) = \sum_{i=1}^{n} (-P_i \log_2 P_i) \quad (1) \tag{1}$$

- Determining the Gain(G) using the following formula::

$$Gain(S, A) = Entropy(s) - \sum_{i=1}^{n} \left(\frac{S_v}{S} \times Entropy(S_v) \right) \tag{2}$$

3.4.2. ***Support Vector Machine(SVM):*** Support Vector Machine serves as a versatile tool for both classification and regression tasks, effectively partitioning n-dimensional space into distinct categories using optimal decision boundaries. The identification of support vectors, located closest to these boundaries, plays a critical role in defining the margin of the decision plane, thus augmenting SVM's capacity for generalization and resilience to novel data. Its efficiency in accurately allocating future data points to their respective categories underscores its utility in scenarios demanding precise decision boundaries for accurate classification or regression. Overall, SVM's adaptability and effectiveness make it a powerful asset across various domains in machine learning. [31]. figure 2 depicts a classifier implemented using the Support Vector Machine algorithm.

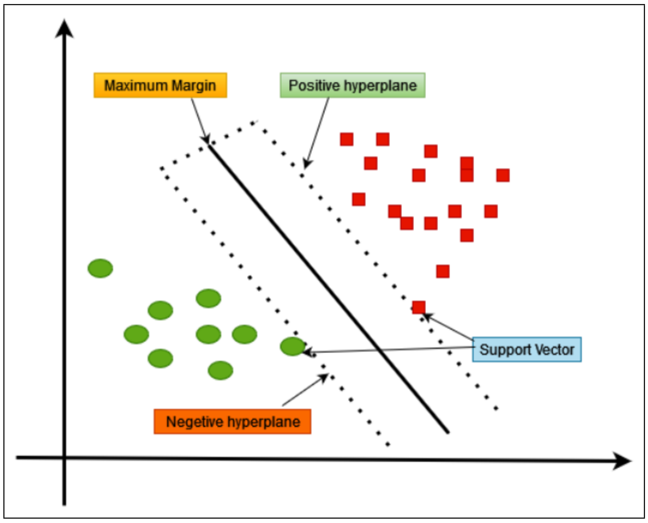


Figure 2. Support Vector Machine(SVM)

The equation for a support vector machine (SVM) can be represented as follows:

$$\text{minimize} \left(\frac{1}{2} \|\mathbf{w}\|^2 + C \sum_{i=1}^{n} \xi_i \right) \tag{3}$$

$$y_i(\mathbf{w} \cdot \mathbf{x}_i + b) \geq 1 - \xi_i, \quad \xi_i \geq 0, \quad i = 1, 2, ..., n \tag{4}$$

Where $\mathbf{w}$ represents the weight vector, b is the bias term, C is the regularization parameter, $\mathbf{x}_i$ is the feature vector of the i-th training example, y_i is the label of the i-th training example, and ξ_i are slack variables.

3.4.3. ***Random Forest(RF):*** Random Forest, a renowned ensemble learning technique, constructs multiple decision trees by utilizing random subsets of features and training data, then combines their predictions for final outcomes. Its versatility extends to both regression and classification tasks, while its ability to handle large datasets and reduce noise enhances its standing in the machine-learning community. Recognized for its adaptability, simplicity, and efficiency, Random Forest remains a highly favored approach in various application domains. Its amalgamation of diverse decision trees allows for robust predictions, contributing to its widespread adoption and continued relevance in modern machine learning practices[32]. Figure 3 depicts a classifier implemented using the Random Forest algorithm.

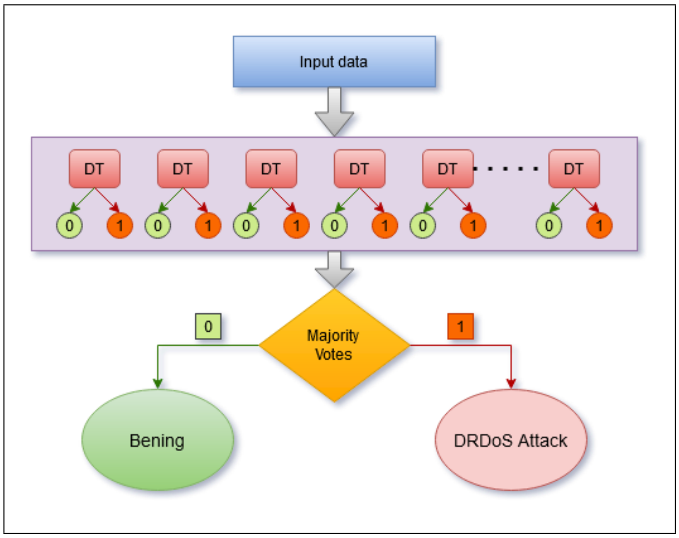


Figure 3. Random Forest

The operational procedure of the Random Forest algorithm is outlined as follows:

Training Phase:

- Let X represent the feature matrix containing m features and n samples. $X = \{x_1, x_2, ..., x_n\}$, where $x_i \in \mathbb{R}^m$.
- Let Y be the target vector with corresponding labels for the n samples: $Y = \{y_1, y_2, ..., y_n\}$, where $y_i \in \{1, 2, ..., K\}$ for classification (with K classes) or $y_i \in \mathbb{R}$ for regression.
- Let T be the number of decision trees in the forest.
- For each decision tree $t = 1, 2, ..., T$:
    - Randomly sample X_t and Y_t from X and Y with replacement (bootstrap sample).
    - Choose a portion of the features at random for every decision tree split.
    - A DT trains by using X_t and Y_t.

Prediction Phase:

- For each new sample x_{new}, predict its label using each decision tree in the forest.
- Utilize majority voting in the classification process to identify the final anticipated class.
- The final prediction for regression should be the mean of all the decision trees' predictions.

3.4.4. ***Logistic Regression(LR):*** One popular machine learning method for binary classification problems is logistic regression (LR). It is used to ascertain if an input is benign or not. Logistic regression (LR), sometimes referred to as the log-linear classifier, logit regression, or maximum-entropy classifier (MaxEnt), uses the sigmoid function to generate predictions. In this method, a linear equation (equation 1) is calculated for the input data values, denoted by A = A1, A2, A3, ... An. The logit function, described by equation (3), is then applied to transform the outcome of the linear equation into a probability between 0 and 1. Equation (1) plays a crucial role in calculating the regression coefficient using maximum likelihood estimation (MLE). Overall, LR serves as a powerful tool for classification tasks, leveraging mathematical functions to make accurate predictions based on input data [33].

$$W^T = \max \sum_{j=1}^{n} (Y_j \cdot W_j A_j) \tag{5}$$

$$r = Y_j \cdot W^T A_j \tag{6}$$

$$P(r) = \frac{1}{1 + \exp(-r)} \tag{7}$$

When $P(r) > 0.5$, it displays the likelihood that the input instance is a DDoS attack, whereas when $P(r) < 0.5$, it indicates the likelihood that the input instance is benign. The data points are denoted by Y_j.

3.5. Feature Importance Analysis

The process of figuring out which features (or variables) in the dataset have the biggest impact on a model's prediction is known as feature importance analysis. It is essential for figuring out which features have the greatest influence, enhancing model performance, and comprehending the decision-making process of the model. In this work, the contribution of each feature to the model's predictions is revealed by the importance scores, which are directly analyzed in tree-based models such as RF and DT. The coefficients are analyzed for SVM and LR with a linear kernel to determine how each feature affects the detection of DRDoS attacks. PCA is also used for feature reduction, which reduces the size of the original features into a smaller group of uncorrelated components that represent the majority of the variance in the dataset of DDoS attacks. Through this process, important patterns can be found, noise and redundancy can be removed, and the data can be more easily managed for modeling and visualization.Next, we will provide a detailed discussion of Principal Component Analysis (PCA) in the upcoming section.

3.5.1. ***Principal Component Analysis (PCA):*** PCA is a technique used for dimensionality reduction in machine learning [34]. It identifies the most important features in a dataset by transforming the data into a new coordinate system. PCA aims to capture as much of the dataset's variability as possible with a smaller number of dimensions.By determining the eigenvalues and eigenvectors of the data's covariance matrix, it accomplishes this. The principal components, also referred to as eigenvectors, show which directions in the data have the greatest variance. PCA makes it possible to reduce the dimensionality of the dataset while maintaining the highest level of information. It helps to alleviate the curse of dimensionality, reduce computational complexity, and visualize high-dimensional data. PCA is sensitive to scaling, so it is often preceded by standardization of the features. It is widely used in various fields such as image processing, genetics, and finance for exploratory data analysis and feature extraction. [35]. In this study, four machine learning algorithms (SVM, DT, RF, and LR) were trained to detect denial-of-service (DRDoS) attacks using features that were selected through feature reduction using Principal Component Analysis (PCA), which yielded features that account for 95% of the variance in the dataset.

Following steps for PCA:

- The dataset is obtained.
- Putting data into an organized format.
- Data standardization.
- Determining the Covariance matrix.

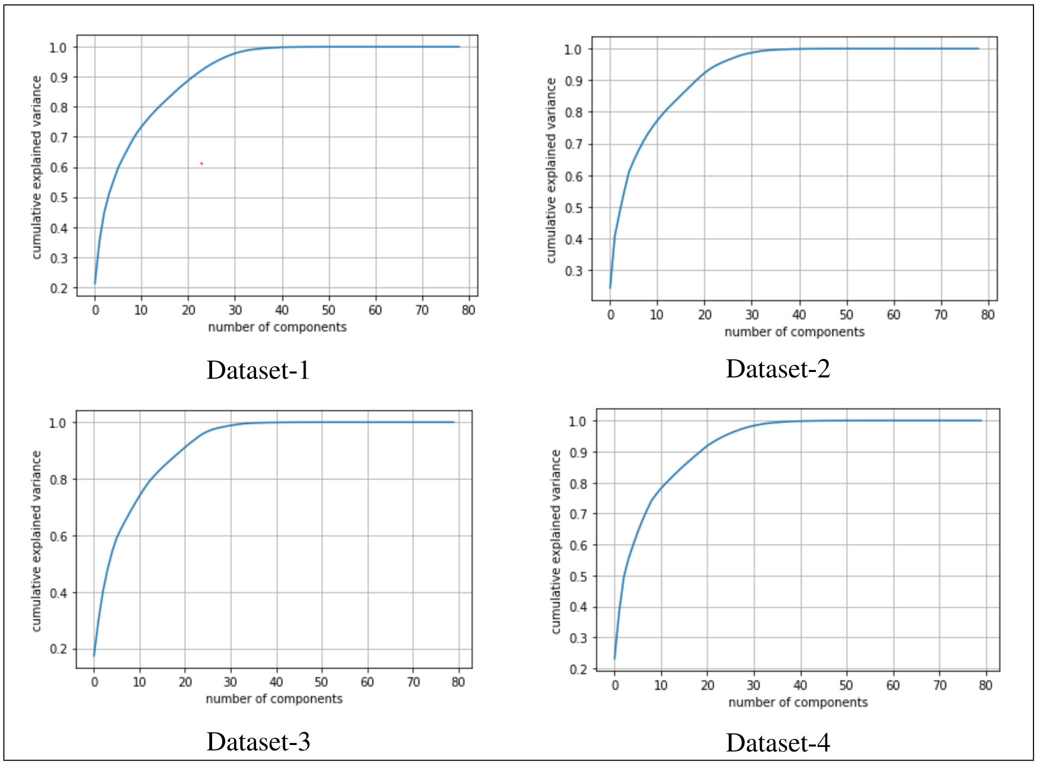
$$\Sigma = \frac{1}{m}(X - \bar{X})^T (X - \bar{X}) \tag{8}$$

- Compute Eigen Vectors and Eigen Values as following equation:

$$A\mathbf{v} = \lambda\mathbf{v} \tag{9}$$

Where A is a square matrix, λ is a scalar known as the eigenvalue, and $\mathbf{v}$ is a non-zero vector known as the eigenvector associated with the eigenvalue λ.

In a scatter plot of two variables, the covariance curve visually represents how the covariance between those variables changes as one variable varies while the other is held constant. A positive covariance, or the tendency for one variable to increase along with another, is indicated by an upward-sloping curve. A downward-sloping curve denotes a negative covariance, which implies that one variable tends to decrease as the other increases. If the curve is flat, it implies no covariance between the variables. We have now plotted the covariance curve for the entire dataset in our study.



Dataset-1

Dataset-2

Dataset-3

Dataset-4

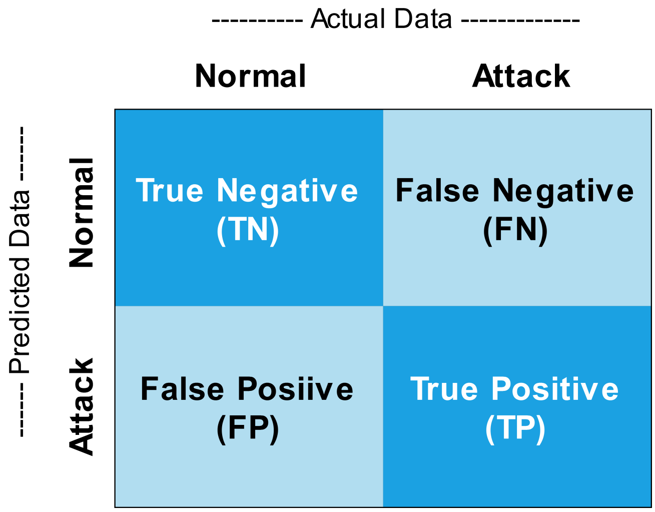
Figure 4. Covariance Curve for all datasets

3.6. Performance parameters

In our study, we utilized four distinct datasets and applied various machine learning models for training. We used important metrics like F1 score, Accuracy, Precision, and Recall to evaluate each model's performance. The confusion matrix, a vital tool for assessing model performance, is the source of these metrics. While the confusion matrix itself does not offer direct performance measures, it plays a crucial role in computing other essential metrics. To gain deeper insights into the classification performance of the models, we visually represented the confusion matrix in a figure. This visualization aided in understanding the model's ability to accurately classify instances and guided further analysis. Overall, this methodology provided a comprehensive framework for evaluating the efficacy of each machine learning model in identifying DRDoS attacks. Figure 5 shows the confusion matrix diagram.

Here's the description of the parameters in a confusion matrix:

- **True Positive (TP):** When the algorithm predicts a positive outcome, and it is actually true, it is referred to as True Positive.



------ Predicted Data ------	---------- Actual Data ------------- Normal	Attack
Normal	True Negative (TN)	False Negative (FN)
Attack	False Posiive (FP)	True Positive (TP)

Figure 5. Confusion Matrix Diagram

- **False Positive (FP):** When the algorithm predicts a positive outcome, but it is actually false, it is termed False Positive.
- **False Negative (FN):** FN refers to an algorithm's prediction of a negative outcome that turns out to be true.
- **True Negative (TN):** When the algorithm predicts a negative outcome, and it is actually false, it is known as True Negative.

In Table [2],We outline critical performance measures, such as F1-score, Accuracy, Precision, and Recall, that are necessary to assess how well each model detects DRDoS attacks.

Table 2. Performance Measurement Parameters

Metrics	Formula
Accuracy	$\frac{(TP+TN)}{((TP+FP)+(FN+TN))} \times 100$
Precision	$\frac{TP}{(TP+FP)} \times 100$
Recall	$\frac{TP}{(TP+FN)} \times 100$
F1-score	$2 \times \frac{(Recall \times Precision)}{(Recall+Precision)} \times 100$

Accuracy represents the overall rate of correct predictions made by a classifier. Precision measures the percentage of accurate predictions of a specific class among all predictions for that class. Recall quantifies the proportion of accurately predicted instances of a particular class out of all instances belonging to that class. The F1-score combines precision and recall to provide a single metric that reflects the reliability and accuracy of the classifier. It is particularly useful when there is an imbalance between the classes in the dataset.[36].

3.7. Receiver Operating Characteristic (ROC) Curve

A graphical tool for assessing the effectiveness of binary classification models is the ROC curve. It displays, for a range of threshold values, the true positive rate (Sensitivity) versus the false positive rate (1-Specificity). A visual evaluation of the trade-off between sensitivity and specificity is provided by the curve. A model that performs better overall in differentiating between the two classes is indicated by a higher area under the ROC curve (AUC).

When there is an imbalance in the class distribution or a difference in the cost of false positives and false negatives, ROC curves are especially helpful. They help determine the ideal threshold for classification decisions and provide insightful information about a classifier's discriminatory power. The True Positive Rate (TPR) and False Positive Rate (FPR) can be defined mathematically as follows:

$$\text{True Positive Rate (TPR)} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}}$$
$$\text{False Positive Rate (FPR)} = \frac{\text{False Positives}}{\text{False Positives} + \text{True Negatives}}$$

These rates are calculated for various threshold values used to convert the continuous output of a classifier (e.g., probability score) into binary predictions. By varying the threshold, we can generate different points on the ROC curve, with each point representing the trade-off between TPR and FPR at a specific threshold.

4. Experiment Results and Discussion

We have covered the outcomes of all four models for every dataset in this section. Initially, we talked about the outcomes using five times the number of models for each dataset, both with and without feature reduction using PCA. Second, we display an overview of all the findings. The authors employed four machine learning algorithms, namely Support Vector Machine (SVM), Logistic Regression (LR), Random Forest (RF), and Decision Tree (DT), across two approaches for each of the four datasets. Additionally, they conducted 5-fold cross-validation for each algorithm. Subsequently, they observed and documented the findings.

4.1. Result Analysis of Dataset 1

In Dataset-1, the RF and DT classifiers both demonstrate the best performance, achieving 100% accuracy without feature reduction. Meanwhile, the SVM and LR classifiers achieve accuracies of 98% and 99%, respectively, under the same conditions. Furthermore, RF and DT exhibit 100% precision, recall, and F1-score, while SVM and LR achieve 49.8% and 88.2% F1-score, respectively, along with 59.2% and 89.4% precision, and 50% and 87.6% recall, respectively, without feature reduction.However, in the feature reduction using PCA approach, both the RF and DT classifiers continue to demonstrate the best performance, achieving 100% accuracy. Meanwhile, the SVM and LR classifiers achieve accuracies of 99% and 98%, respectively, under the same conditions. Additionally, RF and DT exhibit 97.2% and 97% F1-score, 98.4% and 97.8% precision, and 96.4% and 96.4% recall, respectively. In contrast, SVM and LR achieve 66.6% and 61.4% F1-score, along with 98.6% and 93.6% precision, and 60.2% and 56.4% recall, respectively.

4.2. Result Analysis of Dataset 2

In Dataset-2, RF and DT classifiers both demonstrate the best performance, achieving 100% accuracy without feature reduction. Meanwhile, the SVM and LR classifiers achieve accuracies of 99.19% and 99.89%, respectively, under the same conditions. Furthermore, RF and DT exhibit 100% precision, recall, and F1-score, while SVM and LR achieve 60.2% and 86.4% F1-score, respectively, along with 60% and 87.8% precision, and 60.2% and 86.4% recall, respectively, without feature reduction.But in the feature reduction using PCA approach, both the RF and DT classifiers continue to demonstrate the best performance, achieving 100% accuracy. Meanwhile, the SVM and LR classifiers achieve accuracies of 99.48% and 99.50%, respectively, under the same conditions. Additionally, RF and DT exhibit 97.4% and 96.8% F1-score, 97.4% and 96.20% precision, and 97.4% and 96.80% recall, respectively. In contrast, SVM and LR achieve 59.2% and 63.40% F1-score, along with 100% and 95.6% precision, and 55% and 58% recall, respectively.

4.3. Result Analysis of Dataset 3

In Dataset-3, RF and DT classifiers both demonstrate the best performance, achieving 100% accuracy without feature reduction. Meanwhile, the SVM and LR classifiers achieve accuracies of 99.09% and 99.40%, respectively, under the same conditions. Furthermore, RF and DT exhibit 100% precision, recall, and F1-score, while SVM and LR achieve 50.2% and 85.2% F1-score, respectively, along with 90% and 90.4% precision, and 50% and 77.8% recall, respectively, without feature reduction.However, in the feature reduction using PCA approach, both the RF and DT classifiers continue to demonstrate the best performance, achieving 100% accuracy. Meanwhile, the SVM and LR classifiers achieve accuracies of 99.13% and 99.40%, respectively, under the same conditions. Additionally, RF and DT exhibit 94.6% and 92.8% F1-score, 96.6% and 92.6% precision, and 92.4% and 92.6% recall, respectively. In contrast, SVM and LR achieve 52.4% and 65% F1-score, along with 100% and 71.2% precision, and 51.2% and 61.4% recall, respectively.

4.4. Result Analysis of Dataset 4

In Dataset-4, RF and DT classifiers both demonstrate the best performance, achieving 100% accuracy without feature reduction. Meanwhile, the SVM and LR classifiers achieve accuracies of 87.60% and 98.75%, respectively, under the same conditions. Furthermore, RF and DT exhibit 100% precision, recall, and F1-score, while SVM and LR achieve 80.8% and 96.4% F1-score, respectively. Additionally, SVM and LR achieve precision rates of 94.4% and 96.40%, and recall rates of 50% and 98%, respectively, without feature reduction. However, in the feature reduction using PCA approach, both the RF and DT classifiers continue to demonstrate performance, achieving accuracies of 98.79% and 98.50%, respectively. Meanwhile, the SVM and LR classifiers achieve accuracies of 93.61% and 88.80%, respectively, under the same conditions. Additionally, RF and DT exhibit F1-scores of 97.8% and 96%, precision rates of 97.4% and 96.20%, and recall rates of 97% and 96.8%, respectively. In contrast, SVM and LR achieve F1-scores of 80.8% and 57.8%, precision rates of 95.8% and 91.6%, and recall rates of 74.8% and 55.8%, respectively.

4.5. Summary Table of Result Analysis

We have summarized all the results of five fold cross validation and presented them in the following table.

Table 3 presents the mean value derived from five fold cross-validation scores for all machine learning models applied to dataset-1.

Table 3. Summary of the results for Dataset-1

Dataset 1					
Model	**Method**	**Accuracy**	**Precision**	**Recall**	**F1-Score**
SVM	Without Feature Reduction	98%	59.2%	50%	49.8%
	With Feature Reduction Using PCA	99%	98.6%	60.2%	66.6%
LR	Without Feature Reduction	99%	89.4%	87.6%	88.2%
	With Feature Reduction Using PCA	98%	93.6%	56.4%	61.4%
RF	Without Feature Reduction	100%	100%	100%	100%
	With Feature Reduction Using PCA	100%	98.4%	96.4%	97.2%
DT	Without Feature Reduction	100%	100%	100%	100%
	With Feature Reduction Using PCA	100%	97.8%	96.4%	97%

The mean value obtained from five fold cross-validation scores for each ML model used with dataset-2 is displayed in Table 4.

Table 4. Summary of the results for Dataset-2

Dataset 2					
Model	**Method**	**Accuracy**	**Precision**	**Recall**	**F1-Score**
SVM	Without Feature Reduction	99.19%	60%	50.4%	60.2%
	With Feature Reduction Using PCA	99.48%	100%	55%	59.2%
LR	Without Feature Reduction	99.89%	87.8%	80%	86.4%
	With Feature Reduction Using PCA	99.50%	95.6%	58%	63.4%
RF	Without Feature Reduction	100%	100%	100%	100%
	With Feature Reduction Using PCA	100%	97.4%	97.4%	97.2%
DT	Without Feature Reduction	100%	100%	100%	100%
	With Feature Reduction Using PCA	100%	96.2%	96.8%	96.8%

Table 5 displays the mean value obtained from five fold cross-validation scores for each machine learning model applied to dataset-3.

Table 5. Summary of the results for Dataset-3

Dataset 3					
Model	**Method**	**Accuracy**	**Precision**	**Recall**	**F1-Score**
SVM	Without Feature Reduction	99.09%	90%	50%	50.2%
	With Feature Reduction Using PCA	99.13%	100%	51.2%	52.4%
LR	Without Feature Reduction	99.40%	90.4%	77.8%	85.2%
	With Feature Reduction Using PCA	99.04%	71.2%	61.4%	65%
RF	Without Feature Reduction	100%	100%	100%	100%
	With Feature Reduction Using PCA	100%	96.6%	92.4%	94.6%
DT	Without Feature Reduction	100%	100%	100%	100%
	With Feature Reduction Using PCA	100%	92.2%	92.6%	92.8%

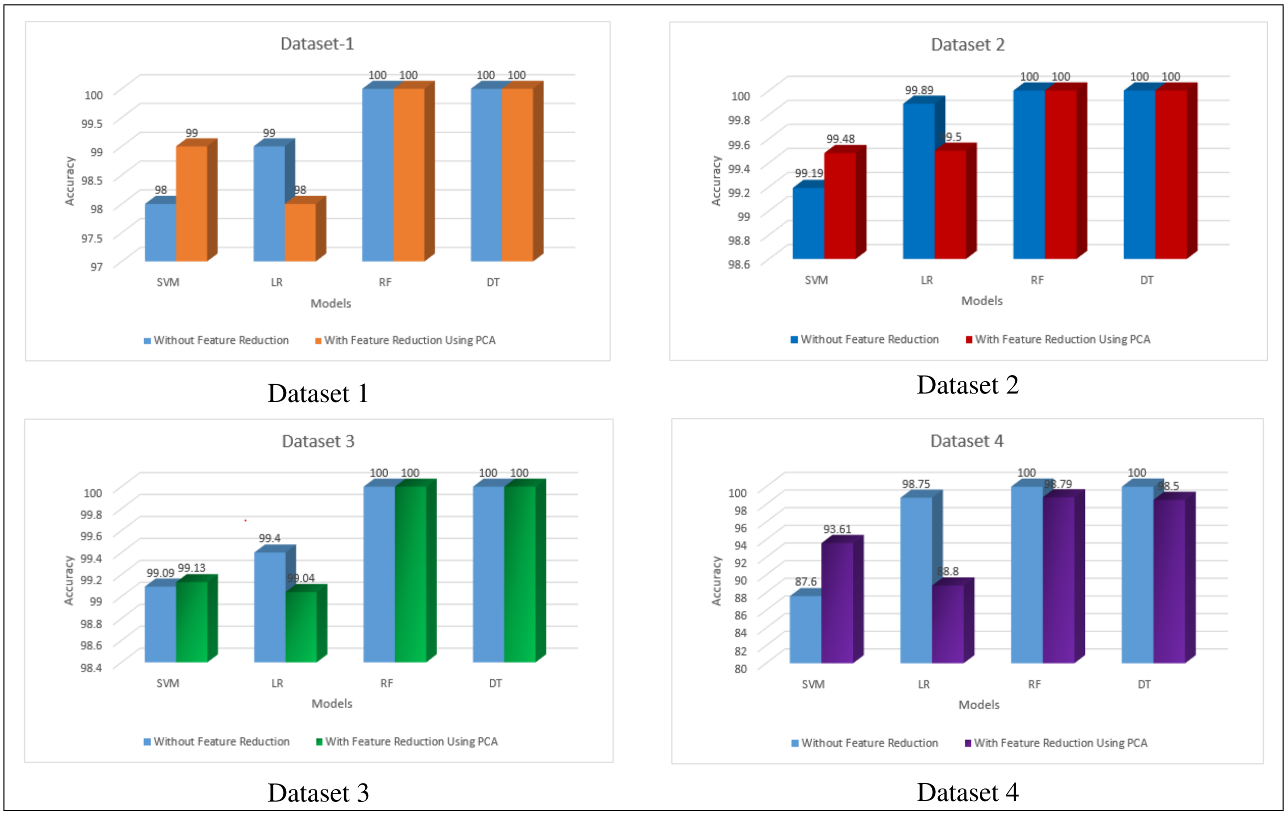
The mean value derived from five fold cross-validation scores for every ML model used with dataset-4 is displayed in Table 6.

Table 6. Summary of the results for Dataset-4

Dataset 4					
Model	**Method**	**Accuracy**	**Precision**	**Recall**	**F1-Score**
SVM	Without Feature Reduction	87.60%	94.4%	50%	47%
	With Feature Reduction Using PCA	93.61%	95.8%	74.8%	80.8%
LR	Without Feature Reduction	98.75%	96.4%	98%	96.4%
	With Feature Reduction Using PCA	88.80%	91.6%	55.8%	57.8%
RF	Without Feature Reduction	100%	100%	100%	100%
	With Feature Reduction Using PCA	98.79%	97.4%	97%	97.8%
DT	Without Feature Reduction	100%	100%	100%	100%
	With Feature Reduction Using PCA	98.50%	96.4%	96.8%	96%

4.6. Bar chat representation of Accuracy, Precision, Recall, F1-Score

To visualize the accuracy, precision, recall, fa-score results of all machine learning models across all datasets, bar chart is presented below.



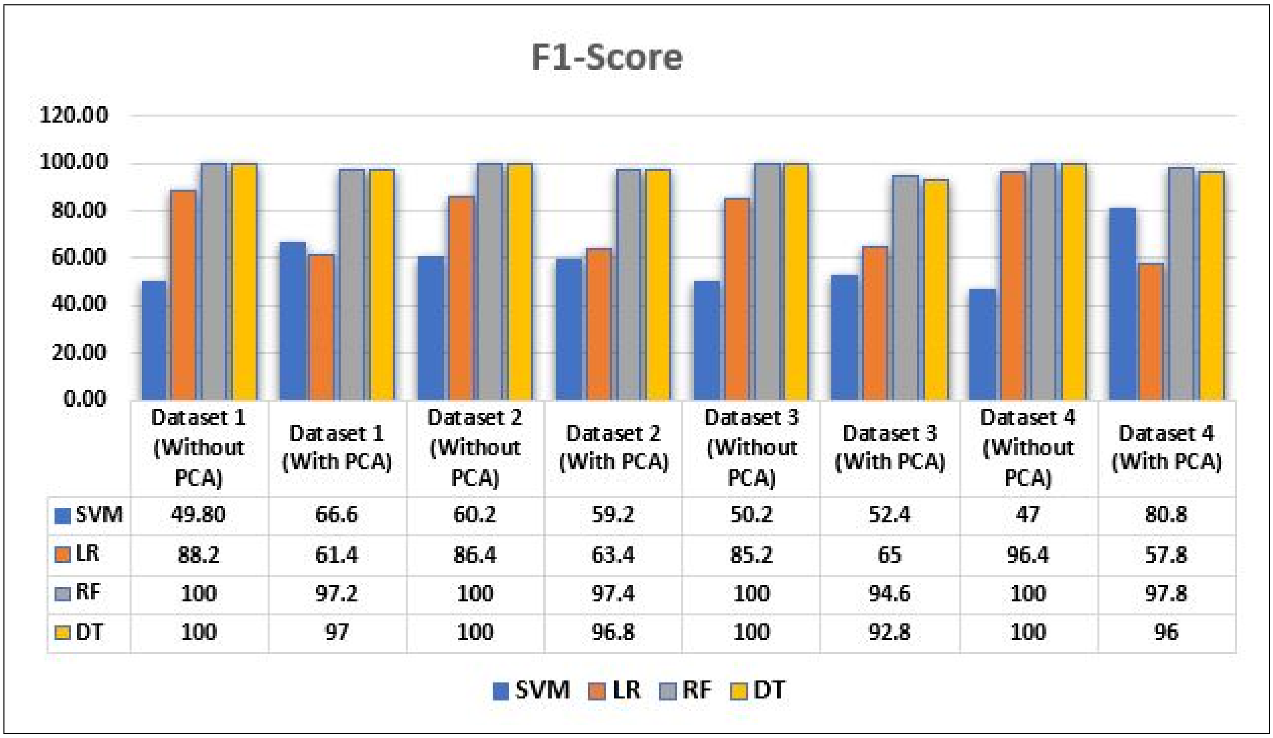
Dataset 1

Dataset 2

Dataset 3

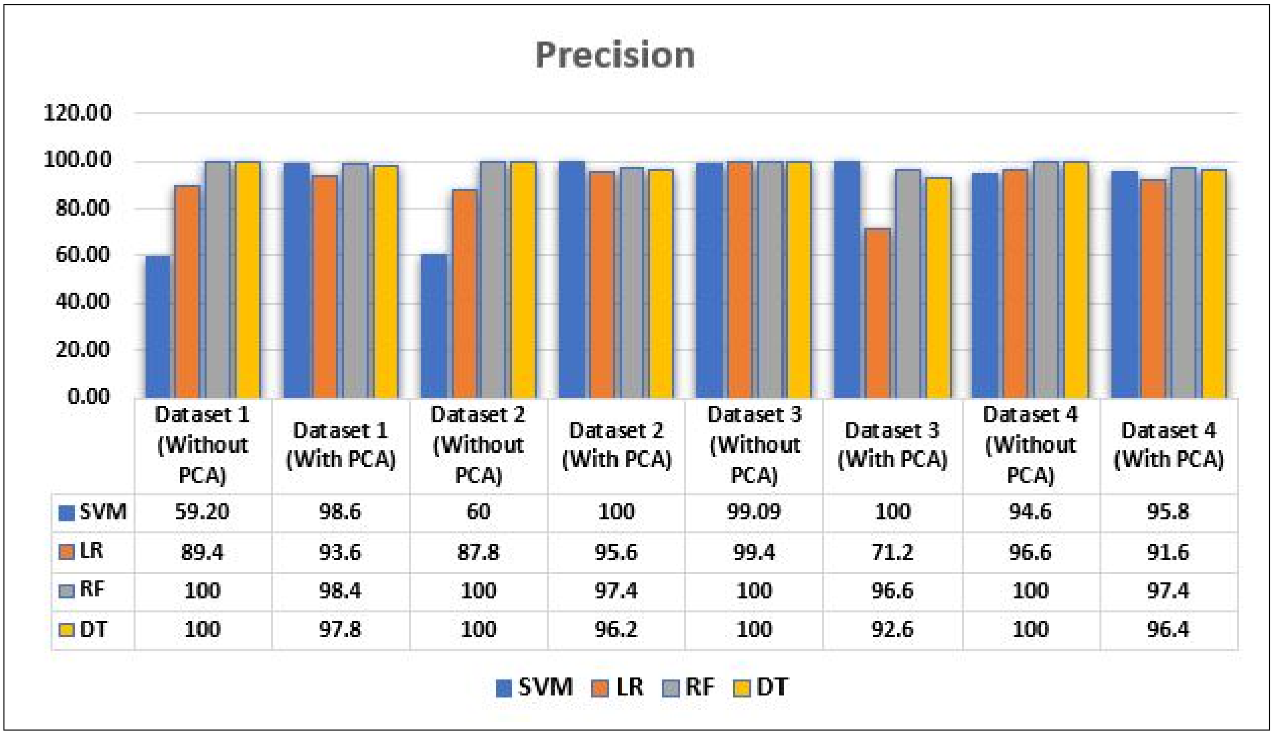
Dataset 4

(a) Accuracy of all models for all four datasets



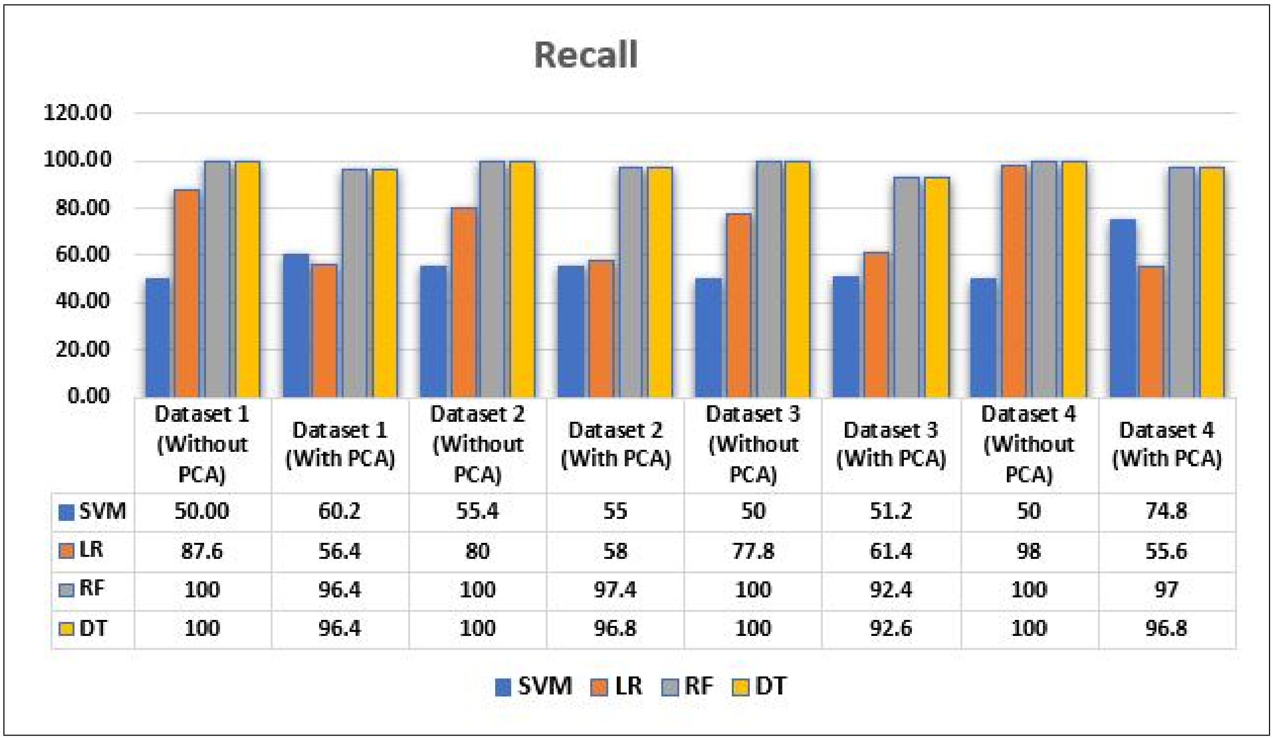
	Dataset 1 (Without PCA)	Dataset 1 (With PCA)	Dataset 2 (Without PCA)	Dataset 2 (With PCA)	Dataset 3 (Without PCA)	Dataset 3 (With PCA)	Dataset 4 (Without PCA)	Dataset 4 (With PCA)
■ SVM	49.80	66.6	60.2	59.2	50.2	52.4	47	80.8
■ LR	88.2	61.4	86.4	63.4	85.2	65	96.4	57.8
■ RF	100	97.2	100	97.4	100	94.6	100	97.8
■ DT	100	97	100	96.8	100	92.8	100	96

(b) **F1-Score result for all the Datasets**



	Dataset 1 (Without PCA)	Dataset 1 (With PCA)	Dataset 2 (Without PCA)	Dataset 2 (With PCA)	Dataset 3 (Without PCA)	Dataset 3 (With PCA)	Dataset 4 (Without PCA)	Dataset 4 (With PCA)
■ SVM	59.20	98.6	60	100	99.09	100	94.6	95.8
■ LR	89.4	93.6	87.8	95.6	99.4	71.2	96.6	91.6
■ RF	100	98.4	100	97.4	100	96.6	100	97.4
■ DT	100	97.8	100	96.2	100	92.6	100	96.4

(a) **Precision result for all the Dataset**



	Dataset 1 (Without PCA)	Dataset 1 (With PCA)	Dataset 2 (Without PCA)	Dataset 2 (With PCA)	Dataset 3 (Without PCA)	Dataset 3 (With PCA)	Dataset 4 (Without PCA)	Dataset 4 (With PCA)
■ SVM	50.00	60.2	55.4	55	50	51.2	50	74.8
■ LR	87.6	56.4	80	58	77.8	61.4	98	55.6
■ RF	100	96.4	100	97.4	100	92.4	100	97
■ DT	100	96.4	100	96.8	100	92.6	100	96.8

(b) **Recall result for all the Dataset**

4.7. *ROC Curve Representation*

For dataset-1, employing the without feature reduction technique, both RF and DT algorithms exhibit outstanding performance, evidenced by a mean ROC area under the curve (AUC) of 1.00 shown in figure 8.

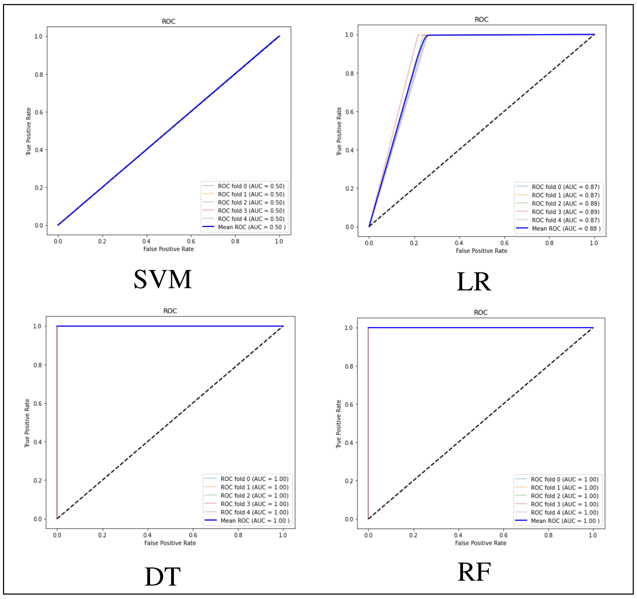


Figure 8. ROC Curve for dataset-1(without Feature Reduction)

For dataset-1, utilizing the feature reduction technique, RF and DT algorithms continue to demonstrate exceptional performance, achieving a mean ROC area under the curve (AUC) of 1.00 as seen in figure 9.

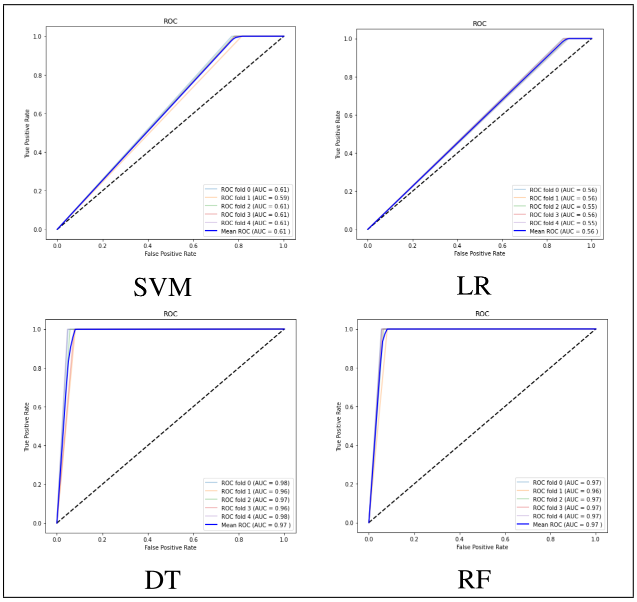


Figure 9. ROC Curve for dataset-1(with Feature Reduction)

Similarly, for dataset 2, RF and DT algorithms showcase superior performance when no feature reduction strategy is employed, achieving a mean ROC area under the curve (AUC) of 1.00 presented in Figure 10.

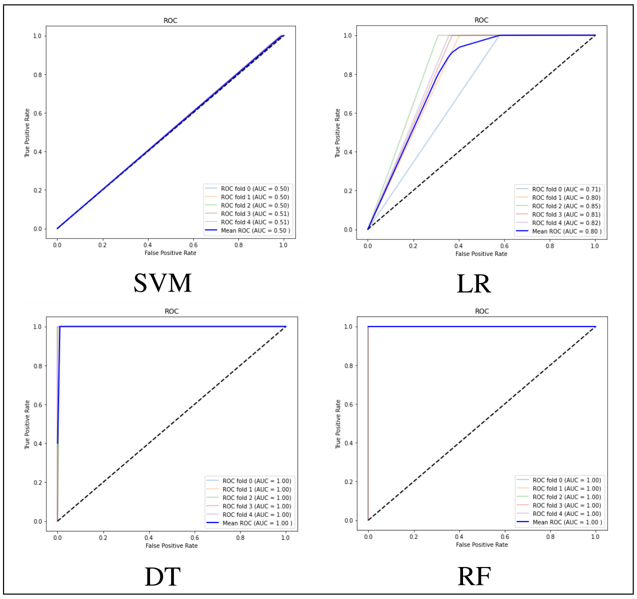


Figure 10. ROC Curve for dataset-2(without Feature Reduction)

Additionally, for dataset 2, employing the feature reduction strategy, RF and DT algorithms maintain their superior performance, achieving a mean ROC area under the curve (AUC) of 1.00 displayed in Figure 11.

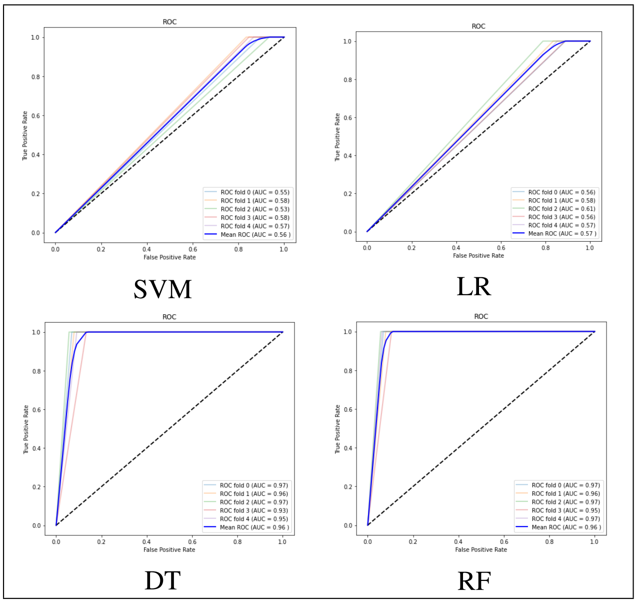


Figure 11. ROC Curve for dataset-2(with Feature Reduction)

For dataset-3 employing no feature reduction strategy, the RF and DT once more provide the best results with mean ROC (AUC=1.00) is illustrated in Figure 12.

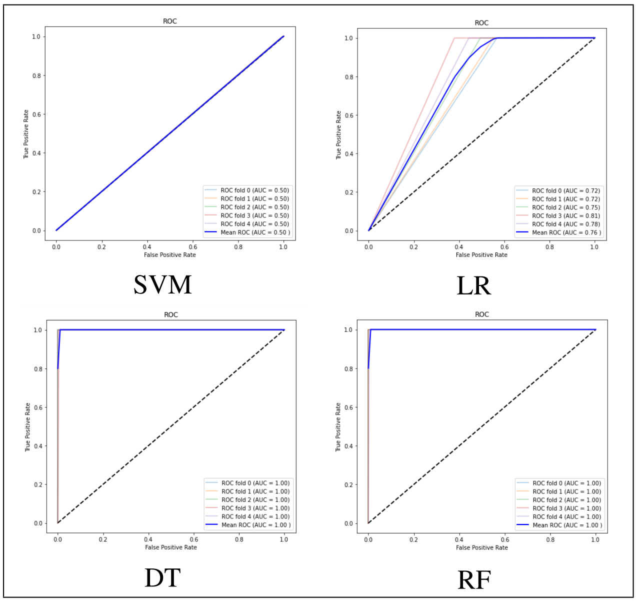


Figure 12. ROC Curve for dataset-3(without Feature Reduction)

For dataset-3, when employing the feature reduction strategy, RF and DT algorithms once again demonstrate the best performance, achieving a mean ROC area under the curve (AUC) of 1.00 is depicted in Figure 13.

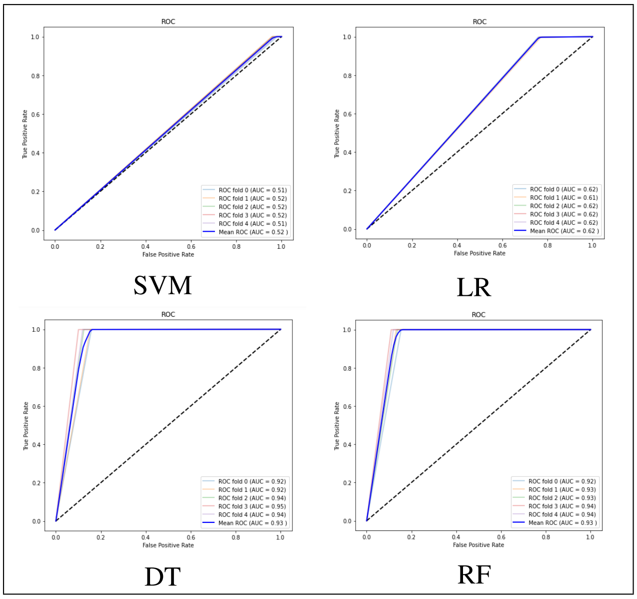


Figure 13. ROC Curve for dataset-3(with Feature Reduction)

Ultimately, for dataset-4, the DT and RF algorithms showcase the highest performance, achieving a mean ROC area under the curve (AUC) of 1.00, without employing the feature reduction technique is seen in Figure 14.

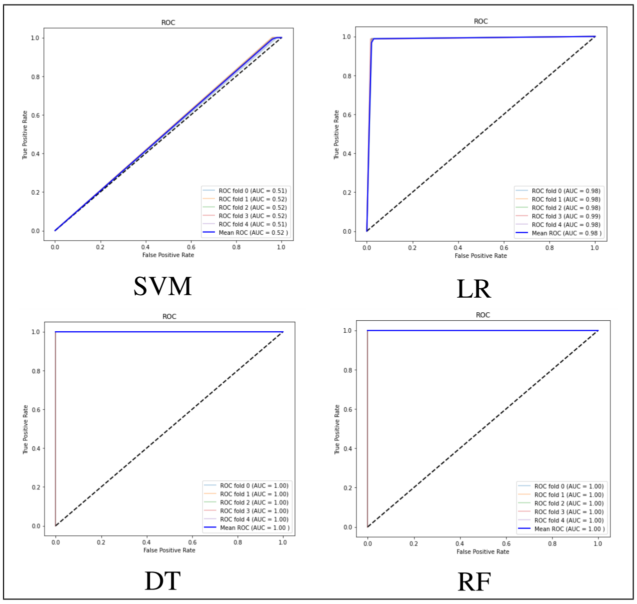


Figure 14. ROC Curve for dataset-4(without Feature Reduction)

The DT and RF algorithms ultimately exhibit the highest performance for dataset-4, achieving a mean ROC area under the curve (AUC) of 1.00 when utilizing the feature reduction technique is despalyed in Figure 15.

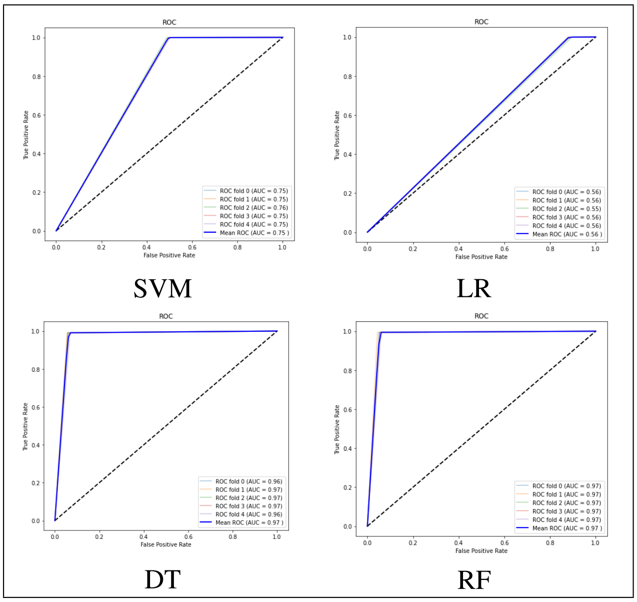


Figure 15. ROC Curve for dataset-4(with Feature Reduction)

4.8. Discussion

While some research has been done on DRDoS attacks in the past, it is not up to date. For this reason, the authors attempted to propose a novel machine learning model for early detection of DDoS attacks.The author noted that the Random Forest (RF) and Decision Tree (DT) algorithms both performed remarkably well, continuously producing perfect F1 scores and 100% accuracy in DRDoS attack detection. Except for Dataset 4, this exceptional performance persisted even when PCA-based feature reduction was used. A few preventative measures are taken to stop the DRDoS attack.By preventing malicious traffic and managing data flow, network traffic filtering and rate limiting can be used to lessen the impact of DDoS attacks. Deploy strong security measures as well, such as intrusion detection systems and firewalls, to find and stop possible attack points. Now we demonstrate the comparison of our model to existing work conducted by others. The comparison between our suggested method and the other current method is shown in Table 7.

Table 7. Comparison of DRDoS Attack Detection Methods

Ref.	**Model + Dataset**			**Algorithms /Methods**	**Major Findings**
1	Feature Selection Model			Nature-inspired optimization, KNN, RF, SVM	89.59% accuracy
4	Deep Forest-Based Method			Deep Forest, IoT, Big Data techniques	Higher detection rate, false alarms
7	Machine Learning Approach			SVM algorithm	Detection success rate, false positive rates
8	PIDC System			Data mining,C4.5 algorithm	True positive rate 99%, false positive rate <1%
10	UDP Protocol-Based			Detection algorithm	Higher detection rate
11	CARD in MANET			Continuous and Random Dropping	Successfully Detected.
12	Integrated Approach			E-RED, ANT Classification	99% true positives, 1% false positives
Pro-posed Model	**Feature Optimization + Machine Learning**	**Dataset-1**	**With Feature Reduction**	**SVM , LR**	**98% , 99%**
				RF , DT	**100% ,100%**
			Without Feature Reduction	**SVM , LR**	**99% , 98%**
				RF , DT	**100% ,100%**
		Dataset-2	**With Feature Reduction**	**SVM , LR**	**99.19% , 99.48 %**
				RF , DT	**100% ,100%**
			Without Feature Reduction	**SVM , LR**	**99.89% , 99.50%**
				RF , DT	**100% ,100%**
		Dataset-3	**With Feature Reduction**	**SVM , LR**	**99.09% , 99.40%**
				RF , DT	**100% ,100%**
			Without Feature Reduction	**SVM , LR**	**99.13% , 99.04%**
				RF , DT	**100% ,100%**
		Dataset-4	**With Feature Reduction**	**SVM , LR**	**87.60% , 98.75%**
				RF , DT	**100% ,100%**
			Without Feature Reduction	**SVM , LR**	**99.61% , 88.80%**
				RF , DT	**98.79% , 98.50%**

5. Conclusion

The paper presents the utilization of four machine learning (ML) algorithms, namely DT, SVM, RF, and LR, for detecting DRDoS attacks. Additionally, the PCA technique is employed for feature reduction. Both without feature reduction and with PCA-based feature reduction are explored for optimal results and time efficiency. Evaluation metrics such as accuracy, precision, F1-score, and recall are employed to assess the performance of each model. Experimental findings reveal that RF and DT algorithms outperform SVM and LR, achieving a detection accuracy of 100% and consistent F1 scores, except for Dataset-4. Notably, the focus of the paper lies solely on detecting DRDoS attacks without proposing prevention strategies.While the models perform well in an experimental setting, the paper does not address the challenges of real-time detection, including the computational cost and scalability of implementing these algorithms in large-scale networks. The study primarily focuses on DT, RF, SVM, and LR, potentially overlooking other machine learning or deep learning models that might offer better performance or resilience against DRDoS attacks. Potential areas of future research could include creating and evaluating the suggested models' real-time application. To handle massive amounts of network traffic, this might entail evaluating their scalability, latency, and computational efficiency in a production setting, maybe with the help of distributed computing systems or streaming data frameworks. Future studies might investigate the application of sophisticated deep learning models, like Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs), which have demonstrated promise in other areas of network security, in order to overcome the drawback of concentrating on a small number of machine learning models. Furthermore, ensemble learning techniques that combine multiple algorithms could be studied to enhance detection performance and robustness.

Authors Contributions

All authors were involved in the design, analysis, writing, and revision of this research. Furthermore, all authors have reviewed and approved the final version of the manuscript for submission.

Acknowledgements

Special thanks are extended to all the authors for their invaluable contributions and unwavering support, which have been instrumental in the success of this remarkable research endeavor.

Conflict of Interest

No conflicting financial or non-financial interests are disclosed by the authors.

Declaration of DRDoS attack detection in the Writing Process:

The writers used ChatGPT and Grammarly to enhance the work's language and readability while it was being prepared. Following their use of this tool or service, the authors assumed full responsibility for the publication's content and reviewed and edited it as necessary.

Data Availability

Data are available at the link: https://www.unb.ca/cic/datasets/index.html

REFERENCES

1. R. R. Nuiaa, S. Manickam, A. H. Alsaeedi, and E. S. Alomari, "A new proactive feature selection model based on the enhanced optimization algorithms to detect drdos attacks," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 2, p. 1869, 2022.
2. H. Tsunoda, Y. Nemoto, K. Ohta, and A. Yamamoto, "A simple response packet confirmation method for drdos detection," in *2006 8th International Conference Advanced Communication Technology*, vol. 3. IEEE, 2006, pp. 5–pp.
3. K. M. Shayshab Azad, N. Hossain, M. J. Islam, A. Rahman, and S. Kabir, "Preventive determination and avoidance of ddos attack with sdn over the iot networks," in *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, 2021, pp. 1–6.
4. M. H. Khairi, S. H. Ariffin, N. A. Latiff, A. Abdullah, and M. Hassan, "A review of anomaly detection techniques and distributed denial of service (ddos) on software defined network (sdn)," *Engineering, Technology & Applied Science Research*, vol. 8, no. 2, pp. 2724–2730, 2018.
5. A. Rahman, M. S. I. Khan, A. Montieri, M. J. Islam, M. R. Karim, M. Hasan, D. Kundu, M. K. Nasir, and A. Pescapè, "Blocksd-5gnet: Enhancing security of 5g network through blockchain-sdn with ml-based bandwidth prediction," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 4, p. e4965, 2024.
6. F. J. Ryba, M. Orlinski, M. Wählisch, C. Rossow, and T. C. Schmidt, "Amplification and drdos attack defense–a survey and new perspectives," *arXiv preprint arXiv:1505.07892*, 2015.
7. Y. A. Bekeneva and A. V. Shorov, "Simulation of drdos-attacks and protection systems against them," in *2017 XX IEEE International Conference on Soft Computing and Measurements (SCM)*. IEEE, 2017, pp. 165–167.
8. W. Zhijun, X. Qing, W. Jingjie, Y. Meng, and L. Liang, "Low-rate ddos attack detection based on factorization machine in software defined network," *IEEE Access*, vol. 8, pp. 17 404–17 418, 2020.
9. Y. Bekeneva, N. Shipilov, and A. Shorov, "Investigation of protection mechanisms against drdos attacks using a simulation approach," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Springer, 2016, pp. 316–325.
10. D. Kundu, M. M. Rahman, A. Rahman, D. Das, U. R. Siddiqi, M. G. R. Alam, S. K. Dey, G. Muhammad, and Z. Ali, "Federated deep learning for monkeypox disease detection on gan-augmented dataset," *IEEE Access*, 2024.
11. A. D. Olaniyi, R. Christoph, S. A. Simon, A. A. Taofeek, and B. S. Badmus, "Resolving drdos attack in cloud database service using common source ip and incremental replacement strategy," in *Proceedings of SAI Intelligent Systems Conference*. Springer, 2016, pp. 725–737.
12. I. M. Tas, B. G. Unsalver, and S. Baktir, "A novel sip based distributed reflection denial-of-service attack and an effective defense mechanism," *IEEE Access*, vol. 8, pp. 112 574–112 584, 2020.
13. K. Subramani, R. Perdisci, and M. Konte, "Ixmon: detecting and analyzing drdos attacks at internet exchange points," *arXiv preprint arXiv:2006.12555*, 2020.
14. R. R. Nuiaa, S. Manickam, and A. H. Alsaeedi, "Distributed reflection denial of service attack: A critical review," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 6, p. 5327, 2021.
15. X. Chen, W. Feng, Y. Ma, N. Ge, and X. Wang, "Preventing drdos attacks in 5g networks: a new source ip address validation approach," in *GLOBECOM 2020-2020 IEEE global communications conference*. IEEE, 2020, pp. 1–6.
16. R. Xu, J. Cheng, F. Wang, X. Tang, and J. Xu, "A drdos detection and defense method based on deep forest in the big data environment," *Symmetry*, vol. 11, no. 1, p. 78, 2019.
17. H. Fujinoki, "Cloud-base defense against drdos attacks," in *2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*. IEEE, 2018, pp. 1–2.
18. M. Aupetit, Y. Zhauniarovich, G. Vasiliadis, M. Dacier, and Y. Boshmaf, "Visualization of actionable knowledge to mitigate drdos attacks," in *2016 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE, 2016, pp. 1–8.
19. Y. Gao, Y. Feng, J. Kawamoto, and K. Sakurai, "A machine learning based approach for detecting drdos attacks and its performance evaluation," in *2016 11th Asia Joint Conference on Information Security (AsiaJCIS)*. IEEE, 2016, pp. 80–86.
20. P. M. Priya, V. Akilandeswari, S. M. Shalinie, V. Lavanya, and M. S. Priya, "The protocol independent detection and classification (pidc) system for drdos attack," in *2014 International Conference on Recent Trends in Information Technology*. IEEE, 2014, pp. 1–7.
21. H. Tsunoda, K. Ohta, A. Yamamoto, N. Ansari, Y. Waizumi, and Y. Nemoto, "Detecting drdos attacks by a simple response packet confirmation mechanism," *Computer Communications*, vol. 31, no. 14, pp. 3299–3306, 2008.
22. C. Liu, G. Xiong, J. Liu, and G. Gou, "Detect the reflection amplification attack based on udp protocol," in *2015 10th International Conference on Communications and Networking in China (ChinaCom)*. IEEE, 2015, pp. 260–265.
23. R. Rani and A. Vatsa, "Card (continuous and random dropping) based drdos attack detection and prevention techniques in manet," *International Journal of Engineering and Technology*, vol. 2, no. 8, pp. 1449–1456, 2012.
24. I. M. Tas and S. Baktir, "A novel approach for efficient mitigation against the sip-based drdos attack," *Applied Sciences*, vol. 13, no. 3, p. 1864, 2023.
25. A. Rahman, M. Hossain, G. Muhammad, D. Kundu, T. Debnath, M. Rahman, M. Khan, S. Islam, P. Tiwari, S. S. Band *et al.*, "Federated learning-based ai approaches in smart healthcare: concepts, taxonomies, challenges and open issues," *Cluster Computing*, pp. 1–41, 2022.
26. S. I. Khan, A. Shahrior, R. Karim, M. Hasan, and A. Rahman, "Multinet: A deep neural network approach for detecting breast cancer through multi-scale feature fusion," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 6217–6228, 2022.
27. M. Hasan, A. Rahman, M. R. Karim, M. S. I. Khan, and M. J. Islam, "Normalized approach to find optimal number of topics in latent dirichlet allocation (lda)," in *Proceedings of International Conference on Trends in Computational and Cognitive Engineering*. Springer, 2021, pp. 341–354.
28. S. Islam, U. Sara, A. Kawsar, A. Rahman, D. Kundu, D. D. Dipta, A. R. Karim, and M. Hasan, "Sgbba: An efficient method for prediction system in machine learning using imbalance dataset," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 3, 2021.

29. M. J. Islam, A. Rahman, S. Kabir, M. R. Karim, U. K. Acharjee, M. K. Nasir, S. S. Band, M. Sookhak, and S. Wu, "Blockchain-sdn-based energy-aware and distributed secure architecture for iot in smart cities," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3850–3864, 2022.
30. L. Berti-Equille and Y. Zhauniarovich, "Profiling drdos attacks with data analytics pipeline," in *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*, 2017, pp. 1983–1986.
31. A. Alfraih Abdulaziz Nasser and W. B. Chen, "Ntp drdos attack vulnerability and mitigation," in *Applied Mechanics and Materials*, vol. 644. Trans Tech Publ, 2014, pp. 2875–2880.
32. B. A. Sassani, C. Abarro, I. Pitton, C. Young, and F. Mehdipour, "Analysis of ntp drdos attacks' performance effects and mitigation techniques," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 421–427.
33. S. Mahdavifar, N. Maleki, A. H. Lashkari, M. Broda, and A. H. Razavi, "Classifying malicious domains using dns traffic analysis," in *2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. IEEE, 2021, pp. 60–67.
34. M. S. I. Khan, N. Islam, J. Uddin, S. Islam, and M. K. Nasir, "Water quality prediction and classification based on principal component regression and gradient boosting classifier approach," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 4773–4781, 2022.
35. M. S. I. Khan, A. Rahman, T. Debnath, M. R. Karim, M. K. Nasir, S. S. Band, A. Mosavi, and I. Dehzangi, "Accurate brain tumor detection using deep convolutional neural network," *Computational and Structural Biotechnology Journal*, vol. 20, pp. 4733–4745, 2022.
36. T. Debnath, M. M. Reza, A. Rahman, A. Beheshti, S. S. Band, and H. Alinejad-Rokny, "Four-layer ConvNet to facial emotion recognition with minimal epochs and the significance of data diversity," *Scientific Reports*, vol. 12, no. 1, p. 6991, dec 2022.