DETECTION OF DDoS ATTACK USING MACHINE LEARNING TECHNIQUES

Table of Contents

Title	Page No.
Bona-fide Certificate	i
Declaration	ii
Acknowledgements	iii
Abstract	iv
List of Figures	viii
Abbreviations	ix
1. Introduction	1
1.1. DDOS vs DOS	3
1.2. Dataset	5
1.3. Practical Applications	7
2. Related Works	
2.1. Literature review	8
2.2. Evaluation metrics	9
3. Methodology	
3.1. Why Machine learning	11
3.2. Supervised Machine learning algorithms	12
3.3. Workflow	13
3.2.1. Naïve bayes	15
3.2.2. K Nearest Neighbor	16
3.2.3. Random forest	17
4. Results and Discussion	23
5. Conclusions and Further Work	27
6. References	28
7. Appendix	
Similarity Check Report	29

List of Figures

Figure No.	Title	Page No
1	DDOS attack	1
2	DDOS verses DOS	3
3	Cicflowmeter-live packets	6
4	Confusion matrix	9
5	Types of Machine learning techniques	11
6	Types of Supervised learning	12
7	Workflow	13
8	KNN	16
9	Random forest	18
10	No. of features does not contain NULL values	23
11	Total NULL values in each features	24
12	No. of Benign labeled rows and DDOS labeled rows	24
13	Performance metrics of Random Forest	25
14	Performance metrics of Naïve Bayes	25
15	Performance metrics of KNN	26
16	Comparision of performance metrics	26

ABBREVIATIONS

1. DDoS - Distributed Denial of Service
2. DoS - Denial of Service
3. IoT - Internet of Things
4. IDPS - Intrusion Detection and Prevention Systems
5. CDNs - Content Delivery Networks
6. IDS - Intrusion Detection Systems
7. KNN - K Nearest Neighbor
8. NAN - Not a Number

CHAPTER 1
INTRODUCTION

The Internet is omnipresent today. By using different forms of networks, the systems communicate with one another. A network can be defined as n computers, routers, and other devices. A network can have both legitimate & criminal users (i.e) Hackers. The individual who illegally gets and steals another person's data is known as a hacker. For that, a hacker has a number of options. Attacks fall into two categories: active and passive. In a passive assault, the hackers simply observe and evaluate all the data without altering any resources. However, hackers also modify data as part of active attacks, and they prevent people from acting. One of the most well-known and significant current attacks nowadays is the Distributed Denial of Service (DDoS) attack. As seen in Fig. 1, DDoS attacks are a persistent attack that overwhelm servers and systems on the network by flooding packets or requests into the system. There might only be a very small number of people on the network nowadays because of its massive size. It becomes exceedingly challenging to determine who is the hacker and who is a legitimate user. As technology develops, so do the methods employed to produce DDoS attacks.

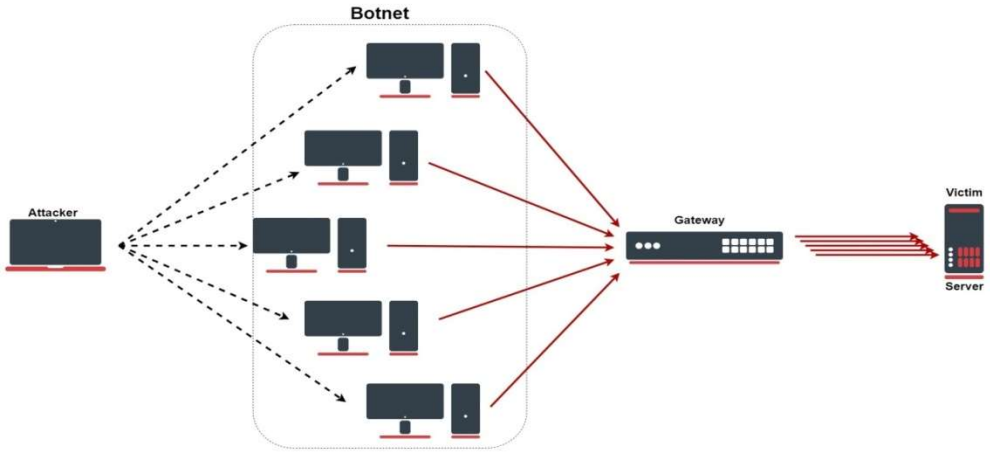


Fig 1: DDoS attack

The primary purpose of a DDoS attack is to flood a targeted system with traffic in order to overload its bandwidth or resources and prevent it from functioning normally.

Unlike traditional Denial of Service (DoS) attacks, which start with a single infected device, DDoS attacks involve a network of infiltrated devices known as a botnet.These hacked devices, sometimes called "zombies," can be PCs, servers, Internet of Things (IoT) devices, or even cellphones that have been unintentionally brought under the attacker's control by exploiting holes or infecting malware.

The distribution nature of the DDoS attacks is one of its key characteristics, which makes it difficult to cope with. The Miscreant can increase the intensity and scale of their attacks through coordinated attacks from a variety of sources, often occurring in different geographic areas. In addition, the use of botnets provides attackers with a degree of deniability and anonymity which makes it difficult to track down and identify those who are responsible.DDoS attacks can be carried out for a variety of reasons, such as political campaigns, monetary gains, or even cyberwarfare. DDoS attacks are a method used by hacktivist groups to express disapproval of governments or organizations and to protest against them. DDoS attacks may be started by criminal groups as a part of extortion schemes, with the attackers demanding ransom payments to stop the attack. The impact of DDoS attacks may be severe and extensive, extending beyond immediate financial losses to include reputational damage, legal liabilities, and regulatory consequences. A brief interruption of service can lead to significant revenue losses and erode customer confidence for businesses relying on online services, such as e-Commerce Platforms or Cloud Based Applications. Additionally, DDoS attacks pose a greater risk to vital infrastructure sectors like banking, healthcare, and utilities since interruptions to these services can have a domino effect on public safety and wellbeing. It takes a multifaceted strategy that includes preventative measures, reliable infrastructure, and coordinated response mechanisms to mitigate the threat posed by DDoS attacks. To filter out malicious traffic and lessen the impact of attacks, organizations can implement firewalls, rate-limiting strategies, and Intrusion Detection and Prevention systems (IDPS).Cloud-based DDoS protection services or Content Delivery Networks (CDNs) can also be used to spread and absorb incoming traffic, lessening the impact on specific resources.

Effective DDoS defense tactics, however, also need to include incident response procedures and cooperation with law enforcement and other industry players. Adaptive response systems, threat intelligence exchange, and real-time monitoring are essential for the timely identification and mitigation of DDoS attacks. Furthermore, by reducing the possibility of insider threats or human error, developing a culture of cybersecurity awareness and funding employee training can strengthen an organization's resistance against DDoS attacks. To summarize, DDoS attacks represent a serious risk to the integrity and availability of internet networks and services. In order to protect themselves from and lessen the effects of DDoS attacks, organizations must comprehend the nature of these attacks and put in place the necessary security measures.

1.1 DDOS verses DOS:

While both DDoS and DoS attacks aim to maliciously interfere with the availability of a specific system or network, they differ greatly in how they are carried out and how they affect the target. Using weaknesses, a single source floods the target with traffic, overwhelming its resources in a DoS attack. Since this traffic usually comes from a single source or a limited number of sources, it is easier to detect and reduce. A DDoS attack, on the other hand, entails a number of infected devices working together to overwhelm the target with traffic.

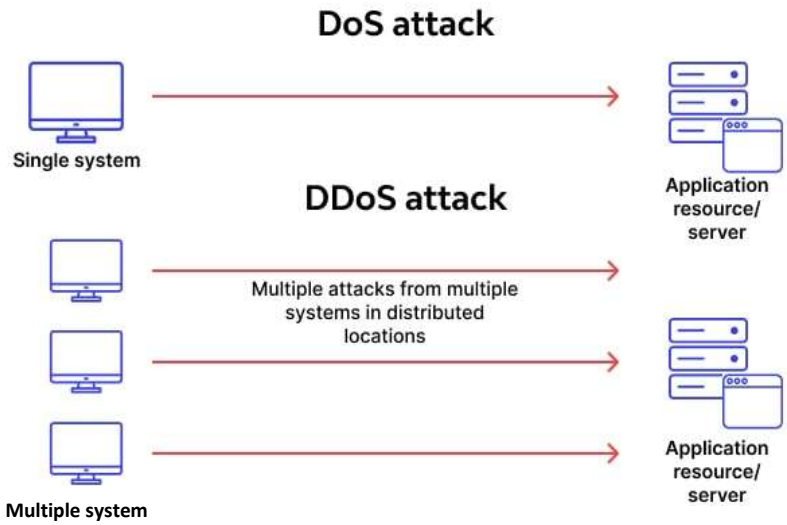


Fig 2 : DDoS verses DoS

By establishing a botnet, these devices spread the attack over multiple geographic regions, making it difficult to identify and stop. DDoS attacks can be more intense and large-scale than DoS attacks because of the botnet's combined processing power. As a result, DDoS attacks frequently cause targeted organizations to experience more severe interruptions, extended downtime, and large financial losses in addition to possible legal consequences and reputational harm. Although the goal of both kinds of attacks is to prevent authorized usersfrom accessing a system, DDoS attacks create a more complicated and formidable challenge that must be successfully countered with sophisticated mitigation techniques and industry-wide cooperation.An intentional attempt to overload a specific server, service, or network with unsanctioned traffic in order to prevent it from functioning normally is known as a denial-of-service (DoS) or distributed denial-of-service (DDOS) assault. By prohibiting authorized users from accessing the target, these attacks seek to interfere with operations and perhaps result in financial losses.

DDoS attacks come in a variety of forms, including:

Volume based Attacks:

These attacks use a large amount of traffic to overwhelm the target as shown in Fig 2, like in the case of a DDoS attack, which uses several hacked systems to launch the attack at once. The target's resources may be overloaded by the sheer volume of traffic, rendering it unreachable.

Protocol-based attacks:

These attacks take use of holes in network protocols to burn up too much server power or break network devices. A SYN flood attack, for instance, ties up resources and blocks valid connections by sending a lot of SYN requests to a target.

Application layer attacks:

These attacks focus on particular services or apps that are operating on the server that is the target. Since they imitate genuine traffic, they are frequently more sophisticated and challenging to identify. Attacks like Hyper Text Transfer Protocol(HTTP) flooding and Slowloris, which try to deplete server resources by maintaining connections open for as long as possible, are two examples. DoS attacks can result in downtime, lost revenue, reputational damage, and even data breaches if hackers take advantage of the confusion to access systems without authorization. Various measures can be implemented by companies to lessen the impact of DoS attacks.

Network Security: Intrusion detection/prevention systems, firewalls, and load balancers are examples of network security tools that can be used to filter and control incoming traffic in order to spot and stop dangerousrequests.

DDoS mitigation services: They are experts at identifying and thwarting DDoS attacks. They frequently do this by combining traffic redirection, rate limitation, and network traffic analysis techniques.

Application security: It can be defended against by employing web application firewalls, applying secure coding techniques, and routinely upgrading and patching software.

Traffic analysis and monitoring: By tracking and examining patterns in network traffic, one can quickly identify abnormalities that point to a DoS attack.

To sum up, DoS and DDOS attacks are a serious risk to enterprises, so it's critical to have strong security measures in place to identify, lessen, and stop them from interfering with business activities.In conclusion, DDoS and DoS attacks both seek to impede the availability of networks or services, but because DDoS operations are spread and include numerous hacked devices, they are more complex, well planned, and challenging to counter.

1.2 Dataset

The CSE-CIC-IDS2019 dataset is used to do in-depth cybersecurity research and evaluation in the field of network intrusion detection systems (IDS). It was developed by the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick. This dataset aims to specifically address the need for realistic and diverse data to evaluate the effectiveness of intrusion detection techniques, particularly in the context of cyber threats such as denial-of-service attacks. In contrast to synthetic datasets, the dataset is more reflective of real network behavior because it is made up of real network traffic data that was taken from a virtualized network environment. The dataset is large, with millions of network flow records and hundreds of attributes retrieved from payload information and packet headers. Researchers can use this massive dataset to train and assess machine learning models on huge quantities of data. In order to distinguish between malicious activity and regular behavior, ground truth information is appended to each network flow record in the dataset.

This labeling makes supervised learning methods for creating intrusion detection models easier to implement. Numerous details derived from network traffic are included in the dataset, such as protocol type, packet timings, source IP addresses, destination IP addresses, port numbers, and packet sizes. These characteristics offer useful data for developing machine learning models that identify unusual or malicious activity. Totally twenty one features are used for the demonstration. These includes 'Fwd Packet Length Min', 'Flow IAT Max', 'ACK Flag Count', 'Flow Duration', 'Average Packet Size', 'Init_Win_bytes_backward', 'Init_Win_bytes_forward', 'Total Length of Fwd Packets', 'Fwd IAT Max', 'Fwd IAT Mean', 'Fwd Header Length', 'Fwd Packet Length Std', 'Label', 'Fwd Packet Length Max', 'Min Packet Length', 'Packet Length Std', 'Max Packet Length', 'SubflowFwd Bytes', 'Flow IAT Mean', 'Total Length of Bwd Packets', 'Fwd Packets/s'.There are two categories in this dataset. In the dataset, 20% is used for testing and the remaining 80% is for training. Three machine learning algorithms K-Nearest Neighbor (KNN), Naïve Bayes, and Random Forest are used for training. It is discovered that, in comparison to the other algorithms, random forest has a high accuracy.

A program called CICFlowMeter was created specifically for flow-based network traffic analysis in cybersecurity applications as shown in Fig 3. Its main objective is to collect and evaluate network flow data which is comprised of details about network device communication sessions as quickly and effectively as possible. By analyzing flow data in real time or from archived datasets, CICFlowMeter seeks to provide insights into network traffic patterns, abnormalities, and security issues. Dedicated flow collectors, routers, switches, and other network monitoring equipment provide the flow data that CICFlowMeter gathers.

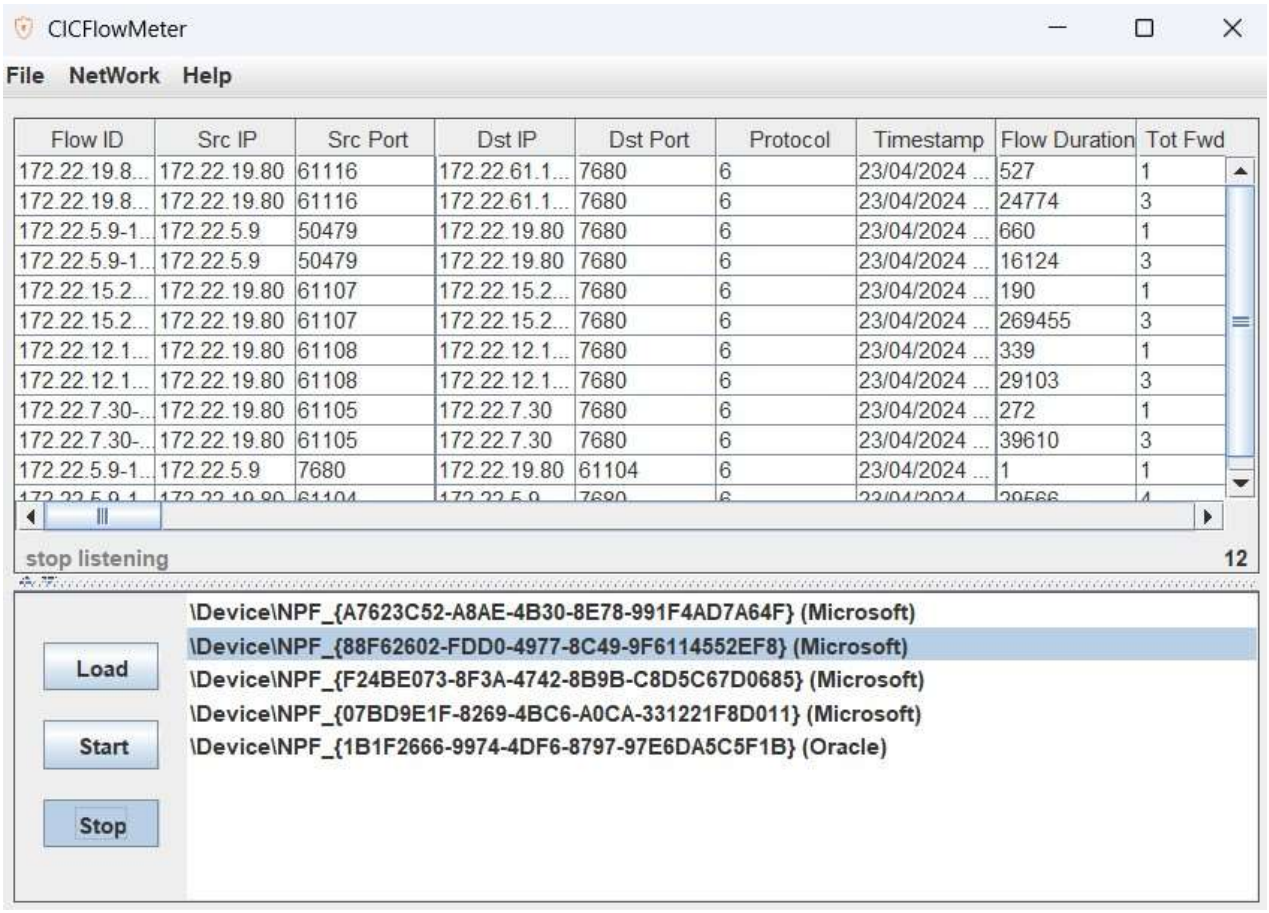


Fig 3 : Cicflowmeter-live packets

It is compatible with multiple flow protocols, such as sFlow, IPFIX, NetFlow, and others. The application analyses flow data to extract relevant details, including timestamps, protocol types, source IP addresses destination IP addresses, port numbers, packet and byte counts, and packet counts.

These characteristics are employed in anomaly identification and traffic analysis.Network traffic anomalies, such as odd patterns, sudden increases in traffic volume, or departures from typical behavior, can be found using the algorithms in CICFlowMeter. Potential security incidents, such as DDoS attacks canbe indicated by these anomalies. It produces a dataset consisting of desired features.

1.3 Practical Applications

The use of DDoS attacks is quite common in both malicious and non-malicious scenarios. DDoS attacks are frequently used maliciously to obstruct websites, network infrastructure, and online services from being accessible. DDoS attacks are used by cybercriminals to overload systems with traffic, making them unusable for authorized users. Financial losses, harm to one's reputation, and interruption of vital services are possible outcomes of this. Furthermore, DDoS attacks can be used in extortion schemes, in which the attackers threaten to conduct a DDoS attack until they get a ransom. But not every DDoS attack is malicious. Organizations occasionally carry out DDoS stress testing to evaluate how secure their infrastructure and networks are against simulated attacks. Organizations can improve their resilience against actual attacks by implementing mitigation measures, optimizing network setups, and identifying vulnerabilities by purposefully exposing their systems to DDoS traffic. DDoS attacks have also been employed in activism and protest movements as a digital form of protest to bring attention to social or political concerns or to interfere with the operations of targeted businesses. DDoS attacks are a serious cybersecurity issue, despite their wide range of uses. Proactive steps must be taken to identify, lessen, and stop their effects on online services and infrastructure. Cybercriminals frequently use DDoS attacks to interfere with websites, internet services, and corporate operations. Attackers may aim to inflict monetary losses, harm to their reputation, or disruptions in service to e-commerce platforms, financial institutions, gaming servers, or government websites. DDoS attacks are a topic of study and investigation for cybersecurity professionals. To improve defenses and countermeasures against future attacks, researchers examine attack methods, mitigation mechanisms, and the effects of DDoS attacks on network infrastructure.DDoS attacks are generally used for a variety of goals, from legal testing and research purposes to malevolent actions intended to cause harm or financial benefit. Nevertheless, DDoS attacks require strong defenses and proactive mitigation strategies since they constitute a serious danger to the availability and integrity of online services and infrastructure, regardless of their motivation.

Distributed servers situated in several geographical locations are utilized by material CDNs to effectively distribute material to users. For the goal of managing traffic, CDNs can use DDoS techniques. Through the analysis of inbound traffic patterns and the dynamic modification of server routing, content delivery networks (CDNs) are able to distribute traffic in a way that minimizes the effects of abrupt spikes in traffic or surges in demand.It is difficult for telecommunication networks to control congestion during periods of high usage or in the event of unexpected increases in traffic, like during significant events or emergencies.

CHAPTER 2
RELATED WORKS

2.1 Literature Review

i. Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning.Francisco Sales de Lima Filho, Frederico A. F. Silveira, Genoveva Vargas-Solar.The Smart Detection system, an online method for detecting DoS/DDoS attacks, has been introduced in this article. Based on samples collected directly from network devices by the sFlow protocol, the software use the Random Forest Tree method to categorize network traffic. The suggested system was able to identify different kinds of DoS/DDoS assaults, including TCP flood, UDP flood, HTTP flood, and HTTP slow, based on the evaluation of three intrusion detection benchmark datasets: CIC-DoS, CICIDS2017, and CSE-CIC-IDS2018.

ii. Implementation of Machine Learning Based DDOS Attack Detection System-IEEE 2022. Bhargava R, Dr. Yash Pal Singh,Dr. Nawanath S Narawade. Unlike rules-based approaches, the model is produced using a statistical model that modifies its behavior dependent on the input parameters specified in the training. This leads to the generation of output variables with a low percentage of misclassification, which improves model reliability and enables the detection of these behaviors. It was found that during the training phase, standardization and appropriate input parameter selection are directly related to a higher classification rate for both normal and anomalous requests.

iii. A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Akgun, D., Hizal, S. and Cavusoglu, U. This article's goal is to create a Deep Learning-based system that can accurately and frequently identify false-positive DDoS attack types. It enhanced the system by the use of preprocessing methods such feature selection and deletion. Compared to previous methods, the suggested CNN-based approach with its one-dimensional convolution layers yields more accurate and successful results.

iv. Machine Learning based DDOS Detection.S.Shanmuga Priya, M.Sivaram, A.Jayanthiladevi. Compared to previous methods, we can identify risks much more quickly and easily when we use a machine learning methodology. Three machine learning algorithms were employed in the proposal: Random Forest, KNN, and Naive Bayesian. Any kind of DDoS assault can be accurately and quickly detected.

2.2 Evaluation Metrics:

A number of assessment measures produced from the confusion matrix are frequently used to evaluate performance in the context of DDoS attack detection using machine learning models. These measurements shed light on how well the model differentiates between legitimate and malicious traffic.

Confusion Matrix:

An evaluation table that is frequently used to assess a classification model's performance is called a confusion matrix. The comparison between the model's predictions and the actual ground truth for each class is summarized in Figure 4. A confusion matrix usually comprises four elements in order to detect DDoS attacks using machine learning.

		Actual	
		Benign	Attack
Predicted	Benign	True Positive	False Positive
	Attack	False Negative	True Negative

Fig 4: confusion matrix

True Positives (TP): Example accurately assessed as normal (Benign).

True Negatives (TN): Examples properly classed as Attacks (DDOS).

False Positives (FP): Example misclassified as normal while it is actually under attack.

False Negatives (FN): Example misclassified as an attack when it is truly normal.

Accuracy:

Accuracy is defined as the proportion of correctly detected occurrencestrue positives and true negatives—out of all instances. It provides an overall assessment of the accuracy of the model.

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

Precision:

The percentage of real attack cases among all cases classified as attacks is determined by Precision. It demonstrates the accuracy of optimistic projections.

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

Recall:

Recall measures the proportion of actual assault instances that are correctly classified as attacks. It is also known as sensitivity or true positive rate (TPR). It demonstrates the model's ability to recognize attacks.

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

F1 Score:

The F1-score is defined as the harmonic mean of recall and precision. It allows for an equitable evaluation of a model's efficacy by accounting for both erroneous positives and incorrect negatives.

$$\text{F1 score} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

These assessment indicators provide several angles on the performance of the model and are frequently combined to produce an all-encompassing evaluation. Precision, recall, and F1-score are particularly significant metrics to take into account in the context of DDoS attack detection, where precisely identifying attacks while minimizing false alarms is critical. Furthermore, accuracy offers a broad measure of the model's correctness, but it should be used cautiously, particularly in datasets that are imbalanced and have a disproportionately high proportion of normal cases compared to attack instances.

CHAPTER 3

METHODOLOGY

3.1 Why Machine learning?

Machine learning is used in DDoS attack detection because of its capacity to quickly evaluate enormous volumes of network traffic data and identify patterns suggestive of malicious activity. The purpose of denial-of-service (DDoS) attacks is to overload a system or network with traffic so that authorized users are unable to utilize it. Because there are so many real communications, it is challenging for conventional attack detection techniques to accurately and swiftly detect these kinds of attacks. However, machine learning systems that have been taught to detect them can identify anomalous patterns in network traffic that are suggestive of DDoS attacks. By using variables like packet size, frequency, and source IP address, machine learning models may be able to distinguish between malicious and genuine traffic.This allows for early detection and timely reaction to reduce the effects of DDoS attacks. Furthermore, as time goes on, machine learning systems can adjust and change, enhancing their efficiency and accuracy in identifying novel and developing DDoS assault methods. All things considered, the use of machine learning in DDoS detection strengthens network resilience and helps in security against disruptive cyberthreats.

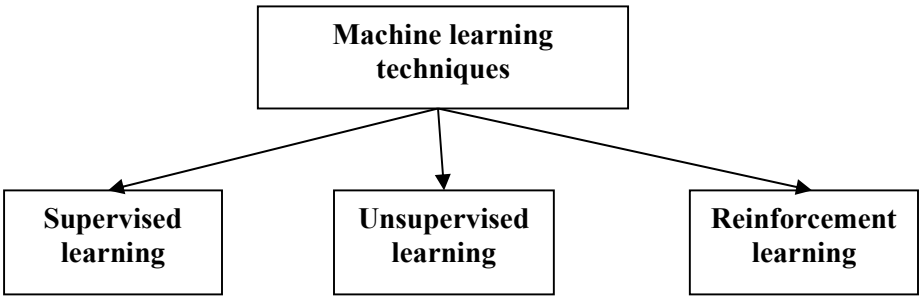


Fig5 : Types of Machine learning techniques

As illustrated in Fig. 5, machine learning can be roughly divided into three types. Reinforcement learning, supervised learning, and unsupervised learning are all included. In supervised learning, the computer can learn from labeled data by combining the input data with the right output.

Through training with labeled examples, the algorithm seeks to learn a mapping function from the input to the output.Unsupervised learning is the process of extracting knowledge from unlabeled data and looking for patterns or structures. Without explicit direction, the algorithm searches through the input data to uncover hidden patterns or clusters.Reward-maximizing actions over time teach an agent with reinforcement learning how to interact with its environment through trial and error. Thanks to supervised learning, the algorithm can distinguish between hostile and typical network traffic patterns, making it easier to classify DDoS attacks correctly. The program can learn from labelled data. For the purpose of detecting DDoS attacks, supervised learning is used.

3.2 Supervised Machine Learning Algorithms:

In the supervised learning model of machine learning, the algorithm is trained on labeled data, which is data that has been associated with labels for the appropriate output. As a result, the algorithm is able to predict outcomes for data that has not yet been observed by learning the correlation between input attributes and the intended output. Regression and classification are the two primary subtypes of supervised learning. Based on the input features, the algorithm predicts a class or categorical label for future occurrences in classification tasks, and a continuous value in regression tasks. Regression algorithms are used to estimate property prices based on features like square footage and location, whereas classification algorithms are employed when the result is discrete, such deciding if an email is spam or not. Among the methods used in supervised learning include Random Forest, KNN, decision trees, and Naïve Bayes's as shown in Fig6. These algorithms are extensively employed in many different fields, including as cybersecurity, image recognition, natural language processing, and medical diagnosis. They are also utilized in DDoS attack detection.

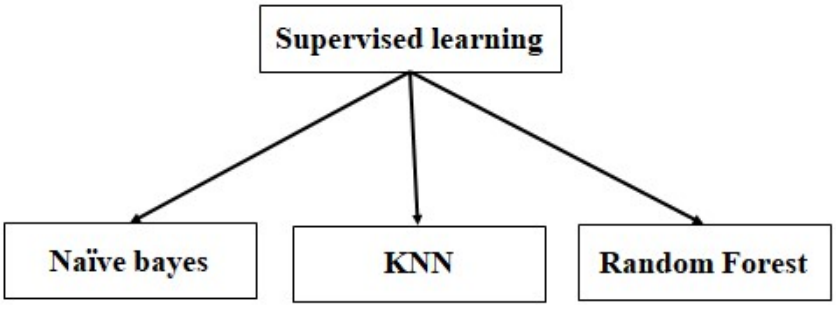


Fig 6 : Types of Supervised learning

3.3WORKFLOW

Raw Data Collection:

Gathering data directly from the source, devoid of any modification or processing, is referred to as "raw data collection."With this raw dataset, a machine learning model for DDoS attack detection can be created. Before using this raw data for model training or analysis, pre-processing may be necessary to extract pertinent characteristics and transform it into a format that machine learning algorithms may use as input.

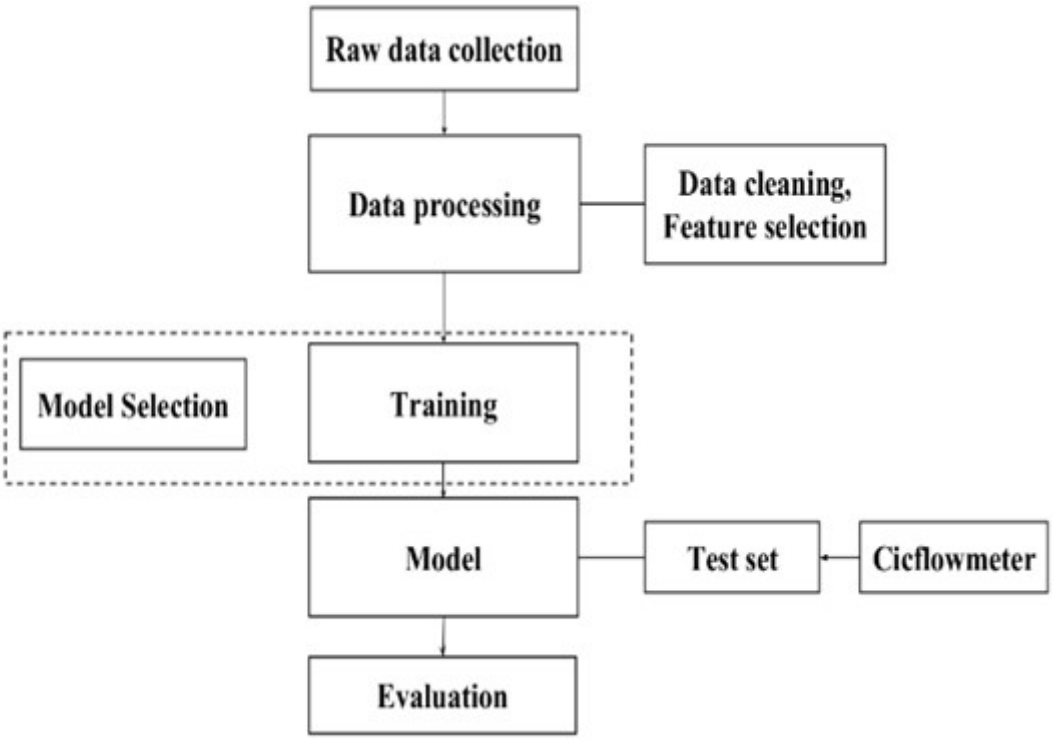


Fig 9 : Workflow

Data Processing:

Data preparation for DDoS attack detection involves many important steps in order to prepare the raw data for analysis using machine learning techniques. The pre-processing steps are summarized as follows:

- **Data Cleaning:**

To make sure that only the necessary information is used for analysis, remove any duplicate or unnecessary data items from the dataset. By taking this step, the dataset's quality is raised and noise is decreased.

- **Feature Selection:**

Selecting the most relevant features from the dataset that are essential for identifying DDoS attacks is known as feature selection. By taking this step, the dataset's dimensionality is decreased, machine learning algorithms operate better, and the results are easier to interpret. Among the methods employed in feature selection are: Feature Importance Ranking: This technique ranks features according to how important they are in predicting the target variable. It uses algorithms such as Random Forest or Gradient Boosting. Finding and eliminating characteristics that have a strong correlation with one another in order to avoid redundant information is known as correlation analysis.

Domain Knowledge: Using domain knowledge to choose features based on network traffic characteristics that are recognized to be the pertinent for detecting the DDoS attacks.

The effectiveness of machine learning algorithms can be greatly enhanced, resulting in more precise and effective detection of DDoS attacks in network traffic, by carefully choosing features that are most relevant to identifying DDoS attacks.

Data Splitting:

To evaluate the machine learning model's performance, divide the dataset into training and testing sets. The testing set is used to assess the model's performance after it has been trained using the training set. The raw data collected for DDoS attack detection can be transformed into a clean, organized dataset using these pre-processing approaches, ready for examination by machine learning algorithms.

Model Selection:

Model selection in DDoS attack detection refers to the process of choosing the optimal machine learning model for a task, taking into consideration variables like robustness, accuracy, and computational efficiency. The goal of the model selection process is to choose the model that most closely matches the requirements of the specific DDoS attack detection scenario.

3.3.1 Naïve Baye's:

Based on Bayes' theorem, the widely used probabilistic machine learning technique known as Naive Bayes relies on the "naive" assumption that each feature is independent of every other characteristic. Despite this simplification, Naive Baye's often performs well in classification tasks, especially for high-dimensional data sets like text categorization and spam filtering. It calculates the likelihood that a given instance belongs to each class based on the attributes that appear, and it selects the class with the highest probability as the predicted class. Naive Bayes is computationally efficient, resistant to irrelevant characteristics, and requires little training data.With real-world data, however, the independence assumption might not hold true, which occasionally could lead to less than optimal performance.There are numerous variations of Naive Baye's, including Gaussian, Multinomial, and Bernoulli varieties, each tailored to a certain type of data distribution. Naive Bayes, despite its simplicity, is a useful tool in many applications due to its speed, ease of use, and efficiency, especially when dealing with large datasets and limited processing resources.

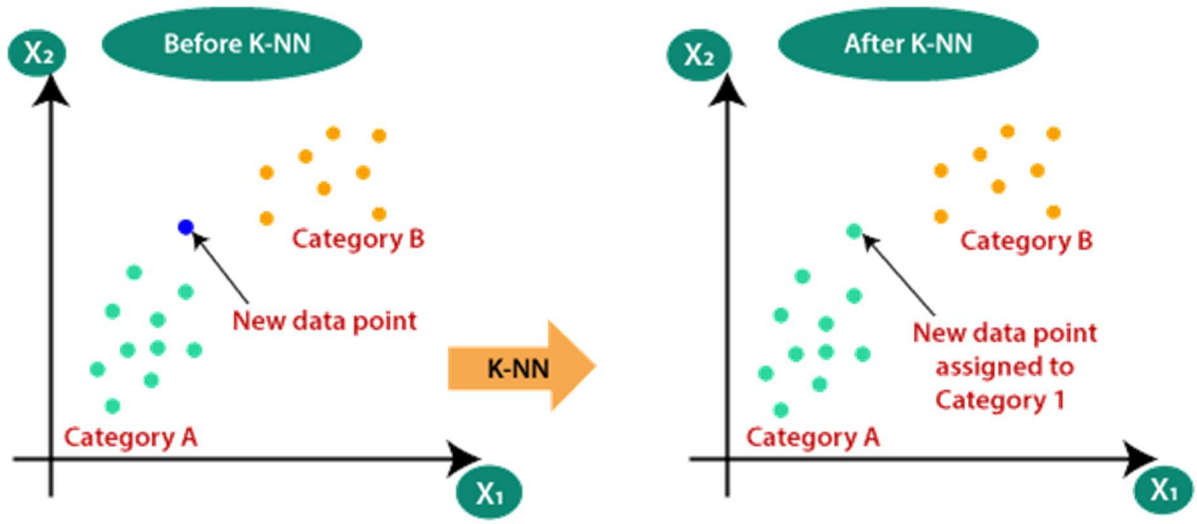
The Naive Bayes algorithm analyses network traffic characteristics including packet size, frequency, and source IP addresses to detect DDoS attacks. Based on these factors, it determines the likelihood that an observed traffic pattern belongs to the normal or attack category. Naive Bayes gains knowledge of the probability distribution of characteristics for each class through training on labeled datasets that include instances of both normal and attack traffic. By choosing the class with the highest probability during inference, it makes predictions about whether or not incoming traffic is suggestive of a DDoS attack. Even with its oversimplifying premise of feature independence, Naive Bayes is capable of accurately classifying DDoS attacks.

$$P(H\backslash E) = \frac{P(E\backslash H) * P(H)}{P(E)}$$

P(H\E) = Hypothesis's posterior probability assuming the veracity of the evidence
P(E\H) = Probability that the Hypothesis is True based on the Evidence
P(E) = Prior Probability that the evidence is True
P(H) = Prior Probability of the Hypothesis

3.3.2 K NEAREST NEIGHBOUR:

While it is not as popular as Random Forest,KNN is another machine learning method that can be utilized for DDoS attack detection. KNN is an easy to understand technique that uses the majority class of its KNN in the feature space to classify fresh data points.Based on the features extracted from the traffic, KNN can be used to categorize network traffic data as malicious or benign in the context of DDoS attack detection. The new data point's distance from every other data point in the training set is first determined by the algorithm, which then chooses the k closest neighbors. Next, a majority vote among the class labels of its KNN determines the class label of the new data point.



Category A : BENIGN Category B : DDOS

Fig 7 : KNN

KNN's simplicity and ease of implementation are two of its main benefits. It is an easy choice for quick and easy DDoS attack detection systems because it does not require the training step that is required for algorithms like Random Forest. Furthermore, KNN is a non-parametric algorithm, which might be useful for handling intricate and variable network traffic patterns because it makes no assumptions about the data's underlying distribution.KNN does, however, have significant limitations that could have an impact on how well it detects DDoS attacks. Its processing efficiency is one of its primary drawbacks, particularly when working with big datasets.

Because KNN calculates the distance between each new data point and every old data point in the training set (Fig. 7), it can be computationally expensive. This is particularly true for applications that require low latency in real-time.Furthermore, the performance of KNN may be affected by the choice of k value. When k is little, the approach may be underfitted—too simple, failing to recognize the underlying patterns in the data—while when k is large, the algorithm may be overfitted—too sensitive to noise in the data.

3.3.3 RANDOM FOREST :

Strong and flexible, Random Forest is a machine learning technique that may be used for both classification and regression issues. It belongs to the class of ensemble approaches, which combine multiple independent models to produce a more accurate and dependable final model. As illustrated in Fig. 8, the basic idea behind Random Forest is to build an enormous number of decision trees during training and then aggregate the forecasts from each tree to arrive at a final prediction. The model performs better overall and overfitting is lessened because to this aggregation method.The decision tree is the fundamental component of the Random Forest method. It is a straightforward but powerful model for decision-making based on input data. A decision tree is made up of nodes that represent feature qualities, edges that reflect the decision rules based on those characteristics, and leaf nodes that represent class labels or regression results. During the Random Forest training phase, several decision trees are created via a process called bootstrapping. By randomly picking the training data and using replacement, many subsets of the data are produced through the bootstrapping process. Subsequently, each decision tree is trained using these subsets.

By choosing a random subset of features at each decision tree node, Random Forest adds another degree of unpredictability on top of bootstrapping. Feature bagging is a technique that helps decorrelate the individual trees, strengthening the ensemble and reducing its susceptibility to overfitting. Random Forest outperforms a single decision tree in terms of accuracy and generalization performance by aggregating the predictions of several randomly generated decision trees.

To conclude this Random Forest is a strong and adaptable machine learning technique that works well for a variety of regression and classification applications. Data scientists and machine learning practitioners choose it because of its capacity to minimize overfitting, manage huge datasets, and offer feature importance estimations. Random Forest is a dependable and efficient technique to take into consideration, regardless of the complexity of the regression endeavor or the basic classification challenge you're working on.

RANDOM FOREST IN DDOS ATTACK:

Because Random Forest can manage the complicated and high dimensional nature of network traffic data, it is employed in DDoS attack detection. DDoS attack frequently involve a lot of malicious traffic that is hard to tell apart from good traffic. The ensemble of decision trees from Random Forest is a good fit for this purpose because it can capture the interactions and nonlinear correlations between the various network traffic parameters.

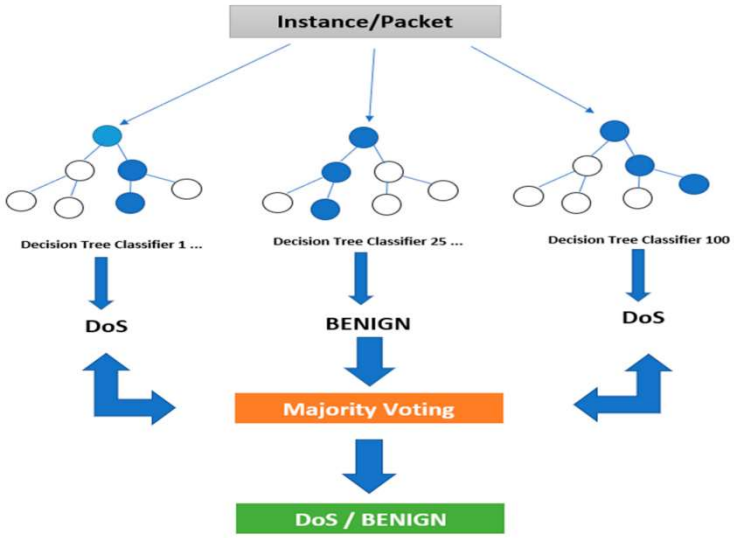


Fig 8 : Random forest

Random Forest's capacity to scale to big datasets is yet another important feature. Massive amounts of traffic data can be produced by DDoS attacks, and Random Forest is well-suited for real time traffic data analysis since it can manage enormous datasets. Random Forest helps to guarantee the availability and security of network services by swiftly detecting and mitigating DDoS attacks through the effective processing and analysis of network traffic data.

Training :

To develop classifiers for DDoS attack detection using Random Forest, KNN, and Naive Bayes.The dataset is divided into training and testing sets so that the model can be trained. While the testing set evaluates the model's performance on observed data, the training set teaches the model to identify patterns associated with DDoS attacks.All of the training cases and their labels would be stored in order to train the model for the KNN classifier. The model would locate the k-nearest neighbours in the training set and categorize a new instance by assigning the majority class label among those neighbours.During the training phase, a DDoS detection model goes through a rigorous learning process to distinguish between normal network traffic and DDoS attacks. This critical phase is feeding the model labeled samples from the training dataset, with each example being a snapshot of network traffic and a label indicating whether it is benign or malicious. Based on these examples, the model adjusts its internal parameters to reduce prediction errors, allowing it to learn to spot patterns in the data that indicate DDoS attacks. At the core of the training procedure is the model's capacity to extract meaningful characteristics from raw network traffic data.
These attributes could include of source and destination IP addresses, protocol type, packet size, packet rate, and other important details for differentiating between legitimate and malicious data. The model can be trained to recognize patterns that are typical of DDoS attacks but uncommon in regular traffic by examining these attributes.The model is trained iteratively by exposing it to batches of training examples; to enhance performance, the model's parameters are refined after each batch. An optimization algorithm, such gradient descent, guides this modification by updating the model's parameters in a way that minimizes the prediction error. The more times this procedure is repeated, the more proficient the model becomes at distinguishing between legitimate and malicious communications.

Performance of the model is monitored using a different validation dataset during the training phase. In doing so, you may make sure that the model can generalize to new samples successfully and does not overfit to the training set. The training procedure contributes to the development of a robust and effective DDoS detection model capable of reliably identifying DDoS attacks while minimizing false positives.It would calculate the probabilities of each feature occurring given each class label in the training set for the Naive Bayes classifier. The model would utilize these probabilities combined with the Bayes theorem to determine which class an instance would most likely belong to when categorizing it, and it would then assign the class with the highest likelihood.An ensemble of decision trees would be trained, with each tree being trained on a different subset of the data, in order to create the Random Forest classifier.

This group method enhances generalization and reduces overfitting.After training, the model can be used to categorize incoming network data in real-time. If the model detects patterns that resemble a DDoS attack and the required mitigation measures are placed in place, the network can be secured.

Output of Model Selection:

Random Forest frequently performs better in terms of accuracy and prediction performance than Naive Bayes and KNN when choosing a model for DDoS attack detection. When compared to Naive Bayes and KNN, Random Forest's ensemble learning method which aggregates the predictions of several decision trees usually yields more reliable and accurate results. When handling high-dimensional data, such network traffic features, Random Forest is especially well-suited since it can efficiently identify complicated patterns in the data. Furthermore, Random Forest is more dependable in real-world situations where the data may be noisy or incomplete than Naive Bayes and KNN because it is less impacted by outliers and noise in the data. All things considered, Random Forest is a good option for DDoS attack detection, providing reliable and accurate predictionscompared to Naive Bayes and KNN.Based on criteria like accuracy, precision, recall, and F1-score, evaluation of each of the three classifiers' performance on the testing set after training to see which one performs best at identifying DDoS attacks.

Testing:

CICFlowMeter is the tool to record and analyze real-time network traffic before capturing packets and turning them into a dataset for Random Forest model testing. In order to do this, CICFlowMeter must be configured to listen on the network interface where traffic is expected to be recorded. CICFlowMeter will evaluate the traffic and produce flow data as soon as it begins to capture live packets.

After that, transform these flow records into a format for a dataset that the Random Forest model can utilize as a test set. In order to do this, relevant data from the flow records, such as protocol type, packet size, and packet rate, are usually extracted and arranged into a structured format (such as CSV) that may be used as input for the Random Forest model.This final evaluation stage is critical for analyzing the model's performance in a real-world setting and predicting how well it will perform when deployed in a production context.

During the testing phase, the model is shown examples of network traffic that it has never seen before. These instances are labeled with their ground truth (i.e., whether they represent normal or attack traffic), but the model's predictions are not used to alter its parameters.

Rather, the test examples' classification accuracy is used to gauge the model's performance. The test dataset is typically large enough to provide a statistically relevant evaluation of the model's performance. Several performance indicators can be computed by comparing the ground truth labels in the test set with the predictions made by the model. Several metrics, including accuracy, precision, recall, and F1 score, shed light on various facets of the model's operation. Put another way, accuracy expresses the percentage of correctly identified cases in the test set relative to the total number of examples, hence revealing the model's overall accuracy. Out of all the positive predictions the model generates, precision indicates the percentage of real positive predictions (attacks that are properly identified). It demonstrates how well the model can stop erroneous alarms. The percentage of real positive cases in the test set that are true positive predictions is measured; it is also frequently referred to as sensitivity. It illustrates how the model can identify attacks.

The harmonic mean of recall and precision is used to compute the F1 score, a balanced measure of a model's performance. By analyzing these indicators, stakeholders can evaluate the model's ability to detect DDoS attacks and reduce false positives and false negatives. A high-performing model on the test set suggests that it would perform well in a production context, delivering dependable DDoS detection capabilities without affecting genuine network traffic.Lastly, it would feed this information into the Random Forest model as the test set, assessing how well it performed in real-time detection of attacks using DDoS.

Evaluation:

To evaluate the results whether the Random Forest model correctly identified the packets as benign or attacked.The binary result of each prediction is more important to this evaluation method than the overall performance of the model. For DDoS attack detection, the Random Forest model's performance is evaluated by comparing its predictions with the ground truth labels, using binary categories (attacked or benign). Rather than emphasizing overall model performance metrics like accuracy or F1 score, this strategy highlights how important it is to accurately identify the character of each packet.For every packet in the dataset, the truth labels and the model's classifications are compared in order to do this evaluation. The classification is considered accurate when the model predicts that a packet is under attack and the ground truth label validates this, or when the model predicts that a packet is benign and the ground truth label agrees. This shows that the character of the packet has been accurately determined by the model.

The model may be successful in accurately recognizing packets if it regularly agrees with the ground truth labels. Nevertheless, additional research is required to determine why the model might have incorrectly classified any packets if there are differences between the model's predictions and the ground truth labels.

It's crucial to remember that although though this assessment technique offers insightful information about the model's performance in binary classification, additional metrics like precision, recall, and F1 score should be taken into account for a more thorough analysis.

These metrics can offer more details about the model's effectiveness, like how well it reduces false positives—normal packets that are mistakenly identified as attacked—and false negatives—attacked packets that are mistakenly categorized as normal.In general, the accuracy of a Random Forest model in determining the type of each packet can be evaluated by analyzing its output for DDoS attack detection using binary classifications. This method offers a targeted assessment that can supplement other performance measures, resulting in a deeper comprehension of the model's capacity to identify DDoS attacks.The model's classifications and the ground truth labels which indicate whether or not each packet is genuinely under attack would be compared to examine the outcomes. When the model's prediction and the ground truth agree, the classification is accurate and the model has properly determined the packet's character.

CHAPTER 4
RESULTS AND DISCUSSION

Number of features does not contain NULL values:

It depicts the total number of features existing in the dataset that does not contain NULL value.Fig 10 shows that totally twenty one feature are of not - NAN(Not a Number) value and zero features are of NAN value.Not NAN and NAN values are represented by a binary number 0 and 1 respectively.

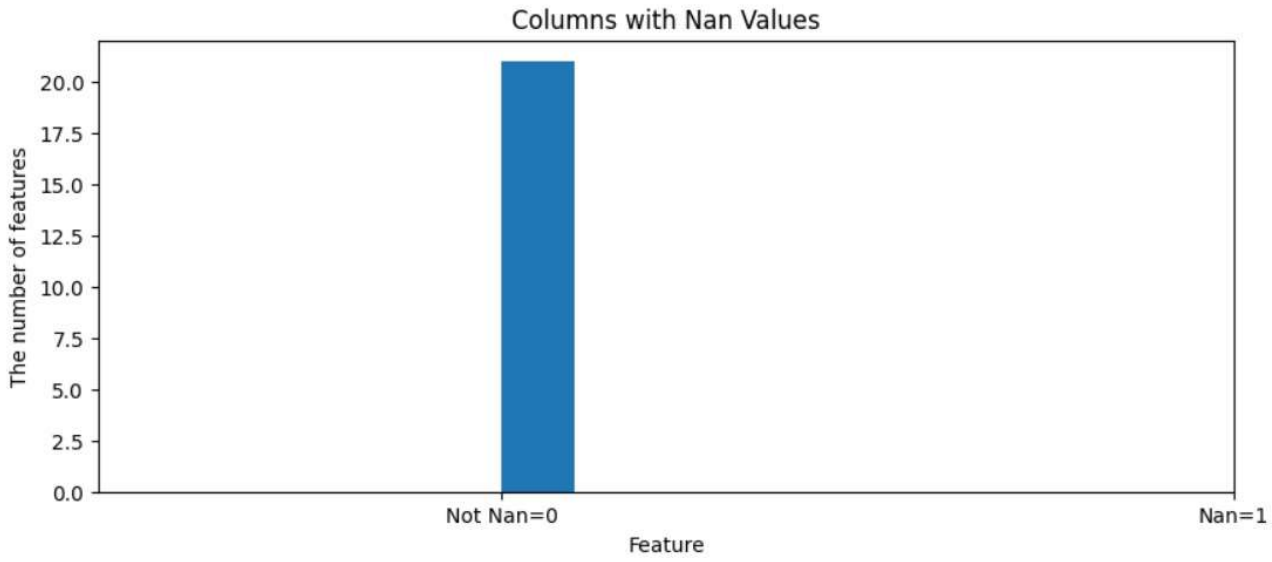


Fig 10 : Number of features does not contain NULL values

Total NULL values in each features:

Fig 11 depicts that, the features like'Fwd Packet Length Min', 'Flow IAT Max', 'ACK Flag Count', 'Flow Duration', 'Average Packet Size', 'Init_Win_bytes_backward', 'Init_Win_bytes_forward', 'Total Length of Fwd Packets', 'Fwd IAT Max', 'Fwd IAT Mean', 'Fwd Header Length', 'Fwd Packet Length Std', 'Label', 'Fwd Packet Length Max', 'Min Packet Length', 'Packet Length Std', 'Max Packet Length', 'SubflowFwd Bytes', 'Flow IAT Mean', 'Total Length of Bwd Packets', 'Fwd Packets/s'. does not contain any NAN values.

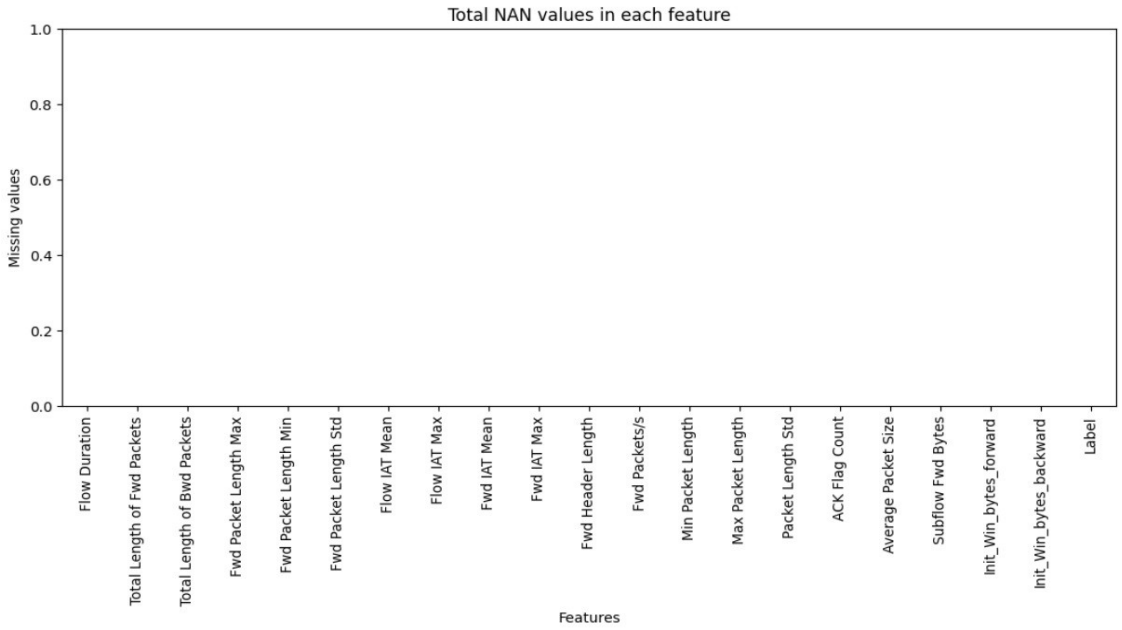


Fig 11: Total NULL values in each feature

No. of Benign labled rows and DDOS labled rows:

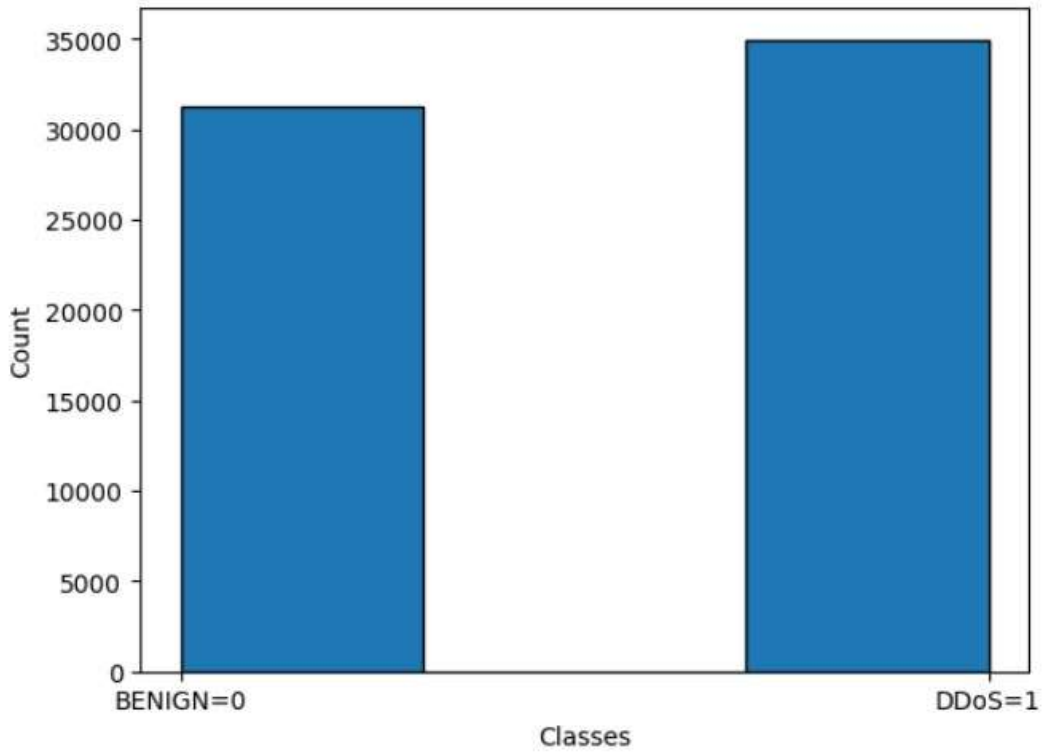


Fig 12 : No. of Benign labled rows and DDOS labled rows

The dataset totally contains 66,236 rows. Benign(normal packet) is represented by a binary number 0 and DDoS(attacked packet) is represented by a binary number 1. Fig 12 shows that, there are 31,284 Benign and 34,952 DDoS are there in the dataset.

Performance metrics of Random Forest:

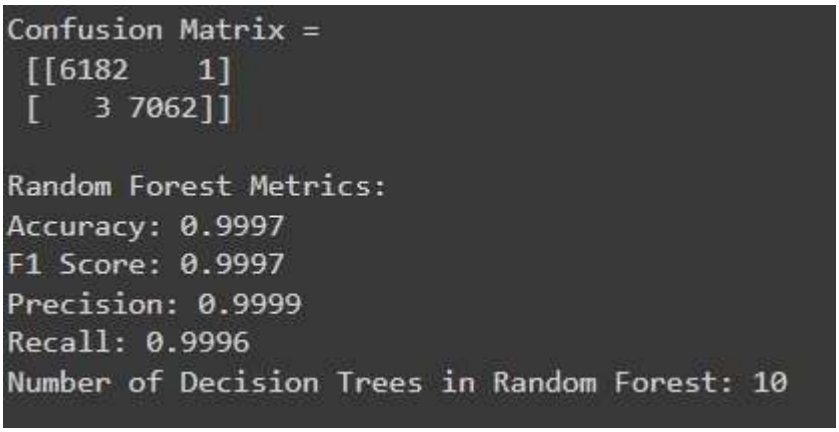


Fig 13 : Performance metrics of Random Forest

Performance metrics of Naïve Bayes:

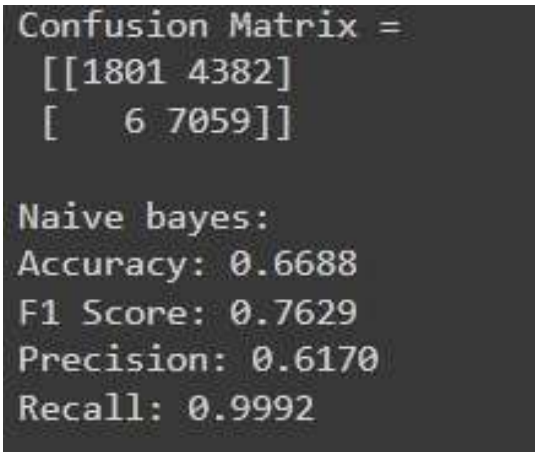


Fig 14 : Performance metrics of Naïve Bayes

Performance metrics of KNN:

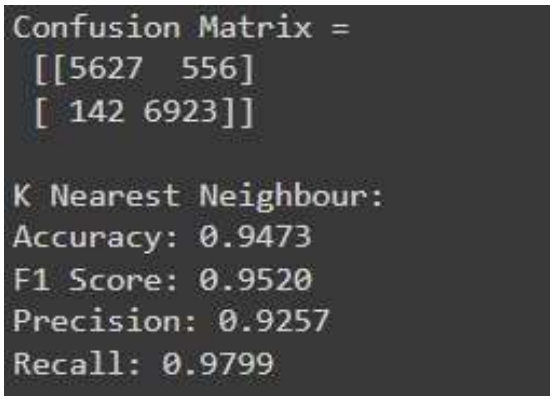


Fig 15: Performance metrics of KNN

Table 1: Comparision of performance metrics

Algorithms	Accuracy	F1 Score	Precision	Recall	Confusion Matrix
Random Forest	0.9997	0.9997	0.9999	0.9996	6182 1 3 7062
Naïve baye's	0.6688	0.7629	0.6170	0.9992	1801 4382 6 7059
K Nearest Neighbour	0.9473	0.9520	0.9257	0.9799	5627 556 1426923

By comparing all three performance metrics of machine learning algorithms,we can arrive at the conclusion that the random forest has higher accuracy. So random forest algorithm is considered for training the model.

Final output:

The predicted and actual values are compared and the final output is detected either as normal or attack packet.

CONCLUSION

In conclusion, this study emphasizes how important it is for protecting against DDoS attacks in order to assure the reliability and accessibility of online services for legitimate customers. To accurately identify and mitigate attacks using DDoS while reducing false positives to prevent unnecessary disturbance to actual traffic by utilizing a model built on machine learning techniques. Collecting the data for training our machine learning model by applying a variety of pre-processing strategies using the CIC-DDoS2019 dataset, a well-known benchmark in the area. To extensively experimented with three distinct methods for evaluating our model's performance using important metrics including F1 score, accuracy, precision, and recall.

Results show the usefulness of using machine learning algorithms to detect and mitigate DDoS attacks, as well as significant insights into the benefits and limitations of open datasets for training .Using tools such as Cicflowmeter to record live packets and transform them into testable datasets, we were able to predict and classify packets as regular or malicious traffic. Our findings highlight the importance of machine learning in improving cyber-security defences against emerging threats in real-world scenarios.

REFERENCE

1. Akgun, D., Hizal, S. and Cavusoglu, U., 2022. A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. *Computers & Security*, *118*, p.102748.

2. Priya, S.S., Sivaram, M., Yuvaraj, D. and Jayanthiladevi, A., 2020, March. Machine learning based DDoS detection. In *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)* (pp. 234-237). IEEE..

3. Bhargava, R., Singh, Y.P. and Narawade, N.S., 2022, May. Implementation of Machine Learning Based DDOS Attack Detection System. In *2022 3rd International Conference for Emerging Technology (INCET)* (pp. 1-5). IEEE.

4. Lima Filho, F.S.D., Silveira, F.A., de Medeiros Brito Junior, A., Vargas-Solar, G. and Silveira, L.F., 2019. Smart detection: an online approach for DoS/DDoS attack detection using machine learning. *Security and Communication Networks*, *2019*, pp.1-15.

SIMILARITY CHECK REPORT

ORIGINALITYREPORT

9%	6%	6%	4%
SIMILARITYINDEX	INTERNETSOURCES	PUBLICATIONS	STUDENTPAPERS

PRIMARYSOURCES

1	www.arcjournals.org InternetSource	1%
2	tede.unioeste.br InternetSource	<1%
3	JamesOduorOyoo,JaelSanyandaWekesa, Kennedy Odhiambo Ogada. "Predicting Road TrafficCollisionsUsingaTwo-LayerEnsemble Machine Learning Algorithm", Applied System Innovation, 2024 Publication	<1%
4	www.grafiati.com InternetSource	
5	AnkurChangela, YogeshKumar, Apeksha Koul."AutomatedSystemtoDiagnoseand DetecttheAllergy,CommonCold,Flu,and Covid using MachineLearning Approaches",2023InternationalConferenceon Communication,SecurityandArtificial Intelligence (ICCSAI), 2023 Publication	<1%

6	SubmittedtoUniversityofHertfordshire StudentPaper	<1%
7	docs.neu.edu.tr InternetSource	<1%
8	SubmittedtoGlyndwrUniversity StudentPaper	<1%
9	"Mobile Radio Communications and 5G Networks",SpringerScienceandBusiness Media LLC, 2024 Publication	<1%
10	PoojaKumari,AnkitKumarJain."Timely detectionofDDoSattacksinIoTwith dimensionalityreduction",ClusterComputing, 2024 Publication	
	ijarcce.com InternetSource	<1%
	www.researchgate.net InternetSource	
11	Joffrey L. Leevy, John Hancock, Richard Zuech, TaghiM.Khoshgoftaar."Detecting cybersecurityattacksacrossdifferentnetwork featuresandlearners",JournalofBigData, 2021 Publication	<1%
12		<1%
13		<1%

14	Pratiksha Chaudhari, Yang Xiao, Mark Ming-Cheng Cheng, Tieshan Li. "Fundamentals, Algorithms,and Technologies ofOccupancyDetectionforSmartBuildingsUsingIoT Sensors", Sensors, 2024 Publication	<1%
	SubmittedtoUniversityCollegeLondon StudentPaper	
	jad.shahroodut.ac.ir InternetSource	
15		<1%
	Nepal,Rajan."Predictionsofthe Survival of BreastCancerPatientsUsingMachine LearningAlgorithms", NorthDakotaState University, 2023 Publication	
16		<1%
	www.arxiv-vanity.com InternetSource	
17		<1%
	123dok.net InternetSource	
	UneneibotejitOtokwala,AndreiPetrovski, HarshaKalutarage."Optimizedcommon featuresselectionanddeep-autoencoder (OCFSDA)forlightweightintrusiondetection inInternetofthings",InternationalJournalof Information Security, 2024 Publication	
18		<1%
19		<1%
20		<1%

21	SubmittedtoUniversityofSouthampton StudentPaper	<1%
22	academic-accelerator.com InternetSource	<1%
23	SubmittedtoConcordiaUniversity StudentPaper	<1%
24	SubmittedtoManchesterMetropolitan University StudentPaper ro.uow.edu.au InternetSource	<1%
25	Moore,GranvilleVincent."ParallelComputerArchitectures andAlgorithms forMedical ImageAnalysis",TheUniversityof Manchester(UnitedKingdom),2020 Publication	<1%
26	SubmittedtoQueenMaryandWestfield College StudentPaper SubmittedtoUniversityofLiverpool StudentPaper	<1%
27	MahimaGaurihar,KaustubhPaonikar, Snehalata Dongre, Prashant Khobragade,Rahul Agrawal, Pranay Saraf. "EnhancingDroughtDetectionandVisualizationwith LSTM and SPEI: Addressing Slow-Onset	<1%
28		<1%
29		<1%

	Climate-InducedWaterScarcity",Research Square Platform LLC, 2023 Publication	
	dspace.daffodilvarsity.edu.bd:8080 InternetSource	
30	article.sciencepublishinggroup.com InternetSource	<1%
31	jomardpublishing.com InternetSource	<1%
32	ris.cdu.edu.au InternetSource	<1%
33	"Web, Artificial Intelligence and Network Applications",SpringerScienceandBusiness Media LLC, 2019 Publication	<1%
34	link.springer.com InternetSource	<1%
	mdpi-res.com InternetSource	
35	www.mdpi.com InternetSource	<1%
36	www.nature.com InternetSource	<1%
37		<1%
38		<1%