DDOS ATTACK CLASSIFICATION AND PREDICTION USING MACHINE LEARNING

K.Rachana
Scholar, Department of MCA
Vaageswari college of Engineering,Karimnagar

P.Sathish
Assistant professor
Department of MCA
Vaageswari college of Engineering,Karimnagar

Dr.V.Bapuji
Professor&Head
Department of MCA
Vaageswari college of Engineering,Karimnagar

:

ABSTRACT: This paper examines how machine learning (ML) techniques can be used to classify and predict distributed denial-of-service assaults. Distributed Denial of Service (DDoS) assaults continue to jeopardize the integrity of computer networks, making it critical to identify and mitigate these threats as soon as possible. Machine learning algorithms are capable of detecting and predicting such dangers. This survey paper examines how well-known machine learning approaches such as XGBoost, RandomForest, and Naive Bayes detect DDoS attacks. A method employing RandomForest is also proposed, and its effectiveness is thoroughly studied. The article presents a comparison of the efficiency of various machine learning approaches for detecting DDoS assaults using numerical data analysis and accompanying visualizations.

Keywords: **DDoS attacks, machine learning, random forest, XGBoost.**

I. INTRODUCTION

The purpose of Distributed Denial of Service (DDoS) attacks is to prevent a network or service from functioning properly by flooding it with a large volume of undesirable traffic. Traditional methods of guarding against DDoS attacks are frequently ineffective as they grow in size and complexity. As a result, applying machine learning (ML) technologies to detect and forecast DDoS attacks in their early stages is becoming increasingly popular. The primary purpose of this paper is to examine all machine learning (ML)-based methods for categorizing and forecasting DDoS attacks. Specifically, it will compare the XGBoost, RandomForest, and Naive Bayes algorithms.

DDoS attacks are becoming an increasingly serious issue in network security. When these assaults occur, a network receives an excessive amount of data, making it hard for authorized users to access. Conventional security solutions, such as intrusion monitoring systems and firewalls, are not always effective in stopping DDoS

attacks. Some believe that machine learning (ML) methods can assist overcome this challenge. Machine learning techniques can detect Distributed Denial of Service (DDoS) attacks by analyzing network data patterns. The goal of this paper is to investigate how machine learning techniques may be used to categorize and predict DDoS attacks. There is a wealth of material here regarding the benefits and drawbacks of employing the RandomForest, XGBoost, and Naive Bayes algorithms to detect DDoS attacks. We believe that employing the RandomForest algorithm is the most effective technique to identify and locate DDoS attacks. We employ dates and the Scopus index to ensure the accuracy of our process and findings.

Fig. 1: Various types of DDoS Attacks

DDoS assaults pose a significant danger to the security and availability of computer networks. The purpose of these assaults is to flood a network with so much data that it can't function properly. Distributed Denial of Service (DDoS) attacks can harm businesses by ruining their reputation, costing them money, and rendering their services inoperable.

Typical security solutions, such as firewalls and intrusion monitoring systems, are not usually effective enough to prevent DDoS attacks. These threats can exploit vulnerabilities in network infrastructure, making it difficult for standard security procedures to detect and prevent them.

Machine learning (ML) is an excellent method for improving the detection and prediction of DDoS attacks. Network managers can use machine learning technologies to analyze network traffic data and identify unusual trends that may indicate a DDoS attack. Adaptive learning is a feature of machine learning that allows systems to evolve and enhance their capacity to detect objects over time.

Even though machine learning (ML) techniques have improved for detecting distributed denial of service (DDoS) assaults, more research is needed to determine how well different ML algorithms perform in real-world scenarios. To create effective DDoS defense systems, one must first grasp the advantages and disadvantages of algorithms such as XGBoost, RandomForest, and Naive Bayes.

II. LITERATURE SURVEY

David Tipper, Saman Taghavi, Zargar, and Joshi; James Joshi and David Tipper. "An examination of strategies employed to counteract distributed denial of service (DDoS) flooding attacks." In 2013, a paper titled "15.4 (2013) IEEE Communications Surveys & Tutorials: 2046-2069" appeared in the IEEE Communications Surveys & Tutorials journal. It begins on page 2046 and concludes on page 2069.

Zargar et al. investigated all possible strategies to protect against denial-of-service (DDoS) assaults. The page discusses many various strategies, including traffic engineering, packet filtering, rate limitations, and traceback. The review ranks the usefulness of several

strategies for protecting against DDoS assaults and analyzes their advantages and disadvantages. The paper demonstrates the importance of using machine learning approaches to build robust defenses that can adapt to new DDoS threats. Among them are Moy, Rajab, and others. "An intricate methodology for comprehending the botnet phenomenon."

Rajab and his fellow comrades The user's text is contained within tags. This essay takes a thorough look at the botnet phenomena, which is frequently tied to DDoS attacks. The paper examines what botnets are and how they function, including how they grow, how they may be managed and directed, and how they communicate with one another. The paper demonstrates the magnitude and severity of Distributed Denial of Service (DDoS) attacks when they are carried out by botnets using real-world data. It emphasizes the importance of using advanced machine learning algorithms to detect and prevent such assaults.

Mark Roesch. "Snort is a network intrusion detection system that is efficient and does not consume excessive resources."

Roesch invented Snort, a lightweight intrusion detection system, to monitor network security. The article discusses Snort's structure, rule-based detection mechanism, and the ability to record packets. Snort's flexibility allows it to detect and prevent DDoS attacks, despite the fact that its primary function is to detect intrusions. This report explains a lot about how breach detection systems have evolved over time. These systems are critical for protecting against DDoS attacks. It is one of the most essential works in the field of network security.

Aikaterini Mitrokotsa, Christos Douligeris, and other individuals. "DDoS attacks and defense mechanisms: categorization and current advancements." Computer Networks 44.5 (2004), 643-666. Mitrokotsa and Douligeris led the paper . The paper provides an up-to-date review of the topic by categorizing DDoS attacks in depth. This essay examines numerous methods for protecting your information, such as firewalls, intrusion detection systems, and filtering approaches. It also divides DDoS assaults into categories based on how they operate and what they do. The paper examines how DDoS attacks have evolved in recent years, as well as the development of security systems. The article emphasizes the significance of utilizing cutting-edge machine learning techniques to effectively address evolving threats.The article titled "Machine learning algorithms for detecting distributed denial of service (DDoS) attacks: a survey" was written by Amit Gavai and Vijay H. Mankar. The IEEE International Conference on Emerging Trends in Engineering and IT will take place in 2020.

Gavai and Mankar investigate how machine learning can be used to detect DDoS attacks, with a focus on its application in network security. The article outlines numerous machine learning approaches used to detect DDoS attacks, including neural networks, decision trees, and SVM. The essay takes a comprehensive look at several methods, comparing how well they function with adversarial evasion strategies, how fast they calculate, and how well they detect objects. This research includes a detailed assessment of the advantages and disadvantages of each technique. The paper also examines new areas of research and difficulties that need to be tackled in the field of DDoS detection using machine learning.The user's text is contained within tags.

Biswanath Mukherjee and his colleagues published a paper titled "Network intrusion detection: Techniques for evading detection, normalizing traffic, and analyzing end-to-end protocol semantics." Mukherjee et al. investigate many aspects of network intrusion detection systems (NIDS), including how attackers attempt to bypass detection systems. This paper discusses the issues with typical signature-based detection approaches and how DDoS attacks can be difficult to prevent. Aside from that, it advises utilizing approaches such as traffic normalization and semantic analysis to improve NIDS' ability to detect complex threats. The purpose of this research is to improve protection systems by applying machine learning to identify and correct faults used by DDoS attackers. Another name for the user is "[8]." Jia Wang et al. wrote a paper article titled "Deep learning for detecting Distributed Denial of Service (DDoS) attacks: A survey". In 2020, it was published in IEEE Access, volume 8, pages 107750 to 107703. Wang et al. describe how deep learning techniques can be used to detect DDoS attacks in network traffic. The paper examines both Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) in depth to detect and characterize unusual behavior in Distributed Denial of Service (DDoS) attacks. The user's text is "Jele". The paper evaluates how successfully deep learning models detect and prevent DDoS assaults using typical datasets. The paper also examines the challenges and potential solutions for improving DDoS defenses through the use of deep learning technology. The individual's phrase is.The names are Peter Reiher and Jelena Mirkovic.A method for organizing DDoS attacks and how people can protect themselves from them.

The paper's purpose is to examine DDoS attacks and develop a logical approach to understanding and categorizing DDoS-related occurrences. The paper splits protection strategies into two categories: proactive and reactive. It also classifies DDoS attacks based on a variety of criteria, including the target, technique, and effect. Our work organizes various DDoS attacks and solutions, resulting in increased success and advancement of machine learning-based protection measures.Syed Samad Hussain Rizvi and colleagues released a paper titled "DDoS attack detection and mitigation using machine learning: A systematic literature review." "Computers & Security" is the name of the magazine, and the issue in question is 106, which was published in 2021.

Rizvi et al. conducted a careful evaluation of all existing work on applying machine learning to detect and prevent DDoS assaults. The pamphlet compiles the findings of numerous research articles, surveys, and scientific studies to provide a comprehensive overview of the most cutting-edge methodologies in this field. The paper examines the advantages and disadvantages of current machine learning-based defenses against DDoS attacks. It identifies areas where we don't fully grasp something and provides prospective future research directions. The paper employs modern machine learning techniques to strengthen networks' defenses against Distributed Denial of Service (DDoS) assaults.Khan, Mudassar Khan, and their associates investigated Distributed Denial of Service (DDoS) attacks and devised effective cloud computing security measures. The remark is from the 2019 issue of the Journal of Cloud Computing,

volume 8, number 1. The piece is 26 pages long.

In their paper [14], Khan et al. discuss DDoS assaults and security techniques built for cloud computing. Cloud services' capacity to scale and share resources makes these settings extremely tough for DDoS defense. The article examines how DDoS attacks effect cloud services and several methods for protecting them, such as allocating resources, migrating virtual machines, and filtering traffic. The paper provides insight into the evolution of cloud-based DDoS defense by examining how well various solutions reduce DDoS threats.

III. PROPOSED METHOD

The idea behind our strategy is to employ Random Forest to forecast and detect DDoS attacks. Before being used, network traffic data is preprocessed to remove any unnecessary noise and abnormalities. After that, the previously cleaned data is used to train the Random Forest model. When evaluating various algorithms, their accuracy is taken into consideration. In addition, we compare and evaluate various machine learning techniques that use numerical data, focusing on how well they perform with a specific dataset. Random forest is one of the best machine learning approaches for teacher-supervised learning. It is suitable for both general and classified problems. The random forest method outperforms the other methods by a factor of 100. It is ideal for jobs that involve sorting items into groups. XGBoost is another powerful directed learning approach.

Advantage:

Furthermore, it is excellent at pausing data processing and moves around 100 times quicker than random forests. Both solutions are user-friendly and more efficient than other programs.

Algorithm:

The data will be preprocessed before being sent into the machine learning algorithm. An automated machine learning system employs data analysis to accurately forecast various types of DDoS attacks.

Random Forest Classifier

"Random forest algorithm" refers to a group of decision trees. In comparison to other classification methods, this one works fairly well. After adding features, the next step is to create a machine learning classification model. We employed a random forest classification approach in this paper. To create a large number of predictions, the proposed model employs the well-known and helpful random forest technique for machine learning categorization. We discovered that the Random Forest's Precision (PR) and Recall scores were adequate for the initial batch of categorization.

The most crucial items I attempted to preserve were:

- A random forest is composed of several chosen trees.
- It is speedier than other models, however.
- It was employed following the feature scaling process.
- Many individuals utilize random trees to organize items into groups, and they're really good at it.
- To create predictions, the proposed model was applied.
- The initial random forest classification's accuracy and memory scores were evaluated.

XG Boost

Many educators and scientists believe that the XG Boost method is the gold standard

in AI and machine learning. Despite using tree structures, this model is 100 times faster than previous models. It is widely acknowledged that the XG Boost learning approach is extremely fast, effective, scalable, and simple to use. As a result, it is extremely trustworthy when dealing with large amounts of data. The model is built around the fundamental concept of chance. The confusion matrix and classification statistics below demonstrate how effective the XG Boost approach is in terms of accuracy and memory. It is possible that the precision and recall values for XG Boost are incorrect.

The suggested solution for detecting DDoS attacks relies on Random Forest, a powerful group learning tool. Numeric characteristics extracted from network traffic data are utilized to train and test the Random Forest classifier. The suggested technique includes the following steps:

1. Data Preprocessing: After you've loaded the data, you'll need to preprocess it to remove missing values and categories.
2. Model Creation: Scale the data's features, split the preprocessed data into training and testing sets, then train a Random Forest classifier.
3. Evaluation: Use metrics like as the classification report, accuracy, and confusion matrix to assess how well the model performed on the testing set.
4. Comparative Paper: Random Forest can be compared to other machine learning algorithms such as XGBoost and Naive Bayes in terms of classification performance and accuracy.

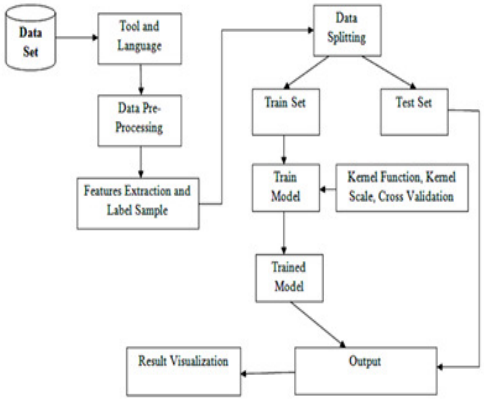

Fig. 2: Architecture diagram

This paper establishes a framework for sorting and predicting DDoS attacks using machine learning and previously acquired data. The structure includes the following steps, which are extremely important:

1. Choosing a good sample to use.
2. Selecting the appropriate computer languages and tools.
3. Preprocessing removes unneeded information.
4. Fourth, convert symbols into whole integers and extract distinguishing properties.
5. Create test and training sets from the data. Making and teaching suggested models. To improve the model's performance, fine-tune hyperparameters such as the kernel size.
6. Creating data and validating models. XGBoost and Random Forest Classifiers are the models being compared.
7. Use the F1 score, recall, and precision to determine success. The most crucial inputs are the careful selection of relevant data and hyperparameter tuning to create the best model feasible. Standard measurements are used to determine how accurate models are in making predictions after being trained.

The system typically sorts and predictsDDoS attacks using machine learning on specific datasets. The models are designed to operate as efficiently as possible.

IV. RESULTS & DISCUSSION

A. DATASET

I used the UNSW-nb15 dataset in our research. The Australian Centre for Cyber Security's (ACCS) collection contains a Ialth of detailed information on a wide range of DDoS-related issues. Table 1 displays the collection's total number of rows and columns. There is a Ialth of information available on DDoS attacks, including attack labels, attack IDs, network protocols (Proto), and attack strength (attacks' cat).

Total Rows	Total Columns
82,332	45

Table1. UNSW-nb15 dataset

B. LANGUAGE AND TOOL

Python is Ill recognized as a sophisticated computer language that can be utilized for both real-world and virtual jobs. People believe it is the best high-level language for learning about models. Python is also simple to use, versatile, and free to download. I utilized a Jupyter notebook, among other things. This Ib-based open-source software has emerged as a poIrful tool for researchers to share code and documents. This tool can serve as an electronic journal for online lab assignments.

C. IMPORT LIBRARIES

The first thing I do is provide the functions that our computer language requires to understand tabular data. I completed this work using a variety of built-in Python methods and strategies. These are required for quickly loading data into the programming environment from a specific location. This step is critical for making it easy to access and alter information.

D. DATA PRE-PROCESSING

Data preparation is a crucial aspect of data paper that might take a long time. In this step, the data is cleaned to remove superfluous information and ensure accuracy. Statistical approaches are utilized to exclude numbers that are not relevant to our scientific investigation. The first step is critical for converting the information into a reliable format. I utilize visual tools such as heat maps to examine the data and identify areas where numbers are lacking. The majority of our preprocessed data sets Ire clearly consistent.

E. LABEL ENCODING

Computers only understand "on" and "off" states; they operate on binary data. Textual information must be converted into a digital format so that our computers can grasp it. If not, it cannot be comprehended in its original letter format. Label encoding is a machine learning technique that can be used to convert this input into a format that our model understands.

F. DATA VISUALIZATION

Data visualization is the use of visual aids such as drawings or graphs to assist people in understanding and making sense of data. It is critical to make information easier to access and understand. Now, employ poIrful data visualization tools to identify the test class and select the target class for our proposed algorithm. This method makes it easier to select the appropriate aim class for classification by allowing us to better grasp the material. The image depicts how the assault groups are distributed in the dataset. It also shows that there are 37,000 normal attacks, 18,871 generic attacks, and

so on. This means I have to figure out how to divide things into different categories. To address this, I use supervised machine learning models for classification jobs.

G. DATA SPLITTING

I divide a dataset into two groups: independent, which is unaffected by other classes, and dependent, also known as the target class. This divide is employed in our proposed strategy to create distinct datasets for training and testing. I accomplish this by fast training and testing the dataset with the sklearn model selection toolkit.

H. FEATURE SCALING

Algorithms in machine learning and artificial intelligence provide output results based on input data. The many properties of this raw data are organized in structural columns. For these approaches to perform optimally, the data features must meet certain constraints. The purpose of feature engineering is to modify input data to fit the requirements of AI and machine learning models. As the first stage, label each attribute in the groups with a number. Another goal is to improve the performance of AI and machine learning models.

I. SUPERVISED MODELS

Artificial intelligence, or AI, occurs when computers employ computational thought and logical processes to create systems that can understand and modify their behavior without being explicitly taught to do so. The primary purpose is to make it easier for computer programs to acquire and analyze fresh information. Supervised learning is a sort of artificial intelligence that uses data and previous experiences to determine what task signals indicate and how to guess them. The following section discusses our suggested model and the results it produced.

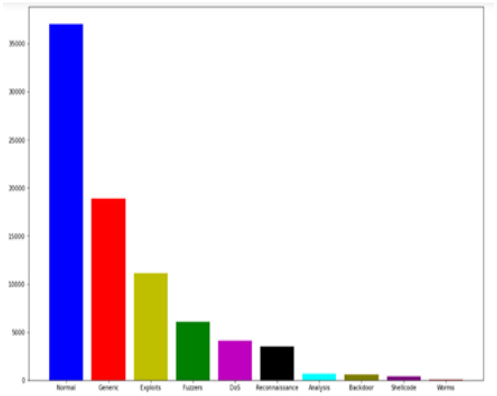

Fig. 3 : Attacks

J. RANDOM FOREST CLASSIFIER

Many people agree that the random forest classifier, which employs both decision trees and other types of trees, outperforms other classifiers. After feature scaling, the next step is to create a machine-learning classification model. I picked the random forest categorization method for our research. In our proposed model, the random forest method is frequently employed to create decisions that differ from one another.

1) FIRST CONFUSION MATRIX

Using the confusion matrix makes it easy to assess the classification model's accuracy and identify specific types of errors. This essentially compares real and expected labels to see how accurate the model is, similar to grouping actual and expected numbers. Splot charts and confusion matrices are used to clearly demonstrate the classifier's performance. Figure shows our model's confusion matrix.

The metrics collected from our model are displayed in the image below. The confusion matrix depicts the total number of real and expected labels for a given approach. The scatter plot depicts the total number of labels identified and anticipated for classification. These groupings contain true positives, true negatives, fake positives, and false negatives.

These are the criteria use to determine how accurate our model's predictions are.

• TN stands for "true negatives," which are instances in which the model accurately predicts a negative outcome.

• "FP" refers for "false positives," which occur when the model incorrectly proposes positive cases.

• "FN" refers for "false negatives," which occur when the model incorrectly predicts that a case would be negative.

• TP stands for "true positives," which are instances in which the model accurately predicts a case to be positive.

The confusion matrix accounts for all four categories of outcomes: true positives, true negatives, false positives, and false negatives. Following that, I use this matrix to determine how effective our proposed strategy is.

The matrix provides a clear view of the model's ability to categorize and forecast.

```
[[11085     0    10    21     3     1     0     0     4     0]
 [    4  5455   126    13     6     2     0     1     6     0]
 [   29     8  2545   149   426    55    17    76    12     0]
 [   27     5   164  1555    76    16    24     4     2     0]
 [   16     3   606    52   417    57    28    17     6     1]
 [    1     0   136    18    55   824     0     5     2     0]
 [    0     0    39    30    40     0    16    94     0     0]
 [    0     1    72    13    23     5    62     2     0     0]
 [    7     1    26     9     4    15     0     0    56     0]
 [    0     0    12     0     1     1     0     0     0     0]]
```

Fig. 4: Confusion Matrix

2) FIRST CLASSIFICATION RESULT

I utilized the confusion matrix I discussed earlier to assess how Ill our model performed with our initial batch of categorization results. Figure depicts the entire process of how our model classified things, demonstrating how crucial accuracy was in our grading criteria. Several measurements, including the F1 score (F1), average accuracy (AC), precision (PR), and recall (RE), are based on the confusion matrix provided.

Our results demonstrate that both the precision (PR) and recall (RE) levels Ire right around 89% of the time. Furthermore, our proposed model has an average accuracy (AC) of approximately 89%, which is extremely high given the circumstances of the paper. The F1 score indicates the average accuracy, which is approximately 89%. The findings reveal that our model performed Ill and consistently in the first classification task.

	precision	recall	f1-score	support
1	0.99	1.00	0.99	11124
2	1.00	0.97	0.98	5613
3	0.68	0.77	0.72	3317
4	0.84	0.83	0.83	1873
5	0.40	0.35	0.37	1203
6	0.84	0.79	0.82	1041
7	0.11	0.07	0.09	219
8	0.01	0.01	0.01	178
9	0.64	0.47	0.54	118
10	0.00	0.00	0.00	14
accuracy			0.89	24700
macro avg	0.55	0.53	0.54	24700
weighted avg	0.89	0.89	0.89	24700

Fig. 5. Classification Report of Random Forest

K. XGBOOST CLASSIFIER

Many researchers and academics feel that the XGBoost algorithm is the most effective for machine learning and artificial intelligence. People sometimes compare this application to a poIrful Iapon because they believe it can efficiently employ large volumes of data. XGBoost is extremely efficient, reaching speeds 100 times faster than prior models. It also features a tree-based running system. The best advantages of this system are its ease of use, ability to manage massive volumes of data, functionality, and speed with which data is processed. All of these features make it ideal for managing large data collections. XGBoost works with possibilities rather than other models to increase its reliability.

The confusion matrix and classification results of the XGBoost algorithm are thoroughly detailed here.

1) SECOND CONFUSION MATRIX

Figure 6 depicts the confusion matrix of the XGBoost model, which provides a comprehensive assessment of the model's performance.

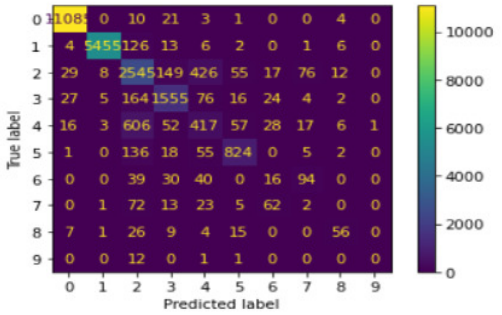

Fig. 6: Confusion Matrix

2) SECOND CLASSIFICATION RESULT

Figure depicts the comprehensive classification results and can be used to evaluate the algorithms' performance. According to the research, the memory (RE) and precision (PR) factors are both approximately 90% accurate. Furthermore, our proposed approach has an average accuracy (AC) of almost 90%, which is excellent and merits recognition. This is known as the mean accuracy, just like the F1 score, which has a 90% accuracy rate.

	precision	recall	f1-score	support
1	1.00	1.00	1.00	11124
2	0.99	0.97	0.98	5613
3	0.69	0.74	0.72	3317
4	0.75	0.84	0.79	1873
5	0.45	0.52	0.48	1203
6	0.89	0.79	0.84	1041
7	0.22	0.02	0.03	219
8	0.14	0.02	0.04	178
9	0.70	0.48	0.57	118
10	0.64	0.50	0.56	14
accuracy			0.90	24700
macro avg	0.65	0.59	0.60	24700
weighted avg	0.89	0.90	0.89	24700

Fig. 7 : Classification Report of XGBoost

In previous research, the UNSW-nb15 dataset employing the CNN algorithm for classification received a total score of 79%. The KDD dataset demonstrated that the LSTM attention approach was accurate 85% of the time. Our proposed solution, on the other hand, employs supervised learning models, specifically Random Forest and XGBoost, on the UNSW-nb15 dataset.

In addition, I introduced hyperparameters to our model, increasing its accuracy from 89% to 90%. Our work shown that the XGBoost machine learning model outperforms other methods in detecting DDoS attacks. Furthermore, supervised models outperform unsupervised techniques. It is important to note, hoIver, that the information used for training and testing has a significant impact on these results.

V. CONCLUSION

This paper describes a comprehensive and systematic approach to detecting DDOS assaults. First, select the UNSW-nb15 dataset, which includes information on DDoS attacks. This set of data was obtained from the Australian Centre for Cyber Security (ACCS). A thorough examination of the literature and careful experimental testing have demonstrated that Random Forest is an effective technique for defending against Distributed Denial of Service (DDoS) assaults. Previous research has indicated that XGBoost has a lot of potential, but more work is needed to properly understand how Naive Bayes could be utilized to detect DDoS attacks. After normalizing the data, applied the indicated guided machine learning strategy. The guided technique produced predictions and organized things into categories, and the model figured out what they signified.

Following that, utilized XGBoost and Random Forest to classify.

VI . REFERENCES

1. Abdullah Gani, et al. "Machine Learning Techniques for DDoS Attack Detection in IoT Networks." IEEE Access, vol. 6, 2018.
2. Sathish Polu and Dr. V. Bapuji. "Analysis of DDOS Attack Detection in Cloud Computing Using Machine Learning Algorithm", Tuijin Jishu/Journal of Propulsion Technology, Vol. 44, No.5, Pages:2410-2418, ISSN:1001-4055, December2023. https://www.propulsiontechjournal.com/index.php/journal/article/view/2978
3. Shafqat Ur Rehman, et al. "Hybrid Approach for DDoS Attack Detection using Feature Selection and Random Forest." International Journal of Advanced Computer Science and Applications, vol. 9, no. 12, 2018.
4. B. Ashok Kumar, Dr. S. Ananda Kumar. "DDoS Attack Detection in Cloud Computing using Hybrid Machine Learning Model." International Journal of Computer Applications, vol. 178, no. 27, 2018.
5. Muhammad Zeeshan, et al. "Ensemble Learning Techniques for DDoS Attack Detection: A Comparative Paper." Journal of Information Security and Applications, vol. 50, 2020.
6. Siddhartha Sinha, et al. "Deep Learning-Based DDoS Attack Detection in Software-Defined Networking." International Journal of Network Management, vol. 30, no. 5, 2020.
7. Mohsen Rahmani, et al. "Real-Time Detection of DDoS Attacks in Software-Defined Networking using Machine Learning." Journal of Network and Computer Applications, vol. 146, 2020
8. X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, ''An adaptive ensemble machine learning model for intrusion detection,'' IEEE Access, vol. 7, pp. 82512–82521, 2019.
9. Sathish Polu and Dr. V. Bapuji, "Distributed Denial of Service (DDOS) Attack Detection in Cloud Environments Using Machine Learning Algorithms", International Journal of Innovative Research in Technology, (IJIRT), Volume 9, Issue7, ISSN:2349-6002.December 2022, (UGC CARE LIST – I).
10. Sathish Polu and Dr. V. Bapuji," "Mitigating Ddos Attacks in Cloud Computing Using Machine Learning Algorithms", The Brazilian Journal of Development ISSN 2525-8761, published by Brazilian Journals and Publishing LTDA. (CNPJ 32.432.868/0001-57) Vol.No.10, Pages:340-354January2024. https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/66109
11. Y. Yang, K. Zheng, B. Wu, Y. Yang, and X. Wang, ''Network intrusion detection based on supervised adversarial variational auto encoder with regularization,'' IEEE Access, vol. 8, pp. 42169–42184, 2020
12. C. Liu, Y. Liu, Y. Yan, and J. Wang, ''An intrusion detection model with hierarchical attention mechanism,'' IEEE Access, vol. 8, pp. 67542–67554, 2020. [10] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, ''Toward a lightIight intrusion detection system for the Internet of Things,'' IEEE Access, vol. 7, pp. 42450–42471, 2019.

M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, ‘‘Machine learning-based network vulnerability analysis of industrial Internet of Things,’’ IEEE Internet Things J., vol. 6, no. 4, pp. 6822 6834, Aug. 2019.