International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 12 | Dec 2023 www.irjet.net p-ISSN: 2395-0072

Cybersecurity Threat Detection of Anomaly Based DDoS Attack Using Machine Learning

Anjali M[1], Smithu B S[2], T Saritha[3]

[1]*Student, Dept. of CSE, Nitte Institute of Technology, Karnataka, India*
[2]*Lecturer, Dept. of CSE, Government Polytechnic College, Karnataka, India*
[3]*Lecturer, Dept. of CSE, Government Polytechnic College, Karnataka, India*

Abstract - *In today's world, network attacks are a major security concern due to the fast-paced progress of the internet and technology. DoS attacks are complex threats that are hard to combat. DDoS attacks are even more hazardous as they can cause significant disruptions. Furthermore, they are particularly challenging because they can strike unexpectedly and quickly cripple a victim's communication or computing resources. DDoS attacks are a constantly evolving threat which is increasingly challenging to detect and effectively mitigate. To counter this menace, we have explored diverse techniques and methods on the DDoS attack dataset i.e. SDN specific dataset .Machine learning has improved DDoS detection by implementing various algorithms, including Decision Trees,Support Vector Machine, Naive Bayes, K-Nearest Neighbour, MultiLayer Perceptron, Quadratic Discriminant, Stochastic Gradient Descent (SGD), Logistic Regression, XGBoost, and deep learning methodologies such as Deep Neural Networks (DNN). An extensive comparative analysis of these algorithms has evaluated their performance based on accuracy metrics.*

Key Words: **Cyber security, DDoS detection, Machine learning, Deep learning, Accuracy, DDoS attack.**

1. INTRODUCTION

Worldwide, companies and organizations face ongoing worries about cyber threats. These malicious individuals target individual computers or whole networks, presenting numerous potential cyber-attacks. Within this array of hazards, DDoS attacks are a major concern for Internet security. DDoS attacks come in various forms, but their ultimate objective is to disrupt services to the extent that they can cause significant problems and even monetary losses. In light of the advancement of Machine learning algorithms that can do massive amounts of data processing, several academics have researched the implementation of various machine learning techniques to prevent DDoS attacks. There is therefore an imminent need for further investigation into this issue, especially given the damaging impact of DDoS attacks on targeted organizations, which underscores the imperative to advance DDoS detection technologies. Machine learning techniques have diverse applications, including addressing cyber security concerns. When constructing a DDoS detection system, the fundamental aim of a classification algorithm is to differentiate and categorizes requests stemming from DDoS attacks amid the typical network traffic. Achieving superior prediction precision and rapid model training times are two crucial aims when harnessing machine learning for DDoS detection. These objectives are significantly impacted by various parameters, which include the chosen classification algorithms. The accuracy and training time of the model are directly affected by the size of the dataset. Feature selection methods have been analyzed to remove unwanted data and accelerate model training. Furthermore, setting the parameters of the machine learning algorithm affects both performance and training time.

2. RELATED WORK

[1] The accuracy and training speed of models are significantly affected by various factors, such as the choice of classification algorithms. Additionally, the precision of the model and training duration are directly influenced by the dataset's size. Another technique to consider is the "Low and Slow" DDoS attacks, which focus on specific protocols while keeping open connections for prolonged periods. This study analyses Slowloris DDoS attacks within a Software Defined Networking (SDN) environment and explores their potential for mitigation and detection. Enabling information sharing between the SDN controller and the mitigation and detection module is essential in detecting and preventing low-intensity DDoS attacks.

[2-3] Recent studies have shown that developing a classifier to detect DDoS attacks using networking flow information can offer superior performance and efficiency compared to the per-packet-based method. However, due to reliance on numerous variables and automatic flow extraction, the current classifier is is not suitable for supporting real-time DDoS protection. This study examines the potential use of a programmable switch to extract concise flow features for the real-time identification of DDoS attacks. The suggested technique considers four flow variables: IP protocols, packet and byte counters, and the variance in delta duration of a network flow. Contrary to research that utilizes a high number of features (24-82 features), the analysis results on the CICDDoS2019 dataset indicate similar data classification performance. The decision tree and random forest classifiers demonstrated outstanding performance, with 89.5%

precision, recall, accuracy, and F1 score, and outperformed other models.

[4] Instantaneous scalability is a major benefit of cloud computing as it meets fluctuating demand. To minimize the adverse effects of DDoS attacks on an organization's uptime, effective DDoS protection is critical. In this presentation, we explore various DDoS detection techniques and compare current detection approaches based on a variety of criteria. To address the existing detection problems and potentially reduce these attacks, we assess their pros & cons, propose a methodology based on support vector machines (SVM) and Self-Organizing Maps. A malicious actor intentionally disrupts and damages the services and assistance offered to legitimate users via a DDoS.

[5] At the heart of this technology is a package filtering mechanism that carries out real-time analysis of network traffic at the packet level. By scrutinizing packets as they move through the network, the system identifies potentially harmful traffic patterns, such as sudden surges, that may indicate a DDoS attack. Additionally, the technology considers particular properties of the cloud, such as virtualization, multitenancy and the cloud computing model. Real-time trials employing a dataset from DARPA reveal the efficacy of the system in detecting and alleviating DDoS attacks in cloud infrastructures. The technology proactively aims to fortify the security and durability of cloud-based applications against DDoS threats.

[6] This study conducted a comparative analysis of two machine learning techniques; logistic regression and a shallow neural network (SNN), for predicting DDoS attacks. Our findings revealed an accuracy rate of 98.63% using logistic regression and an impressive 99.85% with SNN. It is worth mentioning that SNN required ten times longer training time than logistic regression. DOS attacks are usually executed by a lone attacker. Conversely, Distributed DOS (DDOS) attacks pose a greater threat as multiple attackers from different networks join forces to focus on a single user or service.

[7] Cybercriminals commonly employ Distributed Denial of Service (DDoS) attacks against web-based organizations, the Internet of Things (IoT) - which includes smart devices connected to the internet - and critical infrastructure. The aim of this research is to develop a cybersecurity risk model that will allow online businesses to assess the likelihood and potential impact of successful DDoS attacks. However, we could not locate any document that specifically provides a universal mathematical framework for evaluating cyber risks linked to DDoS attacks and their financial losses for firms.

[8] While other techniques exist for identifying unusual network traffic patterns, machine learning is the most effective in detecting denial of service attacks, which is among most significant dangers the internet faces. The algorithms make use of the Random Forest algorithm, co-clustering, information gain ratio, and network entropy estimates. The unsupervised component of this technique allows for the identification of DDoS attacks while minimizing extraneous normal traffic data. Unscrupulously, a DDoS attack entails inundating the infrastructure of internet traffic flow to the extent where it hinders the normal network and traffic operations of a designated server.

[9] The paper proposes a mechanism for detecting DDoS attacks and adapting resources accordingly. To transfer connections to the backup server, we begin by identifying suspicious connections based on DDoS attack traits. A convolutional neural network on the backup server effectively determines whether traffic on these suspicious links constitutes an attack. The simulation results show how well the detection system can determine if a DDoS attack impacts a particular connection. It is also able to move questionable connections, reduce network load and maintain network functionality.

[10] Amazon Web Services (AWS) was hit by a DDoS attack, following an earlier attack on GitHub. Numerous solution options are available. A DDoS attack is a consciously trying to overwhelm a server, network or service legitimate Internet traffic by inundating the target or surrounding network with traffic. If a DDoS attack happens on the system, it might show some or all of the following signs. The server is too occupied handling a huge number of requests to reply to reliable queries. Application-Level Attacks: Web servers are aimed by hackers using GET requests to obtain data. A target web owner gets GET or POST requests from attackers. Resources are consumed considerably by the responses to these queries. Protocol Level Attacks: By taking advantage of vulnerabilities in Protocol stack layers 3 and 4, protocol-based attacks, such as the SYN flood, become feasible.

[11] This study concentrates on recognizing distinct types of DDoS attacks, including UDP-Flood, Smurf, HTTP-Flood, and SiDDoS, implementing artificial neural networks. The focus will be on Distributed Denial of Service (DDoS) attacks targeting the network's connectivity and transport layers. To bridge the research gap and improve the model's effectiveness, we evaluated time and spatial complexities. Our analysis of the dataset led to the conclusion that our proposed remedies can achieve better results.

[12] The objective of this project is to investigate Distributed Denial of Service (DDoS) attacks on SDN networks enabled by Artificial Intelligence (AI) and to explore potential Machine Learning (ML) solutions for avoiding these attacks. By utilizing the principle of network entropy, which suggests that higher unpredictability leads to lower entropy, ML classifiers can be constructed to identify vulnerable networks. Programmable routers using programmable switches can undertake an array of specialized processing tasks. Additionally, this architecture clearly separates the control plane, which was previously managed by an identical device in older switches, from the data plane.

[13] The main target of this study is the estimation of the impact of distributed denial of service (DDoS) attacks on the southbound channel for data-to-controller administration in software-defined networking (SDN) systems. The article aims to comprehend how grid service disruptions can result from a successful DDoS attack against the SDN controller. The simulations aimed to assess the SDN controller's ability to respond to different levels of attack intensity and techniques. The study presents the findings alongside the controller's utilization of CPU and memory during the attacks. Moreover, it evaluates network throughput, packet loss, latency, and other performance indicators that depict the controller's resilience.

[14] This paper explores identifying and mitigating distributed denial of Service (DDoS) attacks in the software-defined networking (SDN) framework with 5G ecosystem. It introduces an innovative DDoS attack detection method that employs a two-tier deep learning model, namely CNN-LSTM, within the SDN infrastructure. Its primary goal is to protect against DDoS attacks in 5G SDN setups. It proposes CNN-LSTM, a state-of-the-art DDoS detection technique that enhances accuracy and reduces detection time. This ensures prompt blocking of DDoS traffic to maintain network service availability.

[15] This paper highlights the importance of understanding DDoS attacks and taking suitable measures. It presents an original technique for detecting and mitigating such attacks, which centers on examining incoming traffic from botnets in the attacker's system. The suggested approach employs machine learning algorithms to make informed judgements as it analyses requests originating from botnets. The team has run simulations to confirm the efficacy of this methodology, with the output yielding insight information on DDoS mitigation.

[16] The paper outlines an experimental method that leverages the OPNET simulation tool. The study uses traffic from three unique applications - VoIP, FTP, and HTTP - to create a practical model. The model incorporates a firewall to mimic DDoS attacks on the internet. The investigation comprises three scenarios that depict different facets of DDoS attacks across networks. The results of these situations emphasize the effectiveness of configuring firewalls to mitigate the impact the DDoS attempts, improving network security and resilience.

3. PROPOSED METHOLOGY

3.1 System Architecture

In today's online landscape, companies and organizations are at a higher risk of experiencing Denial of Service (DDoS) attacks. These assaults can cause disruptions to online services, leading to downtime, financial losses, and damage to reputation. To protect against evolving DDoS threats, conventional security measures are no longer enough. To ensure the availability of uninterrupted service and secure our systems, we suggest developing and implementing an advanced DDoS detection system by implementing suitable model where packets flow from the internet which is preprocessed flowing to internet service provider system detecting DDoS attack as shown in the Fig 1

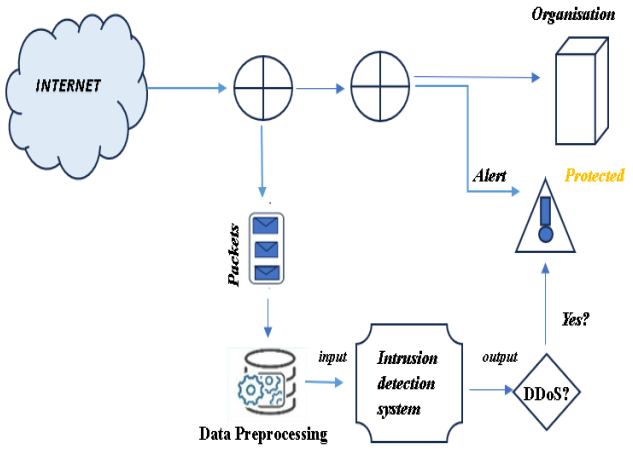

Fig -1: Proposed System

3.2 Model Architecture

The process of machine learning is a systematic method for creating predictive models and gaining insights from data. It can be broken down into several key stages as shown in Fig 2.

The first is Data Collection, during which relevant information is obtained. Accuracy and quantity of data directly affect the model's performance; therefore, both are crucial. The model can learn patterns better when the data is more diverse and representative.

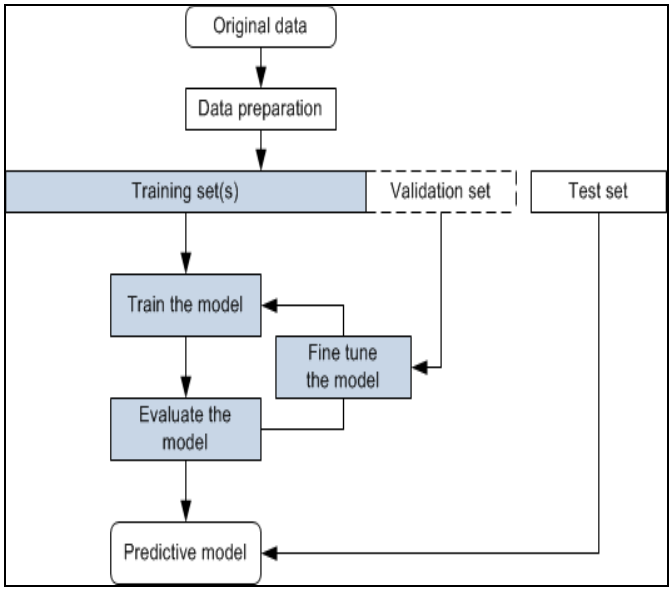

Fig -2: Proposed System

Data Analysis: Analyze the data and its parameters to identify any potential redundancies that may affect prediction results.

Data Preprocessing: Data preprocessing occurs after the data has been gathered. During this step, information is cleaned and prepared for analysis. This process involves addressing missing numbers, eliminating anomalies, and formatting the data accordingly. Clean data ensures the accuracy and reliability of the model.

Feature Engineering: Selecting or creating the most relevant features from the data is a crucial step in the feature engineering process. Techniques such as feature selection, extraction, and transformation can be utilized. The appropriate selection of features is vital for the accuracy of the predictive model's learning process.

The dataset is split into testing, validation and training sets during the data splitting phase. The validation set helps to adjust the model's parameters and prevent overfitting, whereas the training set is used to train the model. The testing set evaluates the model's performance using hypothetical data.

Model selection involves choosing an appropriate model architecture or machine learning method based on the problem type and data properties. Neural networks, support vector machines and decision trees represent typical models. These models serve as common examples.

Model Training: Selecting an appropriate model architecture or machine learning method depends on the problem type and data properties. Common models include neural networks, support vector machines, and decision trees.

Hyperparameter Tuning: To improve the model's effectiveness, its hyperparameters are adjusted. Techniques such as cross-validation and grid search aid in identifying the optimal set of hyperparameters.

Model Evaluation: Data from testing and validation is used to evaluate the model's performance. Evaluation measures such as mean squared error, accuracy, F1-score, precision, recall are used depending on the nature of the problem.

The machine learning process involves collecting and preprocessing data, engineering features, splitting data, selecting and training models, tuning hyperparameters, evaluating performance, and continually monitoring and maintaining them. It requires careful consideration at each stage to develop precise and dependable predictive models through an iterative process.

3.3 SDN dataset

The DDoS attack dataset is specifically tailored for SDN and is evolved through the use of the Mininet emulator. It serves the purpose of facilitating the classification of network traffic by using both deep learning and machine learning algorithms. The dataset creation process involves setting up ten different network configurations in mininet, with links connected to a single ryu controller. The simulated network will contain both benign traffic types like UDP, TCP and ICMP as much as capturing malicious traffic associated with TCP Syn.

In total, the dataset comprises 23 features. Some of these features are directly extracted from the switches, while others are calculated. The extracted features include:

1. Packet_count – indicating the numerous of packets
2. byte count - indicates the number of bytes within each packet
3. Switch-id – representing the ID of the switch
4. Duration_sec – reflecting the duration of packet transmission in seconds
5. Duration_nsec – indicating the duration of packet transmission in nanoseconds
6. Source IP – revealing the IP address of the source machine
7. Destination IP – specifying the IP address of the destination machine
8. Port Number – indicating the port number of the application
9. tx_byte - the number of bytes sent from the switch port
10. rx_byte - the number of bytes received on the switch port
11. dt field - captures date/time information, converted to a numeric format, and monitors flows at 30 second intervals.

The dataset also includes calculated features, which are derived from the raw data. These features are:

1. Byte Per Flow - shows the amount of bytes during a single flow.
2. Packet Per Flow - shows the count of packets during a single flow.
3. Packet Rate - shows the number of packets transmitted per second, calculated by dividing the packets per flow by the monitoring interval.
4. Number of Packet_ins messages– referring to messages generated by the switch and sent to the controller
5. Flow entries of switch – representing entries in the flow table of a switch, utilized for matching and processing packets
6. tx_kbps – indicating the speed of packet transmission (in kilobits per second)
7. rx_kbps - denoting the speed of packet reception (in kilobits per second)
8. Port Bandwidth – calculated as the sum of tx_kbps and rx_kbps, representing the overall bandwidth on the port.

3.4 Data Preprocessing

DDoS attack analysis and detection were conducted using a machine learning approach. The study employed an SDN-specific dataset, which comprises 23 features. The last column, known as the class label, provides the output feature. It categorizes traffic types as either benign or

malicious, with the latter being assigned a 1 label and the former a 0. The dataset consists of 104,345 instances. Null values were observed in rx_kbps and tot_kbps and were therefore removed for model development. Data processing steps, including data preparation and cleaning, One Hot encoding, and normalization, were completed. The resulting data frame had 103,839 instances with 57 features after One Hot encoding and was entered into the model.

4. PERFORMANCE EVALUTION AND RESULTS

The demonstrate the categorization of labels, the distribution of protocols for malicious attacks, and the modelling of accuracy using multiple algorithms, highlighting their superior performance. Moreover, it predicts the confusion matrix, differentiating between actual and false occurrences.

4.1 Classification of labels

A bar chart is produced to visually depict the dataset's composition in relation to two categories: 'benign' and 'malign', illustrated in chart-1. This chart determines the frequency of each category by percentage of the total data points and presents these percentages adjacent to the corresponding category labels. This chart functions as a useful tool for comprehending the distribution of categories among the dataset.

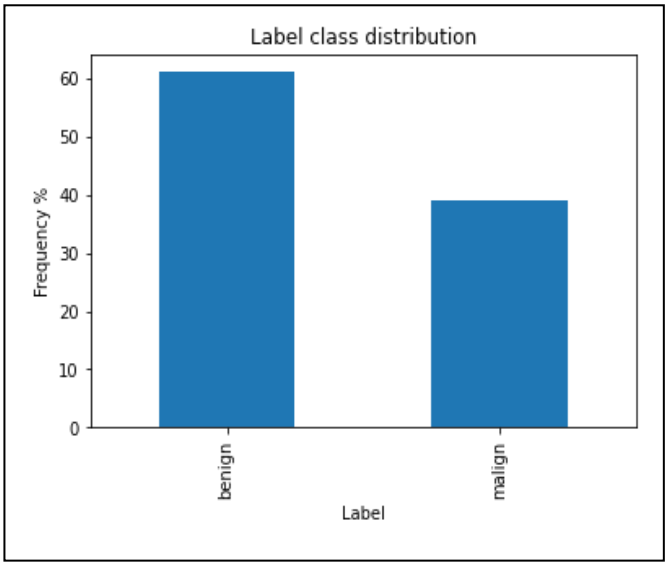

Chart -1: Classification of label

4.2 Analysis of Distribution of Protocol for Malign Attacks

The section produces a pie chart to display the distribution of protocols for malicious attacks, as illustrated in Chart-2, applying Matplotlib. The diagram's dimensions are predefined, and calculates the percentage distribution of various protocols (UDP, TCP, ICMP) involved in malign attacks in sdn dataset.

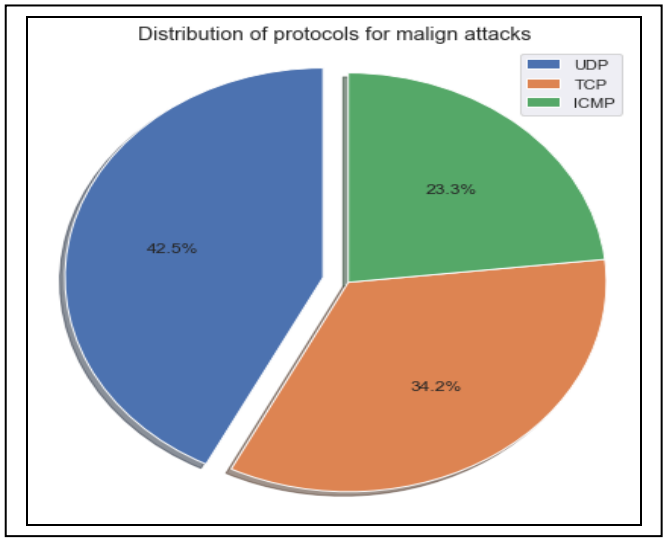

Chart -2: Distribution of Protocol for Malign Attacks

4.3 Analysis of Accuracy of Models

It first defines a list of classifier names and another list of accuracy scores as shown in Table-1

Table -1: Analysis of Accuracy of Models

Name	Analysis of accuracy
	Accuracy
DNN	99.1
XGBoost	98.1
SVM	97.4
Decision tree	96.6
KNN	96.4
SGD	83.9
Logistic Regression	83.6
Naïve Bayes	71.3
Quadratic	50.1

It then combines these lists into the Data Frame and sorts it in descending order based on accuracy. The text already adheres to the principles or lacks context: Finally, it displays the top 10 entries with the highest accuracy.

4.4 Classification Report

To assess a machine learning classifier's performance, a classification report is usually generated using the `classification report` function. As shown in Table-2. For each category in your target variable, it offers a variety of metrics, including support, recall, F1-score, and precision.

Table -2: Classification report

	Classification Report			
	Recall	***Precision***	***F1-score***	***Support***
benign	0.99	0.99	0.99	1882
malign	0.99	0.99	0.99	12270
accuracy			0.99	31152
macro avg	0.99	0.99	0.99	31152
weighted avg	0.99	0.99	0.99	31152

To assess the model's performance, we used various key metrics dedicated to offering valuable insights on the effectiveness of detecting anomalies.

1. True Positive (TP): Cases where the model correctly predicts the positive class and correctly identifies anomalies in the system.
False Positive (FP): instances where the model incorrectly predicts the positive class, suggesting anomalies where none exist.

2. Accuracy: A key metric for assessing the accuracy of positive predictions made by the model. Eq (1) calculates the ratio of correct positive results among all instances predicted as positive, providing a measure of the model's accuracy in identifying anomalies.

$$Precision = TP/(TP+FP) \quad (1)$$

3. Recall, also referred to as Sensitivity or True Positive Rate, quantifies the model's ability to accurately identify all positive instances. Eq (2) computes the proportion of true positive cases to the sum of true positives and false negatives.

$$Recall = TP/(TP+FN) \quad (2).$$

4. F1_score: This metric examines false positives and false negatives. It calculates the symmetric mean of precision and recall. Eq (3) represents the model's balanced performance with the F1 Score.

$$F1\ score = 2* (precision * recall) / (precision + recall) \quad (3)$$

5. Support Score: The support score, a metric from the scikit-learn Python library, shows the frequency of every genuine label in the dataset and the number of instances that fall under each label marked as genuine.

4.5 Confusion Matrix

A confusion matrix is a table that is often used to describe the performance of a classification model on a set of data for which the true values are known. It's a way to understand how well the model is classifying instances into different classes. The confusion matrix provides a more detailed view of the performance of a classification model than accuracy alone as illustrated in Chart-3.

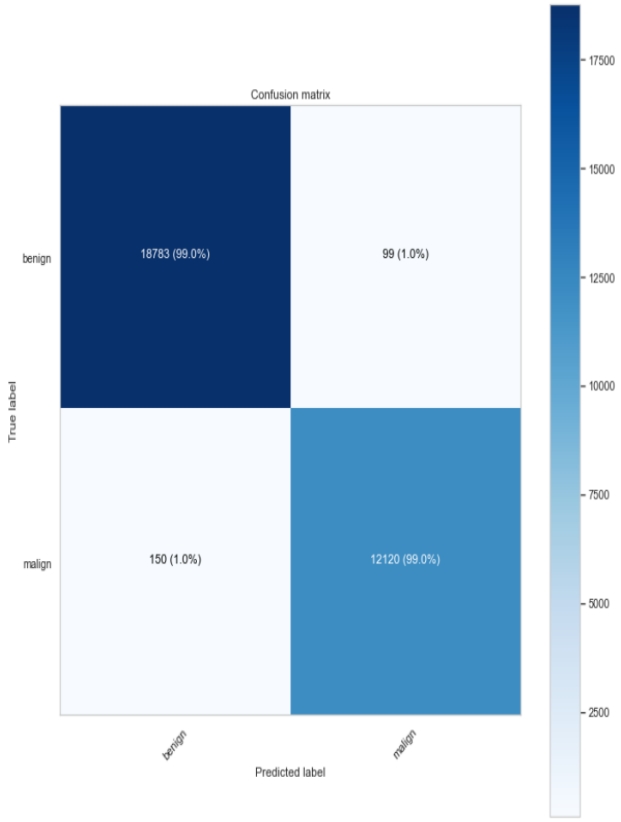

Chart -3: Confusion Matix

5. CONCLUSION AND WAY FORWARD

Deep Neural Network (DNN) algorithms have demonstrated high accuracy in detecting DDoS attacks. This makes them a valuable and efficient solution for improving network security against these specific cyber threats. This project outlines a methodology for systematically detecting DDoS attacks, beginning with the selection of a DDoS dataset containing attack statistics. Using machine learning techniques, we analyzed a specialist SDN dataset with 23 features to identify DDoS attacks. The final column determined whether the traffic was benign (labelled as 0) or

malicious (labelled as 1), resulting in 104,345 instances. These were then used as training data for our proposed Deep Neural Network model. Our model was found to be more effective than the baseline classifiers, achieving an impressive precision of 99.38%. Comparatively, Boost achieved an accuracy of 98.17%, providing evidence of a notable improvement of around 1.21%.

REFERENCES

[1] N. H. D. Sai, B. H. Tilak, N. S. Sanjith, P. Suhas and R. Sanjeetha, "Detection and Mitigation of Low and Slow DDoS attack in an SDN environment," 2022 International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Shivamogga, India, 2022, pp. 106-111, doi: 10.1109/DISCOVER55800.2022.9974724.

[2] M. F. Sidiq, N. Iryani, A. I. Basuki, A. I. Haris and R. A. Ferianda, "Feasibility Evaluation of Compact Flow Features for Real-time DDoS Attacks Classifications," 2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), Solo, Indonesia, 2022, pp. 350-355, doi: 10.1109/COMNETSAT56033.2022.9994323.

[3] M. D. T. Bennet, M. P. S. Bennet and D. Anitha, "Securing Smart City Networks - Intelligent Detection of DDoS Cyber Attacks," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1575-1580, doi: 10.1109/IC3I56241.2022.10073271.

[4] K. Shukla and A. Sharma, "Classification and Mitigation of DDOS attacks Based on Self-Organizing Map and Support Vector Machine," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-5, doi: 10.1109/ISCON57294.2023.10111988.

[5] Vikash C Pandey, Sateesh K Peddoju and Prachi S Despande. (2018), 'A statistical and distributed packet filter against DDoS attacks in Cloud environment', in 'Sådhanå', Vol. 43, Num. 3, pp. 1–9.

[6] S. Tufail, S. Batool and A. I. Sarwat, "A Comparative Study of Binary Class Logistic Regression and Shallow Neural Network for DDoS Attack Prediction," Southeast Con 2022, Mobile, AL, USA, 2022, pp. 310-315, doi: 10.1109/SoutheastCon48659.2022.9764108.

[7] H. Mateen and M. Shahzad, "Factors Effecting Businesses due to Distributed Denial of Service (DDoS) Attack," 2021 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 2021, pp. 1-7, doi: 10.1109/ICIC53490.2021.9692965.

[8] U. Garg, M. Kaur, M. Kaushik and N. Gupta, "Detection of DDoS Attacks using Semi-Supervised based Machine Learning Approaches," 2021 2nd International Conference on Computational Methods in Science & Technology (ICCMST), Mohali, India, 2021, pp. 112-117, doi: 10.1109/ICCMST54943.2021.00033.

[9] W. Jia, Y. Liu, Y. Liu and J. Wang, "Detection Mechanism Against DDoS Attacks based on Convolutional Neural Network in SINET," 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 2020, pp. 1144-1148, doi: 10.1109/ITNEC48623.2020.9084918.

[10] P. R. Pardhi, J. K. Rout and N. K. Ray, "A Study on Performance Comparison of Algorithms for Detecting the Flooding DDoS Attack," 2022 OITS International Conference on Information Technology (OCIT), Bhubaneswar, India, 2022, pp. 433-438, doi: 10.1109/OCIT56763.2022.00087.

[11] J. Dalvi, V. Sharma, R. Shetty and S. Kulkarni, "DDoS Attack Detection using Artificial Neural Network," 2021 International Conference on Industrial Electronics Research and Applications (ICIERA), New Delhi, India, 2021, pp. 1-5, doi: 10.1109/ICIERA53202.2021.9726747.

[12] R. Yadav, A. P. Jain, S. T, A. Rajesh, S. Perumal and G. Eappen, "AI based DDOS Attack Detection of SDN Network in Mininet Emulator," 2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN), Vellore, India, 2023, pp. 1-4, doi: 10.1109/ViTECoN58111.2023.10157074.

[13] B. Mladenov, "Studying the DDoS Attack Effect over SDN Controller Southbound Channel," 2019 X National Conference with International Participation (ELECTRONICA), Sofia, Bulgaria, 2019, pp. 1-4, doi: 10.1109/ELECTRONICA.2019.8825601.

[14] D. Satyanarayana and A. S. Alasmi, "Detection and Mitigation of DDOS based Attacks using Machine Learning Algorithm," 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2022, pp. 1-5, doi: 10.1109/ICCR56254.2022.9995773.

[15] M. Li, B. Zhang, G. Wang, B. ZhuGe, X. Jiang and L. Dong, "A DDoS attack detection method based on deep learning two-level model CNN-LSTM in SDN network," 2022 International Conference on Cloud Computing, Big Data Applications and Software Engineering (CBASE), Suzhou, China, 2022, pp. 282-287, doi: 10.1109/CBASE57816.2022.00062.

[16] M. A. Msaad, R. A. Saed and A. M. Sllame, "A Simulation based analysis study for DDoS attacks on Computer Networks," 2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA, Tripoli, Libya, 2021, pp. 756-761, doi: 10.1109/MI-STA52233.2021.9464444.