[1],*Aditya Kumar Shukla

[2]Ashish Sharma

[3]Sandeep Singh Sengar

Enhancing DDoS Attack Detection with Multi-Layer Perceptron Algorithms: A Machine Learning Approach Using the CICDDoS2019 Dataset

Abstract: **-** There has been a consistent rise in malware assaults with the growing trend of digital transformation across many industries. These attacks, which target networks or applications, result in data theft or service disruptions, ultimately affecting the consumer experience. The internet is continually challenged by Distributed Denial of Service (DDoS) assaults, affecting every business that depends on it. Through the use of a variety of machine learning techniques, we show in this work how they can reliably identify distributed denial of service assaults. We demonstrate that multi-layer perceptron (MLP) algorithms are successful in detecting distributed denial of service attacks (DDoS) in computer networks with a high degree of precision. The CICDDoS2019 dataset, which is extensively used, has been utilized for the training and testing of the MLP algorithms. Our suggested model is experimentally shown to provide a high level of accuracy, around 97.37 percent.

Keywords: DdoS, Network traffic, Security Attack Detection, MLP , Cloud Computing

I. INTRODUCTION

All The rapid expansion of the internet may be attributed to the increasing network traffic resulting from the integration of many devices, including remote sensors, 5G data transfer, intelligent gadgets and cloud computing [1]. The global internet user population now stands at around 4.66 billion, accounting for 59.5% of the entire global population. Similarly, a majority of the global population, namely 53.6%, engage in social media, while 66.6% use cellphones. Denial of Service (DoS) attacks have the goal of causing disruption by making a service or system unavailable. Conversely, deception attacks include manipulating and misleading, whereas replay attacks are focused on intercepting and reusing legal data in order to obtain unauthorized access to or manipulate systems. As the system becomes more complicated, it becomes necessary to analyze its vast array of characteristics [2]. As computer network technologies advance rapidly and internet technology evolves at an even faster pace, people are becoming increasingly aware of the importance of network security [3]. Moreover, Denial of Service (DoS) attacks are closely associated with infringements on user privacy and compromised security [4]. Typically, two types of DoS attacks are causing concern, namely DoS and DDoS attacks. DDoS assaults sometimes include the coordination of several devices located in various areas. The assault might result in unusual activity that disrupts the normal flow of data on certain servers, services, and networks due to an overwhelming inflow of data from neighboring infrastructure. This atypical behavior generates an overwhelming influx of service requests to the servers and networks, posing challenges in discerning a reliable source [5][6]. Recently, machine learning has proven to be an effective tool for securing the cloud. By training machine learning algorithms on various legitimate datasets, we can develop models that automate the detection of cloud attacks with greater accuracy than any other technology[7]. DDoS attacks, also known as distributed denial of service (DDoS) attacks, are a severe threat that can significantly impact network availability[8][9]. The DoS assault is widely recognized as one of the most prevalent forms of cyber-attacks on the Internet. It is accomplished by compelling a hijacked computer to initiate or deplete its resources, such as CPU cycles, memory, and network bandwidth. DDoS has emerged as a prominent obstacle in the field of cyber security in the present day. Despite the collective efforts of both business and academics, the issue of DDoS attacks remains unresolved. The method and degree of DDoS attacks have been continuously evolving in recent years, thanks to

[1,2] GLA Department of Computer Engineering and Applications, GLA University, NH#2, Delhi Mathura Highway, Post Ajhai, Mathura (UP) India

[3]Department of Computer Science; Cardiff School of Technologies, Cardiff Metropolitan University, UK

[1]uraditya@gmail.com , [2]ashishs.sharma@gla.ac.in , [3]sssengar@cardiffmet.ac.uk

*Corresponding author email : **uraditya@gmail.com**

the advancement in attack detection capabilities. The advent of Big Data technologies has significantly increased the challenge of safeguarding the network from diverse DDoS assaults. The exponential increase in network traffic renders earlier detection approaches ineffective in identifying network attack activity among such vast volumes of data. Figure 1 depicts a high-speed network experiencing a DDoS assault. In addition, researchers have significant obstacles when dealing with DDoS assaults, mostly owing to the high network velocity and the diverse array of data entering the network [10]. Multiple strategies for detecting DDoS attacks have been suggested, with two prevalent kinds of detection: abuse detection and anomalous detection [11][12]. Both detection algorithms have restrictions pertaining to the parameters used for identifying network patterns. Misuse detection has the benefit of achieving a high level of accuracy, but it necessitates having comprehensive knowledge about the network. However, anomalous detection does not need acquiring previous knowledge of the network. Nonetheless, this method does not give the same level of accuracy as abuse detection [13].

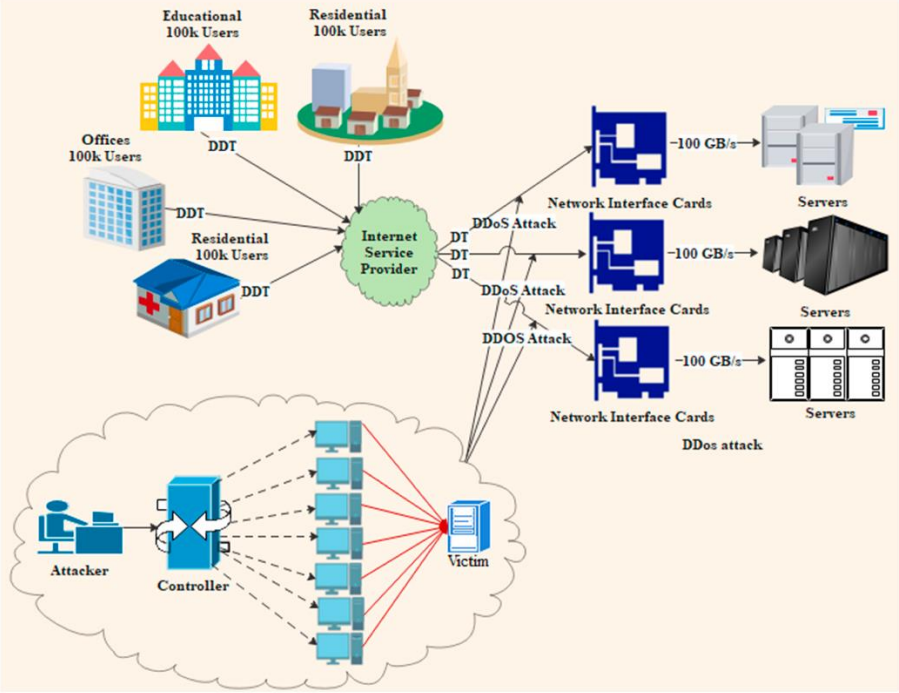

Figure 1. DDoS assault on a high speed network [1].

II. Related Work

Bhayo et al., (2023)[14] examined that the IoT is an intricate and varied network comprising of sensors/devices/things that have limited resources and are susceptible to different security risks, namely DDoS attacks. The combination of SDN with IoT has recently become a potential method for enhancing security and access control measures. Nevertheless, DDoS assaults persist as a substantial menace to IoT networks, since they may be carried out via botnet or zombie attacks. This research presents a machine learning approach to detecting DDoS in an SDN-WISE Internet of Things controller. A detecting module that makes use of machine learning has been included into the controller we have developed. In addition to this, we have created a testbed environment in order to simulate the operation of a distributed denial of service application. In order to determine whether or not the suggested structure is effective, we conduct tests with a variety of traffic simulation situations and compare the outcomes that are produced by the machine learning detection of DDoS module. The actual results reveal that the suggested methodology is highly effective in identifying DDoS assaults within the context of SDN-WISE IoT.

Saini et al., (2023)[15] studied an advanced persistent threat (APT) assault refers to a deliberate and sustained cyber-attack that is specifically aimed at a target. The primary objective of the assault is to acquire confidential data, seize control of the system, and generate financial profits. This poses significant obstacles and difficulties for organizations in their efforts to avoid, detect, and recover from such attacks in the present day. Given the inherent characteristics of Advanced Persistent Threat (APT) assaults, their prompt detection poses a significant challenge. Thus, machine learning methods are used in various study domains. This research employs advanced deep and

machine learning models, including random forest, decision tree, CNN, to accurately classify and identify APT assaults. XGBoost and random forest are two different types of classifiers that are combined in this work to create a unique hybrid ensemble machine learning model. In the literature, these results are contrasted with other recent study that is essentially identical to the one being discussed here. Our model has shown a much-improved performance across all datasets, as demonstrated by the results of our experiment.

Raza et al., (2023)[16] intended that the purposeful exploitation of vulnerabilities in computer networks is an example of network assaults. The goal of these attacks is to gain unauthorized access to sensitive information, degrade network security, or disrupt operations. The objective of our proposed study is to efficiently and promptly identify network threats in order to mitigate any damages. We used the CICIDS2017 benchmark dataset to develop sophisticated machine learning techniques based on artificial intelligence. We provide a new method called Class Probability Random Forest (CPRF) to improve the efficiency of network attack detection. We generated a unique collection of features by using the suggested CPRF methodology. The CPRF method utilizes the network attack dataset to make predictions about class probabilities. These probabilities are then used as features for constructing applicable machine learning techniques. The extensive study findings clearly showed that the random forest strategy surpassed the current leading approach with an exceptional accuracy rate of 99.9%. The effectiveness of each deployed technique is verified using a k-fold methodology and improved through hyper-parameter tweaking. Our innovative research has completely transformed the field of network attack detection, successfully thwarting unwanted access, service interruptions, theft of critical information, and loss of data integrity.

Revathi et al., (2023)[17] examined an analysis is conducted on the effects of a DDoS assault on SDN. Multiple methodologies for identifying DDoS assaults are available, which differ based on the specific characteristic being analyzed and the strategy used. However, the approaches exhibit a shortcoming in effectively identifying and mitigating DDoS assaults. The present paper presents a proposed model called RMCARTAM (Real-time Multi-Constrained Adaptive Replication and Traffic Approximation Model) to enhance the performance of SDN. The RMCARTAM evaluates several factors or limitations while executing different controllers that manage incoming packets. The concept incorporates numerous controllers to manage network traffic, while also allowing for the flexibility to adjust the controllers as needed. The identification of a DDoS assault is performed by assessing the volume of incoming traffic to a certain service and examining several attributes such as hop count, payload, service frequency, and faulty frequency. The technique enhances network performance by modulating the controller based on various parameters, hence decreasing the power factor and thereby cutting costs. Similarly, the suggested approach enhances the precision of identifying DDoS assaults by evaluating the characteristics of incoming data in various contexts. “

Sambanghi et al., (2022)[18] suggested the advancements in artificial intelligence and machine learning have facilitated the emergence of the fourth industrial revolution, sometimes referred to as Industry 4.0. The Industry 4.0 is advancing rapidly, exceeding the velocity of previous revolutions seen by mankind. Industry 4.0 is based on the fundamental principles of Cyber Physical Systems and Cloud computing. An ongoing challenge in cloud computing is the pressing need to address security and data availability issues that occur in modern networking systems. DDoS assaults in cloud provide continuing research problems for the network community in terms of cloud security, since they regularly present new obstacles for detection. The performance assessment of the proposed machine learning model SWASTHIKA is conducted by taking into account many classifier evaluation metrics, including accuracy, precision, detection rate, and F-Score. The experimental findings shown that SWASTHIKA has a notably superior assault detection rate in comparison to contemporary machine learning classifiers.”

Gaur et al., (2022)[19] stated that the objective of a DDoS attack is to threaten network security by inundating target networks with malicious traffic from multiple sources. Although various traditional techniques have been suggested for identifying DDoS attacks, promptly detecting such attacks using feature selection algorithms remains challenging. The proposed system employs a hybrid approach to feature selection, integrating feature selection techniques with machine learning classifiers. The CICDDoS2019 dataset, which includes a wide range of DDoS attacks, is used to train and evaluate the proposed approach in a cloud-based environment. According to the experimental results, the hybrid approach demonstrates exceptional performance, reducing features by 82.5% and achieving an accuracy of 98.34% using ANOVA for XGBoost. Additionally, it aids in the timely detection of DDoS attacks on IoT devices.

Esmaeili et al., (2022)[20] assessed that the IoT is a complex security mechanism that preserves datagrams by providing security, privacy, and authentication services. The network is safeguarded against external disruptions

and invasions. Due to the many technologies and long-term data processing of IoT devices, conventional solutions may not be feasible. Developing intelligent methods that may be applied to various levels of data flow in the system is crucial. This paper investigates the use of deep learning-based Intrusion Detection Systems (IDS) to analyze metainnovations. According to the results of previous testing, BiLSTMs are more effective for classifying data into two categories (regular/attacker). On the other hand, sequential models (LSTM or BiLSTM) are more suitable for identifying severe assaults in classifiers that have many categories. Experts assert that contemporary intrusion detection systems, which use deep learning techniques, has the ability to identify and choose for the most optimal configuration for each category. Nevertheless, future challenges will need resolution. The BiLSTM technique has selected the most secure instances with the best level of accuracy among the models. The BiLSTM design is determined to be the most dependable and appropriate approach for assessing DDoS assaults in IoT, based on the research results.

Revathi et al., (2021)[21] analyzed that SDN has emerged as a novel network technology that has exceptional programming capabilities, allowing network operators to dynamically configure and govern their networks. SDN, or Software-Defined Networking, is a widely studied field that focuses on defending against SDN attacks and identifying and preventing DDoS threats inside the SDN framework. Many academics have been exploring these topics since the emergence of SDN assaults. However, it is important to ensure that security threats are sufficiently safeguarded. “This study proposes a discrete and scalable memory-based support vector machine algorithm for detecting DDoS threats and a software-defined networking (SDN) mitigation architecture for identifying and countering attacks. The proposed technique successfully accomplishes the mitigation of attack traffic and the discarding of benign traffic. We have assessed the whole procedure using the KDD dataset. The recommended network model underwent training and was then deployed in an SDN threat detection and prevention scenario as part of the assessment process. The findings demonstrate that the suggested mechanism surpasses the other examined algorithms, attaining an exceptional accuracy rate of 99.7%, specifically in relation to the duration of training and testing on the KDD dataset.

Chen et al., (2020)[22] studied that DDoS assaults often occur inside cloud servers, resulting in severe disruptions. Nevertheless, the growing prevalence of IoT devices necessitates our acknowledgment of the significant impact posed by large-scale DDoS assaults originating from IoT devices. This study presents a machine learning-driven system for detecting DDoS attacks in a multi-layer IoT environment. The system encompasses IoT devices, IoT gateways, SDN switches, and cloud servers. Initially, we construct a total of eight intelligent poles equipped with diverse sensors on our campus. These sensors enable us to gather valuable data, which we get either via wireless or wired networks. Subsequently, we derive the characteristics by considering the various forms of DDoS attacks. Feature selection may lead to improved accuracy in detecting DDoS attacks in the actual IoT environment. The empirical findings demonstrate that our multi-layer DDoS detection system have the capability to precisely identify DDoS assaults. The SDN controller can efficiently obstruct malicious devices based on blacklists derived from our IoT DDoS attack detection system.

Tuan et al., (2020)[23] analyzed that the botnet is now considered one of the most advanced and dangerous security vulnerabilities. Botnets exert significant control over a substantial amount of network traffic. Botnets are networks of compromised computers, known as bots, that are controlled remotely by their creator, known as the botmaster, via a command-and-control infrastructure. This research conducted an empirical investigation of the machine learning techniques used for detecting Botnet DDoS attacks. The evaluation is performed using the UNBS-NB 15 and KDD99 datasets, which are well acknowledged datasets used for the detection of Botnet DDoS assaults. The research analyzes the precision, rate of false alarms, sensitivity, specificity, rate of false positives, area under the curve, and Matthews's correlation coefficient of datasets employing frequently used machine learning algorithms such as SVM, ANN, Naive Bayes (NB), DT, and Unsupervised Learning (USML). The empirical findings indicate that the KDD99 dataset outperforms the UNBS-NB 15 dataset in terms of performance. This validation has significant significance in the field of computer security and its related fields.

Ajeetha et al., (2019)[24] stated that DDoS attacks often originate from either the application layer or the network layer, where the systems of the victims and attackers are linked inside a network. DDoS attacks may have severe consequences for large businesses and banking industries, including reputational harm, decreased production, financial losses, and even theft. Therefore, it is essential to implement an effective DDoS detection and protection solution. The primary objective is to provide an optimal solution for these issues via feature analysis. Therefore, it is essential to implement an effective DDoS detection and protection method. The primary objective is to provide

the most effective solution for these issues via feature analysis. When encountering a high volume of traffic at the intended server, it is crucial to differentiate between malicious attacks and lawful access. Hence, a unique technique has been suggested for identifying DDoS assaults by analyzing the traces in the network flow. A confusion matrix has been generated based on these traces. The Naive Bayes and Random Forest classifiers are used to classify traffic as either abnormal or normal, using the normal and attack patterns obtained from pre-existing datasets. The Naive Bayes algorithm produces greater results in comparison to the Random Forest approach.

Deepa et al., (2019)[25] analyzed that SDN is an innovative method for constructing computer network architecture that is characterized by its dynamic, adaptive, controllable, and cost-effective nature. The SDN paradigm provides virtualized network services, facilitating an architecture that is compatible with existing networks that use infrastructure-hosted services computing. In the context of SDN, switches do packet matching in the flow tables, but they do not carry out any processing on the packets. Denial of Service (DoS) attacks occur when a network is overwhelmed by a high volume of packets delivered by compromised devices. A kind of attack known as DDoS involves several hacked workstations targeting a single entity concurrently. This paper introduces an innovative ensemble approach that incorporates many machine learning approaches, such as KNN, Naive Bayes, SVM, and Self-Organizing Map (SOM), to detect anomalous data traffic patterns in the SDN controller. The experimental results indicate that the ensemble approach in machine learning achieves higher levels of accuracy, detection rate, and false alarm rate in comparison to a single learning technique.

III. PROBLEM FORMULATION

The increasing frequency and sophistication of DDoS attacks pose a substantial threat to the stability and availability of online services. As organizations rely heavily on digital infrastructure, the need for robust DDoS detection systems has become imperative. Traditional methods often fall short in swiftly identifying and mitigating these attacks, leading to prolonged downtimes and potential data breaches. To address this challenge, there is a critical demand for the design and implementation of a DDoS Attack Detection System leveraging advanced Network Traffic Behavioral Analytics. This system should be capable of analyzing patterns and anomalies in network traffic in real-time, utilizing machine learning algorithms to discern normal behavior from malicious activity. The goal is to enhance the overall cybersecurity posture of organizations by providing an intelligent and proactive defense mechanism against DDoS attacks, ensuring the uninterrupted and secure operation of critical online services.

IV. RESEARCH METHODOLOGY

The objective of this research is to design a DDoS detection using network traffic analysis. This is done with the intention of better analyzing network traffic activities for the purpose of detecting cyber threats. In addition, one of our key objectives is to identify a feature selection technique that, when coupled with a machine learning system, has the potential to enhance the accuracy rates of DDoS detection.

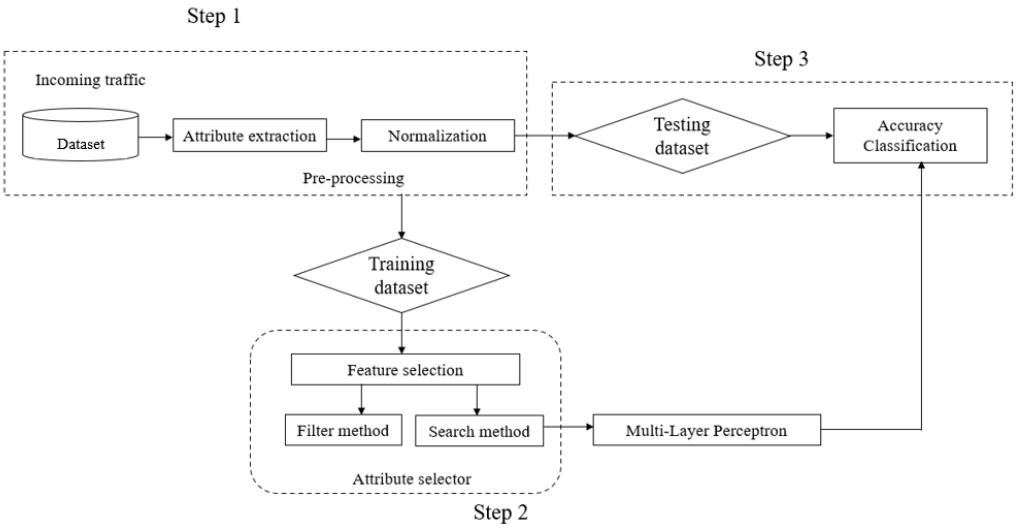

Figure 2. Proposed framework

The proposed framework is described in steps which is follow as:

Step 1: The Pre-processing step includes the gathering and standardization of characteristics from network traffic. The data is partitioned into several subsets for the purposes of training and testing. 80% of the data in CICDDoS2019 is allocated as a training dataset for the attribute selector in Step 2, while the remaining 20% is designated as the test dataset for Step 3.
Step 2: The attribute selection subsystem employs many automated threshold processes to ascertain the minimal number of characteristics. To achieve a more pragmatic arrangement of the outcomes, all the studies were categorized into three distinct phases, as seen in Figure 2. Two tests were conducted during Step 1. The experiments were done using estimators configured with their default defaults. No further parameter optimization or feature selection was performed in this case; instead, a simple percentage split strategy was used. In step 2, a sequence of feature selection trials was conducted. Once again, the use of a percentage split approach was done without considering cross-validation. During Step 2, a series of tests involving a feature selection operation were conducted.
Step 3: (Classification and detection of DDoS) In the third and last step, the classification is responsible for identifying as DDoS traffic data. It was possible to successfully achieve the outcomes of steps 1, 2, and 3. Along with a mix of features selection, adam optimizer, mean absolute error, and oneHotEncoder method, the suggested machine learning model enhanced the approaches to DDOS attack detection and raised the accuracy of DDOS detection overall. After being included into the module, there are consequently test accuracy results.

A. Techiniques(Multi-Layer Perceptron (MLP))

The Multi-Layer Perceptron operates on data that is not amenable to linear separation. Given the ever-changing nature of the current environment, its supplementary benefit proves to be useful. The Multi-Layer Perceptron is a kind of Artificial Neural Network (ANN) that operates in a feed-forward manner. It does this by transmitting the weights associated with each unit (neuron) to the subsequent layer. The layer might be any of the hidden layers, input layer, or output layer. Furthermore, there is a summation function that computes the weighted sum and incorporates a global bias at the conclusion, as well as an activation function that maps the weighted inputs to the outputs. Inputs are translated into outputs using a feed-forward neural network, which is referred to as MLP. As depicted in figure 3, a typical network comprises three layers: a hidden layer or layers, an input layer, and an output layer.

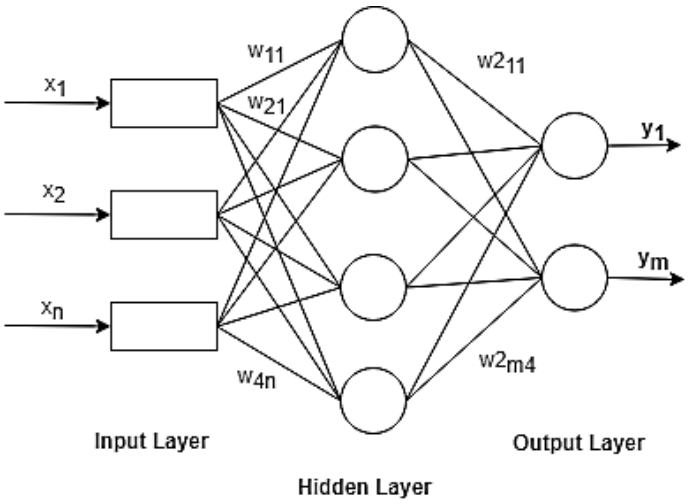

Figure 3. The structure of MLP [26].

Where x represents a node as well as the input layer, y is the output layer, and wi,j represents the weight, and i, j = 1,2, 3.
The operations of a single neuron (or node) in an MLP can be mathematically represented as follows:

$$z = \sum_{i=1}^{n}(w_i \times x_i) + b \qquad (1)$$

$$a = f(z) \qquad (2)$$

Where;
z is the weighted sum of inputs and biases.

w_i are the weights.
x_i is the inputs.
b is the bias
f is the activation function.

B. Algorithm to apply MLP on Network data:

1. Initialize the MLP model: a) Define the architecture (number of layers, neurons per layer, activation functions).
b)Initialize weights and biases for each neuron.
2. Preprocess the data: a) Normalize the input features. b) Split the data into training and test sets.
3. Training:
For each epoch do:
For each training sample (X, y) do:
- Forward propagation: a) Compute the weighted sum and activation for each neuron in each layer. b) Compute the output of the network.
- Compute the loss: Compute the loss function (e.g., cross-entropy loss) between the predicted output and the actual label.
- Backward propagation: a) Compute the gradients of the loss with respect to the weights and biases using backpropagation. b) Update the weights and biases using gradient descent:
*w = w - learning_rate * gradient_w*
*b = b - learning_rate * gradient_b*
4. Evaluation:
For each test sample (X_test, y_test) do:
- Use the trained model to predict the output.
- Compute the accuracy, precision, recall, F1-score, etc., to evaluate the model's performance.
5. Deployment:
- Deploy the trained MLP model in the production environment for real-time DDoS detection
- Monitor the model's performance and retrain or fine-tune as needed

C. Data Description

During this investigation, the data set that was used was CICDDoS2019 [https://data.mendeley.com/datasets/ssnc74xm6r/1]. In order to train algorithms and categorize distributed denial of service attacks (DDOS) based on their distinctive characteristics, this data collection is used. Over eighty different network flow characteristics are included in the data that is included in the "CICDDoS2019" dataset. It is then divided into 80% of the training data set and 20% of the test data set by the use of random splits, which are done on the data.

V. RESULT AND DISCUSSION

Figure 4 shows the comparison of label columns as shown below. In this Figure, there are various labels used such as BENIGN, LDAP, MSSQL, NetBIOS, Portmap, Syn, UDP, and UDPLag. Each bar represents the percentage of label columns for a specific value.

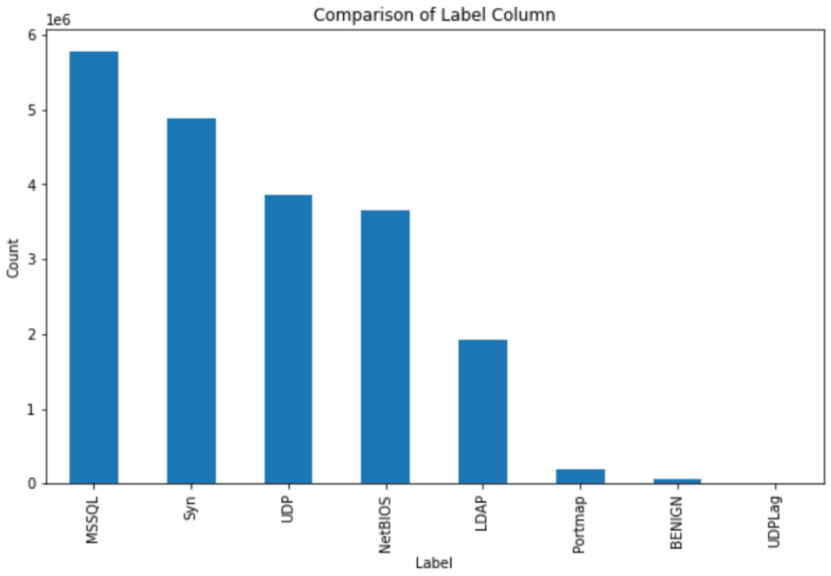

Table 1. Classification report

Table 1 shows the classification report as shown below. The performance metrics such as precision, recall, and f1 score has been described on different labels with their values. The precision, recall, and f1 score of MLP classifier is 0.99 at BENIGN, 1.00 at LDAP, 1.00 at Syn, 1.00 at UDP labels and show on various labels. The accuracy of MLP classifier is 0.98 as shown below.

Labels	Precision	Recall	F1-score
BENIGN	0.99	0.99	0.99
LDAP	1.00	1.00	1.00
MSSQL	0.93	0.84	0.88
NetBIOS	0.95	1.00	0.97
Portmap	0.44	0.00	0.01
Syn	1.00	1.00	1.00
UDP	1.00	1.00	1.00
UDPLag	0.42	0.16	0.24

Accuracy 0.98

Figure 5 depict the classification report of MLP classifier as shown below. This figure expressed in terms of precision, recall, and f1 score value of MLP classifier.

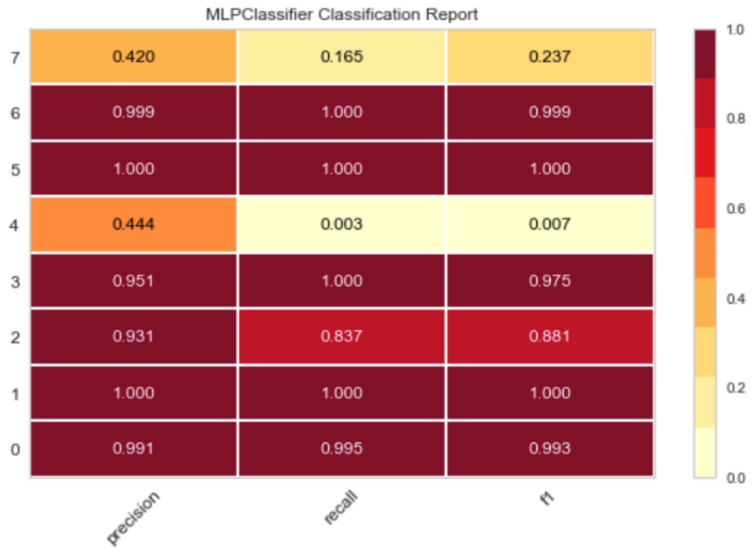

Figure 5 MLP classification report

VI. Conclusion and Future Work

The study has concentrated on showcasing and validating the design, execution, and evaluation of a Machine Learning-based solution for Detecting DDoS assaults. The aim is to provide end-users a detection mechanism that utilizes machine learning techniques. End-users have the ability to redirect all network traffic to an external server that is equipped with DDoS mitigation capabilities. The provided model solution enables researchers to construct network-based detection models for network threats using several machine learning techniques, mostly classification. The purpose of examining the kind and features of a DDoS assault from a machine learning perspective has been effectively accomplished, as seen by this result. Based on the analysis of the outcomes obtained from the implemented machine learning technique, it can be concluded that the MLP algorithm significantly improved the identification of DDoS assaults. The study suggests three components: pre-processing, attribute selection, and a detection and prevention mechanism. Extensive testing was conducted, and the results indicate that MLP significantly outperforms current DDoS attack detection systems. The method achieves a 98% accuracy when identifying the patterns in the dataset. The results of this study focused on achieving the goals of enhancing DDoS attack detection methods through the utilization of a machine learning model for analyzing network traffic patterns in order to identify cyber threats. Additionally, the study aimed to identify a feature selection strategy that, when integrated with a machine learning system, can enhance the accuracy of DDoS detection. For future study, we propose using sophisticated deep learning algorithms to construct a predictive analytics model. This model would enable the development of an automated system capable of responding to real-time circumstances by analyzing incoming data in networks.

References

[1] Haseeb-Ur-Rehman, Rana M. Abdul, Misbah Liaqat, Azana Hafizah Mohd Aman, Siti Hafizah Ab Hamid, Rana Liaqat Ali, Junaid Shuja, and Muhammad Khurram Khan. "Sensor cloud frameworks: state-of-the-art, taxonomy, and research issues." IEEE Sensors Journal 21, no. 20 (2021): 22347-22370.

[2] Shukla, Aditya Kumar, and Ashish Sharma. "Reduce false intrusion alerts by using PSO feature selection in NSL-KDD dataset." (2023): 226-231.

[3] Shukla, Aditya Kumar, and Ashish Sharma. "Cloud Base Intrusion Detection System using Convolutional and Supervised Machine Learning." In 2023 6th International Conference on Information Systems and Computer Networks (ISCON), pp. 1-5. IEEE, 2023.

[4] Cisco, U. "Cisco annual internet report (2018–2023) white paper." Cisco: San Jose, CA, USA 10, no. 1 (2020): 1-35.

[5] Li, Qian, Linhai Meng, Yuan Zhang, and Jinyao Yan. "DDoS attacks detection using machine learning algorithms." In Digital TV and Multimedia Communication: 15th International Forum, IFTC 2018, Shanghai, China, September 20–21, 2018, Revised Selected Papers 15, pp. 205-216. Springer Singapore, 2019.

[6] [6]. Yusof, Ahmad Riza'ain, Nur Izura Udzir, and Ali Selamat. "Systematic literature review and taxonomy for DDoS attack detection and prediction." International Journal of Digital Enterprise Technology 1, no. 3 (2019): 292-315.

[7] Shukla, Aditya Kumar, and Ashish Sharma. "Distributed Attacks Classification Based on Radical Basis Function and Particle Swarm Optimization In Hypervisor Layer." In 2023 6th International Conference on Information Systems and Computer Networks (ISCON), pp. 1-4. IEEE, 2023.

[8] Shukla, Aditya Kumar, and Ashish Sharma. "Classification and Mitigation of DDOS attacks Based on Self-Organizing Map and Support Vector Machine." In 2023 6th International Conference on Information Systems and Computer Networks (ISCON), pp. 1-5. IEEE, 2023.

[9] Shukla, Aditya Kumar, and Ashish Sharma. "Cloud Data Security by Hybrid Machine Learning and Cryptosystem Approach." International Journal of Intelligent Systems and Applications in Engineering 12, no. 2s (2024): 01-14.

[10] El Sayed, Mahmoud Said, Nhien-An Le-Khac, Marianne A. Azer, and Anca D. Jurcut. "A flow-based anomaly detection approach with feature selection method against ddos attacks in sdns." IEEE Transactions on Cognitive Communications and Networking 8, no. 4 (2022): 1862-1880.

[11] Papalkar, Rahul Rajendra, and Abrar S. Alvi. "Analysis of defense techniques for DDos attacks in IoT–A eview." ECS Transactions 107, no. 1 (2022): 3061.

[12] Naqvi, Ila, Alka Chaudhary, and Anil Kumar. "A systematic review of the intrusion detection techniques in VANETS." TEM Journal 11, no. 2 (2022): 900.

[13] Almansor, M., and K. B. Gan. "Intrusion detection systems: principles and perspectives." Journal of Multidisciplinary Engineering Science Studies 4, no. 11 (2018): 2458-2925.

[14] Bhayo, Jalal, Syed Attique Shah, Sufian Hameed, Awais Ahmed, Jamal Nasir, and Dirk Draheim. "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks." Engineering Applications of Artificial Intelligence 123 (2023): 106432.

[15] Saini, Neeraj, Vivekananda Bhat Kasaragod, Krishna Prakasha, and Ashok Kumar Das. "A hybrid ensemble machine learning model for detecting APT attacks based on network behavior anomaly detection." Concurrency and Computation: Practice and Experience 35, no. 28 (2023): e7865.

[16] Raza, Ali, Kashif Munir, Mubarak S. Almutairi, and Rukhshanda Sehar. "Novel class probability features for optimizing network attack detection with machine learning." IEEE Access (2023).

[17] Revathi, M., V. V. Ramalingam, and B. Amutha. "RMCARTAM For DDoS Attack Mitigation in SDN Using Machine Learning." Computer Systems Science & Engineering 46, no. 1 (2023).

[18] Sambangi, Swathi, Lakshmeeswari Gondi, and Shadi Aljawarneh. "A feature similarity machine learning model for ddos attack detection in modern network environments for industry 4.0." *Computers and Electrical Engineering* 100 (2022): 107955.

[19] Gaur, Vimal, and Rajneesh Kumar. "Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices." *Arabian Journal for Science and Engineering* 47, no. 2 (2022): 1353-1374.

[20] Esmaeili, Mona, Seyedamiryousef Hosseini Goki, Behnam Hajipour Khire Masjidi, Mahdi Sameh, Hamid Gharagozlou, and Amin Salih Mohammed. "Ml-ddosnet: Iot intrusion detection based on denial-of-service attacks using machine learning methods and nsl-kdd." *Wireless Communications and Mobile Computing* 2022 (2022).

[21] Revathi, M., V. V. Ramalingam, and B. Amutha. "A machine learning based detection and mitigation of the DDOS attack by using SDN controller framework." *Wireless Personal Communications* (2021): 1-25.

[22] Chen, Yi-Wen, Jang-Ping Sheu, Yung-Ching Kuo, and Nguyen Van Cuong. "Design and implementation of IoT DDoS attacks detection system based on machine learning." In *2020 European Conference on Networks and Communications (EuCNC)*, pp. 122-127. IEEE, 2020.

[23] Tuan, Tong Anh, Hoang Viet Long, Le Hoang Son, Raghvendra Kumar, Ishaani Priyadarshini, and Nguyen Thi Kim Son. "Performance evaluation of Botnet DDoS attack detection using machine learning." *Evolutionary Intelligence* 13 (2020): 283-294.

[24] Ajeetha, G., and G. Madhu Priya. "Machine learning based DDOS attack detection." In *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)*, vol. 1, pp. 1-5. IEEE, 2019.

[25] Deepa, V., K. Muthamil Sudar, and P. Deepalakshmi. "Design of ensemble learning methods for DDoS detection in SDN environment." In *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, pp. 1-6. IEEE, 2019.

[26] Hall, Mark, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, and Ian H. Witten. "The WEKA data mining software: an update." ACM SIGKDD explorations newsletter 11, no. 1 (2009): 10-18.