JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Detection of DDOS attack in a volume Based network

[1]J. Revathi, [2] DrT.Ramashri

[1]M. Tech Student, Department of ECE, S.V. University College of Engineering, Tirupati, Andhra Pradesh, India.
[2] Professor, Department of ECE, S.V. University College of Engineering, Tirupati, Andhra Pradesh, India.

***Abstract*:** DDoS (distributed denial of service) attacks are now widespread. A DDoS hit can totally shut down or significantly slow down an organization's online services, comprising email and webpages, whether it an inconsequential non-profit or a massive international conglomerate. All tenants, subscribers, and users of data centres, colocation facilities, hosting firms, and other service providers are at risk from Digital dangers, which can target the most clientele. Successful DDoS attacks have the potential to harm brand reputation and result in financial losses in gazillions. DDoS attacks are also accustomed to divert cybersecurity activities from unlawful acts like data theft or network intrusion.
There are numerous methods for identifying the DDoS attack. In order to detect the threat, we used machine learning techniques like logistic regression, K-Nearest Neighbour (KNN), multi-layer perceptron (MLP), and decision tree classifiers trained with pre-defined feature sets. These techniques also took into consideration of additional traffic features like source-IP, destination-IP, packet count, protocol type, etc. The algorithm's test findings improved outcomes in identifying DDoS attacks with faster and more accurately and less computational effort. Python 3.10.1 is used to execute the research, and various datasets were taken to train and test the data in order to detect Attack traffic. The proposed algorithm's evaluation metrics- precision, recall, and F1 score are calculated and contrasted against both of the conventional model and machine learning model. In contrast to prior models, methods of machine learning achieved much better accuracy.

***Index Terms* -: Distributed denial of service attacks, attack detection, machine learning algorithms etc.**

I.INTRODUCTION

Distributed denial of service (DDOS) is a style of malicious hacking used by hackers or cybercriminals to deny access to a host machine, network resource, or online service for its intended users. These days, there are advantages and disadvantages to the widespread use of the internet and web services. Although it gives users access to important information sources and possibilities, it also promotes cybercrime threats. such as misuse, information hacking, virus insertion, and attacks like DoS and DDoS attack
Cybercriminals have had two busy years with a significant increase in DDoS weapon production and there was a lot of DDOS activity and some of the largest service denial attacks ever witnessed during pandemic. The COVID-19 lockdown, which caused a quick move to online services for everything from education and healthcare to consumer shopping and office work, was one of the foremost reasons in 2020 DDoS attacks since it gave hackers more targets than ever. Many of these organisations and employees turned out to be severely under protected against cyberattacks as a result of the speed of this changeover because it was challenging to maintain cybersecurity practises in an emergency situation.

The size of these attacks increased to record levels in 2021. The greatest DDoS assault ever documented, 3.45 Tbps bandwidth and 340 million packets per second, was handled by Microsoft in November 2021 and targeted an Azure client. The first known distributed denial of service assault occurred when Panix, one of the earliest broadband providers, was brought down for many weeks straight by a SYN flood, a technique that is now identified as a standard DDoS attack. In the succeeding years, DDoS attacks increased, and by 2023, Cisco predicts that they will have doubled from the 7.9 million recorded in 2018 to over 15 million. The "Google Strike" of 2020 lasted six months and peaked at a staggering 2.5Tbps. It targeted dozens of Google internet protocol addresses and was launched through three Chinese ISPs. DDoS Attack on Amazon Web Services, the 800-pound giant of cloud - based solutions, was the victim of a significant DDoS attack in February 2020. The most severe DDoS assault to date used a method known as Connectionless Lightweight Directory Access Protocol (CLDAP) reflection and was directed against an undesignated AWS patronage. One such method, which is reliant on shoddy third-party CLDAP servers, augments the amount of information supplied to the victim's IP address by 70 times. Over the span of three days, the attack topped at an unprecedented 2.3 terabytes per second. Exploit executed against Brian Krebs' website by Mirai and OVH in 2016 On September 20, 2016, a DDoS attack with a capacity of ever more than 620 Gigabytes per second was initiated. Krebs site was assaulted before. Although Krebs had recorded 269 Cyber threats until July 2012, the intensity of this attack far exceeded anything the internet or his website had ever experienced. The main contributor of the attempt was the Mirai botnet, which at its peak later that year contained and over 600,000 compromised Iot systems, including Cameras and

sensors, home routers, and media player. The Krebs attack was the Mirai botnet's earliest significant attempt, being discovered in August preceding year. On 19 September, OVH, one of the biggest European companies, was the target of the second Mirai attack. OVH hosts over 18 million apps for more than one million customers. An estimated 145k bot, responsible for a traffic size is almost up to 1.1 terabits per second, were used in this attack on a single, unnamed OVH client. About seven days were involved. However, OVH would not be the final Mirai botnet victim of 2016. A 1.5 terabit per second traffic flood on Dyn, a significant domain name service (DNS) provider, occurred on October 21, 2016, and it later set a new DDoS attack record. Numerous well-known websites, including airbnb, pay pal, twitter, Netflix, reddit and git hub became unreachable after the traffic tsunami knocked Dyn's services offline. " As per Kyle York, chief strategy officer at Dyn, "We found tens of millions of distinct Ips connected to the Stuxnet which been involved in the attack". The 2018 GitHub Attack-2018 February 28, a DDoS attack captured with a capacity of 1.35 terabits per second and remain for 20 minutes on GitHub, a platform for software developers. The traffic might be linked to "over a dozen of distinct autonomous systems (ASNs) over thousands of unique endpoints," according to Github.

There is no standard procedure for attack behaviour since distributed denial-of-service attacks have altered the typical peer to peer-based hack style. The attack also makes use of widely used protocols and services. Only using the different types of protocols and services can make it difficult to distinguish between an attack and normal behaviour. It is difficult to identify the distributed denial-of-service assault. Using the suggested feature selection and classification technique, a machine learning approach is employed in this study to predict a DDoS hit in a network with a maximum accuracy of 99.99%.

The research work for this study is divided into many divisions by its organisational structure. In part 2, the Literature Review is provided. In section 3, the idea of approach is discussed. The findings are reported in section 4, and sections 5 present a conclusion and future work suggestions.

II. RELATED WORK

For detecting DDoS attacks, the majority of the currently available work has used datasets like KDD Cup 99 dataset [1] or DARPA dataset [2]. However, as time goes on, cyberattacks and crimes have been committed in a cunning manner to intrude into the target area. Therefore, improving the effectiveness of the classifier requires training many classifiers using a recent dataset that contains a wide range of novel threat patterns. For our investigation, we are use the CICDDoS dataset [3]. By using the CICDoS dataset to train models, our effort aims to construct numerous supervised classifiers to recognise DDoS attacks. Our goal is to decrease false positives with greater precision, which will assist to increase the outage of the manufacturing systems and the company credibility. Based on the characteristics recorded by the logs, such as the packet size, the difference between the bit rates of sent and received packets, the source and destination IP addresses together with their ports, etc. is network traffic is anomalous or not can be determined. Denial of service attack generally are classified into one of two categories. The first type of attack is a distributed denial-of-service (DoS) attack at network level, which depletes network resources and shuts down connectivity for actual users. An alternative type of attack is a distributed denial of service (DoS) attack at the application level, which depletes server resources and prevents legitimate user requests. In attack, the attacker seizes control of a number of workstations, or "zombies," from which they can launch "bot code" scripts and attack the compromised server. There are two main categories. Attacks on reflection come first, followed by attacks on exploits. In a reflection attack, the attacker's identity is concealed, although this is not the case in an exploit assault. Application layer and transport layer protocols, as well as their combination, can be used to implement both reflective and exploitation attacks. MSSQL and SSDP are examples of TCP-based reflective attacks, whereas network time protocol, and trivial file transfer protocol are examples of udp related reflective attacks. In [4], Kurniabudi examined pertinent and important aspects of the massive network traffic. Idhammad proposed a partial supervised ML method for detecting DDoS in accordance with the calculation of network type, data gain ratio, and decision trees methodology [5]. INDB (Intrusion Detection using Nave Bayes) mechanism was suggested by the researchers in [6] to identify intrusion packets. The predictability of naive bayes algorithms is a justification for their use.
Three distinct classification methods were used to analyse the data and describe the challenges and traits of DoS/DDoS attacks. KNN and Random Forest were used in the development of an architecture by Alpna and Malhotra [7] to identify DDoS attacks. There are numerous works that are linked to detecting DDoS attacks. However, the majority of this research focuses on optimization for better performance and evaluates the dataset using a particular classification algorithm. Due of their simplicity and portability, machine learning algorithms are usually utilised for feature engineering [8].

Classification and clustering methods are widely utilised in intrusion detection systems. Data categorization methods including support vector machine [9], [10], Decision Tree [11], [12], and K Nearest Neighbour [13] have produced significant and effective results for network traffic. One of the most recent methods utilised with machine learning methods for immediate results is incremental learning. Machine learning model with neural networks presented a genetic approach to detect with wide application range but extensive training time is necessary. It is frequently used in target identification [15], image classification [14], and intrusion detection [16]. [17] The statistical model approach is nearly entirely dependent on mathematical modelling, which affects accuracy, and is based on a calculation made for a normal behaviour. [18] pay-load based model with [19] gram analysis, the payload type of approach model picks up on the attributes of a typical packet payload and detects aberrant behaviour, which takes longer to handle due to computational cost.
`

A popular DDOS attack is a "ping flooded attack," also known as an "ICMP flood," in which the offender floods the victim's computer with ICMP echo requests, or "pings," in an effort to shut it down. The attack entails flooding the victim's net with request packets, knowing that it will receive an equal number of reply packets in response. Hping and scapy are two examples of custom software or scripts that can be used to disable a target via ICMP probing. This uses up a substantial amount of bandwidth and results in a denial of service on the network's incoming and outgoing routes.

TCP SYN flood, also known as a "SYN flood assault," is a type of Distributed Denial of Service attack that uses connections on the targeted server and disables it by exploiting of a flaw in the common TCP three-way handshake. Flooding attacks DDoS basically happens when the attacker sends TCP connection requests more speedily than the targeted, thereby triggers to network congestion.

III. PROPOSED METHODOLOGY

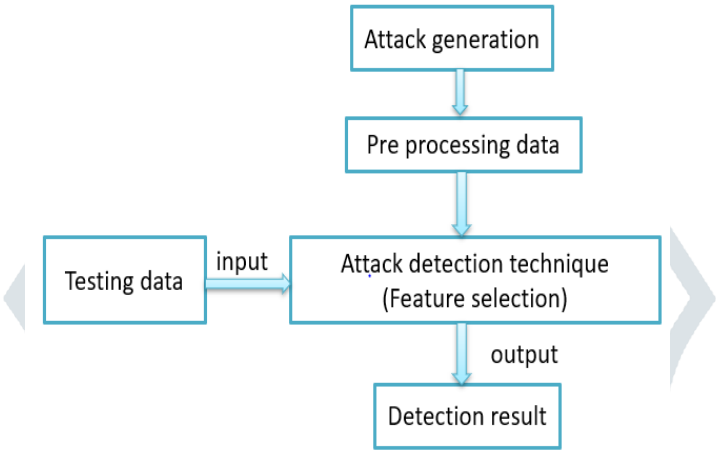


FIG 1. Proposed methodology

Machine learning is subset of artificial intelligence Without user intervention, it helps in automatically learning from data to get better eventually. A more sophisticated AI called machine learning heavily relies on data mining, statistics, pattern recognition, and information finding. learning methods are typically classified into two types: supervised learning and unsupervised learning. Both the inputs and the expected outcomes are included in a data set for supervised learning. By using structured data to predict future occurrences, supervised algorithms for machine learning can apply what they have learned in the past to updated data. The blended learning first analyses an existent training set before creating an inferred function to predict how well the suggested will perform.[20] Following adequate training, the computer may provide expectations for any new data. The learning process methods will also appropriately equate its output with the premediated output and will detect faults to change the pattern. Unsupervised learning, on the other hand, takes a data that just comprises inputs and finds model in the data. On the contrary side, unsupervised machine learning strategies are applied when the data that needs to be trained is neither identifiable nor classified. In order to uncover a hidden structure, unsupervised learning process examines how computers infer a function from unlabelled data. The system analyses the information and can reach inferences from datasets to explain hidden structures from unlabelled variables rather than determining the right behaviour. Machine learning models are shown how to make a range of judgments via reinforcement learning. In a pressurised environment that is unpredictable, the agent learns how to accomplish a task. [21] Artificial intelligence and a premise similar to a game collide in terms of reinforcement learning. The device uses trial and failure to find the answer. The proposed technique in this work is to detect DDOS attacks using supervised learning. For data classification, the various machine algorithms logistic regression, MLP, K-NN, and ID3 were examined and tested. These algorithms were chosen for their efficient speed and Network Security implementation. Legit analysis can be accomplished by classifier because the model may be altered in accordance to recently added features. It is possible to retain significant earlier finds so that learning can be drawn from them for upcoming reliable information. Qureshi et al. [22] who keep earlier samples that are likely to turn into support vectors, use alternative techniques to address the problem of support vectors.

The suggested DDoS attack detection method contains the following steps:

1. data selection
2. data pre processing
3. attribute selection

3.1.1 Data Selection:

The algorithms in the paper were validated and trained using the CCIDS data set. The CICIDS dataset closely replicates factual data and includes regular neutral and current attacks (PCAPs). Additionally, it covers source and destination IP addresses, host counts, diverse ports, protocols type, duration, and attack-based flow type, along with network traffic analysis results from the Wireshark analyser. Over 80 network flow features that were taken from generated network traffic are included in the collection.

3.1.2 Data pre-processing:

It is a way of organizing a chaotic collection of data from raw data. In other words, the study is unfeasible because the data was acquired from numerous sources and was recovered in raw form. The data format needs to be correctly formatted in order to get better results from the model that is used in machine learning projects. Any explicitly specified machine learning model requires data in a particular format. In order to run the Random Forest methods, for instance, null data fields from the original source sample group must be treated because the Random Forest technique does not accept them. It's also important to structure the data collection so that more than one Machine learning and deep learning algorithms are applied to a single set of data, and the most effective machine learning and deep learning algorithms are used.

3.1.3 Attribute selection:

Attribute selection is the vital role in machine learning concepts that strongly effects the model 's efficiency. The performance of machine learning models can attain will be greatly impacted by the data characteristics you use to train them. The most crucial phase of creating a layout is feature collection and data cleaning. The process of feature selection involves either by hand or automatically choosing the attributes that have the greatest impact on the output or predicted attribute you are interested in. When data contains irrelevant characteristics, the accuracy of the model may suffer, and model may have been trained using irrelevant and redundant features. The CCIDS training dataset is used in this research to train the algorithm and categorise DDOS Attacks according to their distinctive characteristics. The data set includes the destination port, several packet attributes including packet length, flow time, header length, etc., an attack label to indicate whether the communication is DDOS traffic, and various TCP flags. DDOS attacks are identified using characteristics like packet size, packet length, flow time, forward packet, backward packet, and other various packet features. A DDOS attack involves flooding a server, service, or network with Internet traffic in an effort to disrupt connection requests on the targeted object. The common features of DDOS traffic include high flow rates, larger packet sizes than usual, longer packet lengths than usual, etc. To allow the algorithms to be trained, the dataset is divided into train data and test dataset. The algorithm is trained using 70% of the data set, then tested using the remaining 30%. To achieve a 99.99% efficiency, many classifications algorithms are applied.

3.2. Classifiers used:

Depending on certain features, a classifier is an algorithm or a technique used to group or categorise accessible data into different groups. A classifier is used in machine learning to categorise data into different categories in accordance with the patterns we have utilised in this research. Logistic regression, MLP, Decision tree -ID 3, and K-nearest neighbour algorithms are some examples of multiple classifiers.

1.Logistic regression

A statistic test procedure called logistic regression uses observed data from a data set to predict a binary result whether true or false. By examining the interaction between one or more current independent variables, a logistic regression excepts a dependent data variable.

2. K- nearest neighbour

The KNN, is a supervised learning classifier that makes predictions or classifications about the grouping of a individual data point based on proximity.

3. Multilayer perceptron

It is a class of artificial neural network that generates a series of outputs from a number of inputs. Multiple layers including input nodes make form the vertical line that connects an MLP's inlet and outlet layers. MLP uses back propagation to train a network.

4. Iterative Dichotomiser 3

The Iterative Dichotomiser 3 algorithm, created by Ross Quinlan, is applied in decision tree learning to create a decision tree from a dataset. In the fields of machine learning and natural language analysis, ID3 is a predecessor to the C4. 5 algorithms.

3.3 Proposed Work:

The research used the CCIDS and DARPA data sets to train and evaluate the model. Logistic regression, MLP, decision tree, and K-nearest neighbour algorithms are utilised for the computation for the best accuracy result based on various classification techniques. Features like packet flows, port numbers, traffic analyses, etc. are the foundation of the model. Training and test data are separated from the whole data set. Thirty percent of the dataset is dedicated to testing, while the other seventy percent is reserved for training. Two steps are taken to develop the detection algorithms:

1.Train stage

2.Test stage

Machine learning algorithms are used to learn the classifiers during the training phase. The machine learning approach that provides the most notable overall classification accuracy will be chosen for use in the proposed detection model during in the testing process. The training portion of the model's detection phase involves observing packet rates, ports, etc. and classifying them to determine whether the traffic is DDOS traffic or not.

4. Results and Discussion

4.1 Evaluation metrics

We have adopted primary performance measures to assess the performance of the classifiers. “The Accurate score and other performance metrics including Precision, Recall, and f1-score” have been applied to analyse and review each classifier. Plot 4 depicts the outcomes for each algorithm and displays the accuracy rating for each categorization technique.

Accuracy:

Rate of instances correctly classified by a classifier

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

Precision:

Total predicted true instances of DDOS attacks divided by the total number of predicted true and false DDOS attacks

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

Recall:

Total predicted number of DDOS attacks divided by the total number of actual DDOS

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

F1 score:

It computes the harmonic mean of the precision and the recall

$$\text{Recall} = 2 * \frac{P*R}{P+R}$$

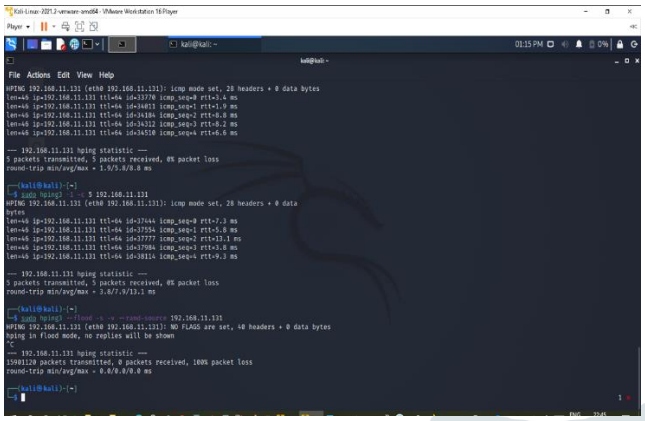


FIG.2 Attack created at attacker machine with single ip address

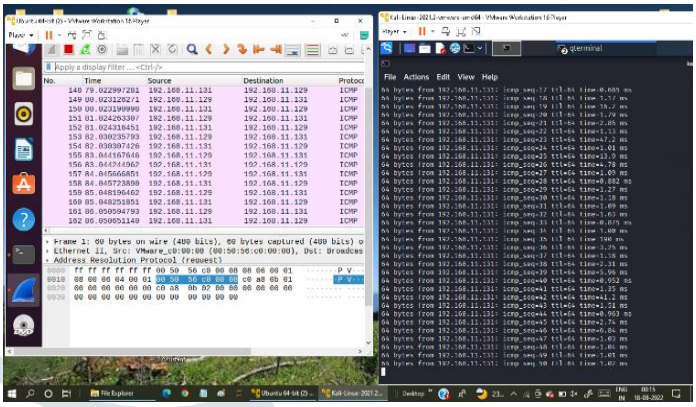


FIG. 3: attack created in a virtual environment

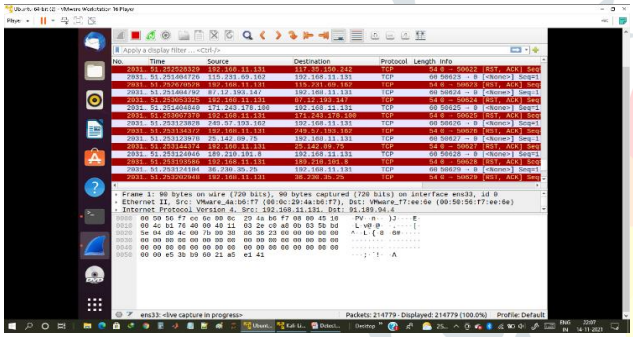


FIG.4: captured a traffic through Wireshark tool

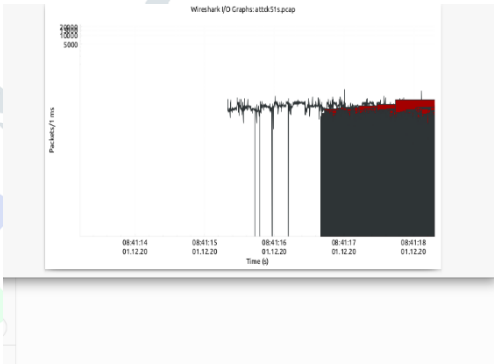
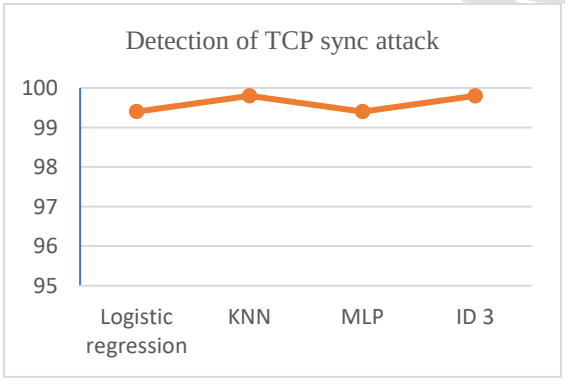
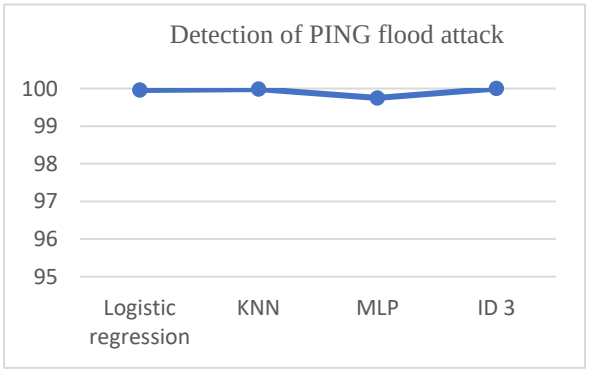


FIG.5: output flow graph



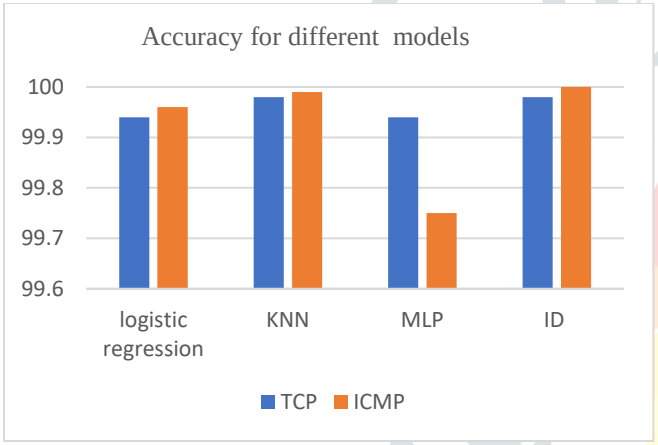
Plot 1: Detection TCP sync attack



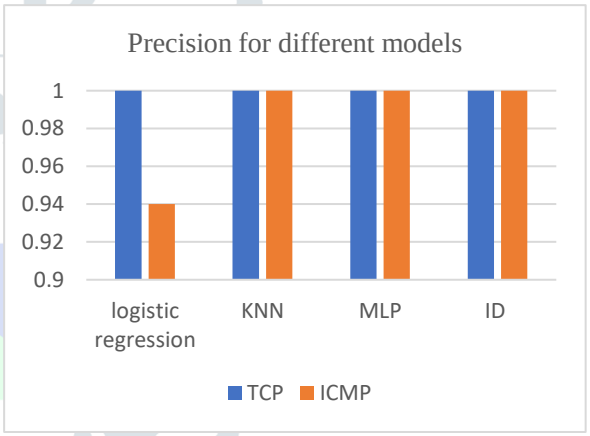
Plot 2: Detection of ICMP attack

	TCP protocol				ICMP protocol			
Model name	accuracy	precision	recall	F1 score	accuracy	precision	recall	F1 score
Logistic regression	99.4	1.00	0.91	0.80	99.96	0.94	0.76	0.92
KNN	99.8	1.00	1	1.00	99.99	1.00	1.00	1.00
MLP	99.4	1.00	0.83	0.90	99.75	1.00	0.98	0.99
ID	99.8	1.00	1.00	1.00	100	1.00	1.00	1.00

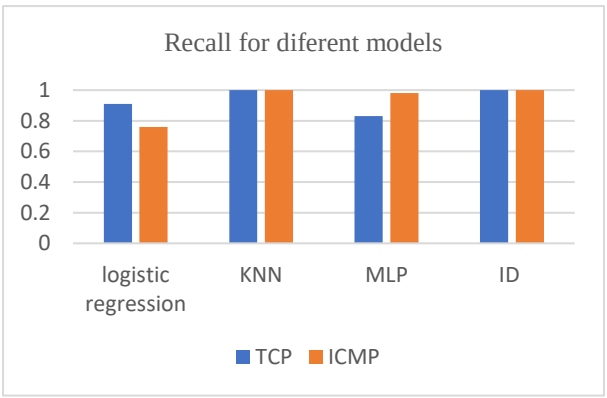
Table 1: performance metrics for each algorithm of TCP sync, ICMP flood attack



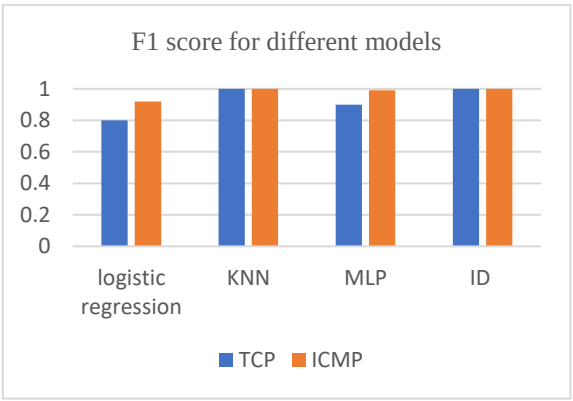
Plot 4: Accuracy of various models



Plot 5: precision for different models



Plot 6: Recall for different models



Plot 7: F1 score for different models

S.NO		Accuracy	Precession	Recall	F1 score
1	Existing method	97.8	0.9	0.89	0.842
2	Proposed method	99.98	0.98	1.00	1.00

Table 2: comparison for existing and proposed methods

Calculating accuracy solely, however, is insufficient to track a classifier's performance evolution. In order to calculate precision, recall, and F1score for various protocol attacks, the data is shown in table 1 After examining the results of all machine learning-based classification algorithms, it was found that their accuracy with datasets was close to 99.9%. These classifiers perform the best, even when additional criteria are taken into account. However, a slight variance in performance can be seen when the specification for each technique gets changed.

Table 1 compare the "predicted precision, recall, and F1 score values" of all classes of classifiers used for attacks on TCP-sync flooding, ICMP flooding Plot 4, 5, 6, and 7 provide comparisons of all classifier performance measures for the various attacks. Table 2 compares the machine learning model to the conventional existing model. In comparison to the current traditional model, the findings showed that the proposed machine learning model performed well in all dimensions.

V. Conclusion

A machine learning algorithm-based method for DDOS attack detection in a volume based network is suggested by the work. To detect DDOS attacks, the project makes use of the trained data set. 20 features, including source and destination IP addresses, host and protocol counts, flow rates, and the size of incoming packets, were selected as characteristics from the 80 variables in the dataset. Then, using the acquired data as inlet features for machine learning models, a number of methods are used to train and obtain the DDoS attack detection. Several techniques, including decision tree models, multilayer perceptron, logistic regression, and KNN, were utilized to evaluate the data set. The study's conclusions showed that trained models are more precise than the established traditional methods.

VI. FUTURE SCOPE

Applying advanced deep learning algorithms to create a predictive analytics model will enable the development of an automated network data analysis system that can respond to changing conditions. It might make decisions about defences, perform evaluations, and offer safety information about what is happening in a network.

REFRENCES

[1] KDDCUP99
http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
[2] DARPA Dataset [Online]. Available: https://www.ll.mit.edu/r-d/dataset
[3] L. Sharafaldin, A. Habibi L.Saqib Hakak, and A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy", IEEE 53rd International Carnahan Conference on Security Technology, Chennai, India, 2019.
[4] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Idris, A. M. Bamhdi and R. Budiarto, "CICIDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection," in IEEE Access, vol. 8, pp. 132911-132921, 2020, doi: 10.1109/ACCESS.2020.3009843.
[5] M. Idhammad, K. Afdel, and M. Belouch. "Semi-supervised machine learning approach for DDoS detection." Applied Intelligence 48, no. 10 (2018): 3193-3208.
[6] V. Hema and C. E. Shin. "DoS Attack Detection Based on Naive Bayes Classifier." Middle-East Journal of Scientific Research 23 (2015): 398- 405
[7] Alpna and S. Malhotra, "DDoS Attack Detection and Prevention Using Ensemble Classifier (RF)", IJARCSSE, 2016.
[8] S. Chesney, K. Roy, and S. Khorsandroo, ''Machine learning algorithms for preventing IoT cybersecurity attacks,'' in Proc. SAI Intell. Syst. Conf., in Advances in Intelligent Systems and Computing, vol. 1252, 2021, pp. 679–686
[9] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin,
A. Gani, E. Ahmed, A. S. M. Nainar, and N. M. Akim, ''Deep learning and big data technologies for IoT security,'' Computer. Communication., vol. 151, pp. 495–517, Feb. 2020.

[10] C. A. Catania, F. Bromberg, and C. G. Garino, ‘‘An autonomous labelling approach to support vector machines algorithms for network traffic anomaly detection,’’ Expert Syst. Appl., vol. 39, no. 2, pp. 1822–1829, Feb. 2012
[11] S. M. Erfani, S. Rajasegarar, S. Karunasekera, and C. Leckie, ‘‘High dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning,’’ Pattern Recognition., vol. 58, pp. 121–134, Oct. 2016.
[12] S. S. Sivatha Sindhu, S. Geetha, and A. Kannan, ‘‘Decision tree based light weight intrusion detection using a wrapper approach,’’ Expert Syst. Appl., vol. 39, no. 1, pp. 129–141, Jan. 2012.
[13] G. Kim, S. Lee, and S. Kim, ‘‘A novel hybrid intrusion detection method integrating anomaly detection with misuse detection,’’ Expert Syst. Appl., vol. 41, no. 4, pp. 1690–1700, Mar. 2014.
[14] C. Tang, W. Li, P. Wang, and L. Wang, ‘‘Online human action recognition based on incremental learning of weighted covariance descriptors,’’ Inf. Sci., vol. 467, pp. 219–237, Oct. 2018.
[15] M. Ristin, M. Guillaumin, J. Gall, and L.Van Gool, ‘‘Incremental learning of random forests for large-scale image classification,’’ IEEE Trans. Pattern Anal. Mach. Intel., vol. 38, no. 3, pp. 490–503, Mar. 2016.
[16] T. H. Hai, L. H. Hoang, and E.-N. Huh, ‘‘Network anomaly detection based on late fusion of several machine learning algorithms,’’ Int. J. Computer. Networks. Communication., vol. 12, no. 6, pp. 117–131, Nov. 2020.
[17] K. Kalkan, L. Altay, G. Gür, and F. Alagöz, ‘‘JESS: Joint entropy-based DDoS Defense scheme in SDN,’’ IEEE J. Sel. Areas Communication., vol. 36, no. 10, pp. 2358–2372, Oct. 2018.
[18] A. Kim, M. Park, and D. H. Lee, ‘‘AI-IDS: Application of deep learning to real-time Web intrusion detection,’’ IEEE Access, vol. 8, pp. 70245–70261, 2020.
[19] V. Kumar, D. Sinha, A. K. Das, S. C. Pandey, and R. T. Goswami, ‘‘An integrated rule-based intrusion detection system: Analysis on UNSW-NB15 data set and the real time online dataset,’’ Cluster Computer vol. 23, no. 2, pp. 1397–1418, Jun. 2020
[20] Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Kumar, N.; Hassan, M.M. A Privacy-Preserving-Based Secure Framework Using Blockchain-Enabled Deep-Learning in Cooperative Intelligent Transport System. IEEE Trans. Intell. Transp. Syst. 2021.
[21] Jan, S.U.; Ahmed, S.; Shakhov, V. Koo, I. Toward a Lightweight Intrusion Detection System for the Internet of Things. IEEE Access 2019, 7, 42450–42471.
Hasan, Z.; Hasan, K.Z.; Sattar, A. Burst Header Packet Flood Detection in Optical Burst Switching Network Using Deep Learning Model. Procedia Computer. Sci. 2018, 143, 970977
[22] A. S. Qureshi, A. Khan, N. Shamim, and M. H. Durad, ‘‘Intrusion detection using deep sparse auto-encoder and self-taught learning,’’ Neural Computer Appl., vol. 32, no. 8, pp. 3135–3147, Apr. 2020.