Pakistan Journal of Engineering Technology and Science (PJETS)
Volume 12. Issue.02, PP. 28-36, December 2024
https://doi.org/10.22555/pjets.v12i2.1068
E-ISSN 2224-2333
P-ISSN 2222-9930

Detection of Distributed Denial of Service (DDoS) Cyber Attacks through Deep Learning Neural Network

Roheen Qamar*[1], Baqar Ali Zardari[2], Zahid Hussain[2], Aijaz Ahmed Arain[1]
[1]*Department of Computer Science Information Technology, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan*
[2]*Department of Information Technology, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan*

*Corresponding Author: *roheen.qamar04@yahoo.com*

Abstract:

Distributed Denial of Service (DDoS) attacks represent a significant and rising threat to internet stability. These attacks, which flood a network with data, can decrease website and application performance, making them unavailable to legitimate users, as unknown attacks can cause substantial damage before being noticed. Computer networks are not immune to additional security threats such as infiltration attempts, traffic bottlenecks, and unauthorized access. These considerations underscore the importance of effective network security measures. DDoS attacks target several machines and internet connections. The suggested system's training consisted of three algorithms using Deep-learning neural networks. This training aimed to teach the system to recognize and categorize input traffic. The technique suggested was trained using three neural network approaches. This study provides a deep learning solution to DDoS attack detection that employs three unique algorithms inside a neural network architecture. Training data from the KDD dataset was preprocessed before being input into the model, which was developed and trained with the MATLAB R2023a "ANN" toolset. This system uses a deep learning neural network to properly assess and identify future DDoS assault threats. As internet dependency increases, so does the need for better security solutions. This research helps to establish effective procedures for protecting valuable online assets from increasingly complex cyber-attacks

Keywords: *DDoS, Deep Learning Neural Network (DLN), Naive Bayes Training Algorithm, K-Nearest Neighbor (KNN) Training Algorithm, Semi-Supervised K-Means Clustering Algorithm.*

I. INTRODUCTION

DDoS (distributed denial of service) attacks are a type of attack that is used to take down a system and pose a serious risk to networks. By saturating them with traffic from several sources, DDoS attacks attempt to interfere with internet services. Although it is not a brand-new problem, it, nevertheless, represents one of the biggest security obstacles for service providers and their clients. Modern networks urgently require quick DDoS attack detection and management. Genetic algorithms and more complicated algorithms like neural networks may be used to find and classify DDoS attack features [1].

Deep learning is a type of learning that relies on methods that are prompted by how the brain works, functions and is organized. Deep learning trains the computer system to create results by using previously accessible instances. Deep learning's capabilities have enabled it to achieve things that were previously unthinkable. They remain the essential mechanism underpinning most of the applications available today, including as self-driving vehicles, and voice control in consumer goods such as phones, televisions, smart equipment, and so on [2].

One of the most dangerous forms of cyberattacks is a denial-of-service (DoS) assault, in which the attackers try to overload the target's system with traffic until the target is unusable by the intended users. These attacks are usually

carried out by overloading the targeted computer with unnecessary traffic until the target stops responding. A DoS assault's cousin, the distributed denial of service (DDoS) attack, is more harmful than a DoS attack. The fact that several infected devices are being used to overwhelm the victim with bogus communications makes defense more challenging. By preventing licit users from accessing the target server until it is exhausted, these assaults result in significant financial losses for the affected sectors.

The first half of 2022 saw a 75.60% increase in the total number of attacks compared to the second half of 2021. Amazon reported a DDoS attack volume of 2.3 Tbps in the first quarter of 2020, with most botnets in China, the US and India -DDoS attacks launched from countries could cause losses to corporate organizations $50,000 in lost revenue from downtime and mitigation costs. In the third quarter of 2022, 71% of the resulting DDoS attacks are SYN floods and DNS attacks. Internet service providers and companies use various solutions and Scrubbing Centers to protect against DDoS attacks. However, real DDoS attacks are fast and sophisticated, and botnets are widely used. Machine learning-based scrubbing centres are considered as next-generation scrubbing centers (NGSC) [3].

Attackers create a network using controller machines to identify the attack type and the victim's address. They launch the attack remotely or program ahead of time, sending a stream of attack packets to the victim. Defendants' systems are overloaded with meaningless data, deplete resources and deny legitimate services. DDoS attacks are usually automated using hacking tools. The attacker sends many packets, the master agent discovers vulnerable devices, and the victim is a victimized host [4].

II. RELATED WORK

Yousuf et al. [5] the study introduced a novel activation function for detecting DDoS using a Recurrent Neural Network (RNN) approach. The Internet of Things (IoT) is a fast-growing communications infrastructure, as is the rise of distributed user attacks (DDoS) has led to a growing demand for solutions. This paper presents a novel algorithm called DALCNN, which uses a recurrent neural network and a software-defined network (SDN) using the Open Daylight platform. The algorithm classifies attacks using a novel activation function and machine/deep learning concepts. The algorithm was tested on 177 instances and its performance was evaluated using tools like Mininet and Wire Shark. The results showed that the proposed algorithm outperforms other existing algorithms, with the Open Daylight controller outperforming other open-source controllers in terms of throughput, latency, and aggregate controller performance.

Hnamte et al. [6] present a deep neural network (DNN)-based approach to detect distributed denial of service (DDoS) attacks in software-defined network (SDN) environments. The model uses deep learning principles to analyze network traffic data to identify complex patterns. The results show superiority over traditional DDoS detection methods, with detection accuracy rates of 99.98%, 100%, and 99.99% In SDN, CICIDS2018, and Kaggle DDoS datasets, respectively the DNN-based model exhibits potential strongly demonstrated in today's DDoS threat mitigation. The study provides insights into the identifying benefits and challenges associated with implementing DNN in real-world SDN environments, and contributes to the ongoing discourse on strengthening digital networks against evolving cyber threats to network security employees have benefited.

Shah et al. [7] DDoS attacks pose a serious threat to network security, consuming resources such as computing power and bandwidth. Machine learning is a proven technology for detecting these attacks, but there is no need to investigate the inefficiencies of performance, accuracy, data collection, dataset regularization, feature reduction, and computational cost in detail Use is not reduced on or did not proliferate in widespread attacks.

Kumar D et al. [8] The growing rise of distributed denial of service (DDoS) threats makes Internet infrastructure more vulnerable to cyber-attacks it is important to quickly identify and isolate network data and protect against DDoS threats. This study builds a model based on long-term and short-term memory (LSTM) to detect DDoS threats in network traffic packets. LSTM is a deep learning algorithm with a self-updating feature selection and extraction algorithm. Using the CIDDDoS2019 dataset, the model achieves an accuracy of up to 98%, outperforming machine learning on the dataset.

S Ahmed et al. [9] Distributed denial of service (DDoS) attacks pose significant risks to businesses and government agencies, limiting access to information and services. Attackers use application-level DDoS attacks that are difficult to detect because they impersonate real users. This study aims to address these attacks by analyzing the incoming

packet characteristics, such as HTTP frame packet size, IP address number, port mapping, and proxy IP address the study uses standard datasets, real networks, and experimentally generated datasets from DDoS attacks use akade. A multilevel perceptron (MLP) deep learning algorithm is used to evaluate the efficiency of metric-based attack detection. Simulation results show that the proposed MLP classification algorithm has 98.99% efficiency in detecting DDoS attacks, with 2.11% lower false positive values compared to traditional classifiers.

Mehmood et al. [10] DDoS attacks pose a serious threat to Internet security by disrupting services and preventing legitimate users from using them. These attacks are carried out by several bots controlled by a botmaster using fake IP addresses, making them less dangerous due to the lack of specialized applications or tools This paper discusses machine learning and deep learning techniques for the detection and analysis of DDoS attacks can be found out. The purpose of the analysis is to provide a comprehensive understanding of the potential risks of DDoS attacks.

Ali Mustapha et al. [11] In a distributed denial-of-service (DDoS) attack, the compromised device overwhelms the target with many requests, making it unable to process a valid request Detection of this type of attack is challenging in cyber security, and using machine learning and deep learning algorithms to improve detection accuracy. However, ML/DL techniques can be circumvented by attack traffic generation, in particular Generative Adversarial Networks (GAN). A new DDoS detection method based on a short-term memory model of recurrent neural networks (RNNs) capable of detecting long-term dependency is proposed the detection algorithm achieves high accuracy in detecting DDoS attacks. However, the LSTM-based detection scheme is not effective against the types of adversarial DDoS attacks carried out with GAN. The detection model performs well and accurately on GAN-generated adversary DDoS traffic, with a detection ratio ranging from 91.75% to 100%.

Ahmed et al. [12] The increasing number of connected devices due to the Internet of Things (IoT) has increased the vulnerability to cyber-attacks, especially distributed denial of service (DDoS) Traditional machine learning methods are often inefficient at DDoS attack detection. This paper introduces a deep learning-based intrusion detection system designed for Cloud or Fog layer deployment in an IoT environment. The model aims to detect all types of DDoS attacks with specific subsets. The hybrid model combines different deep learning models, including convolutional neural networks (CNNs), long-term and short-term memory (LSTM), deep autoencoder, and deep neural networks (DNNs). The performance of the model was evaluated using the CIC-DDoS2019 dataset satisfying the intrusion detection constraint with frozen first-layer output in combination with initial data. The results showed that the proposed model outperformed other machine learning and deep learning models in terms of true positive rate, accuracy, false alarm rate, average accuracy, and percent realization rate.

III. DISTRIBUTED DENIAL OF SERVICE ATTACK

DDoS attacks, are significant and dangerous cyber-attacks that overwhelm websites or servers with bogus traffic, rendering them inoperable. Botnets are utilized in this form of assault, with attackers, masters, zombies, and victims

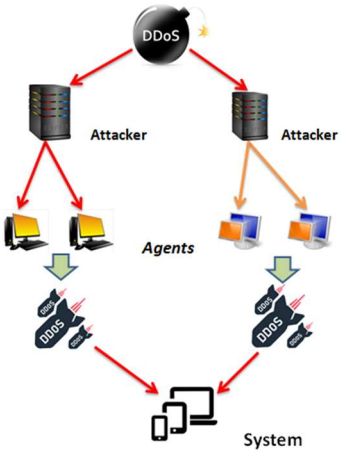

Figure 1: Decentralized Denial of Service (DDoS)

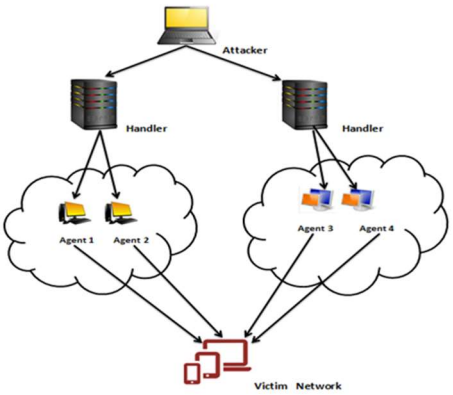

Figure 2: DDOS Zombie Attack

separated into four groups. Resource depletion targets the victim's network resources and prevents legitimate users from using them. Figure 1 illustrates how bandwidth depletion affects the victim's network resources. [13].
Fuzzy end nodes online are used to generate a DDoS attack on the network. Through the Internet, Multiple machines for computing may be transformed into "Botnets" and deployed to harm other websites or systems. In light of this, he has to examine the principles. Features for attack detection and categorization. In distributed P2P networks, a distributed solution is required. Research on the DDoS issue is ongoing and needs to be solved. DDoS attacks surfaced when a user or server was unable to access a valid service offered by a system. The most common technique for creating DDoS attacks on distributed P2P networks is to intentionally deplete resources like memory, CPU, and bandwidth. [14] as shown in Figure 2. The attacks are classified into four types as shown in Figure 3.

IV. DEEP NEURAL NETWORKS FOR LEARNING

One kind of machine learning is called deep learning. That teaches computers to carry out human-like behaviors: learn from your mistakes. Deep learning uses neural networks to directly learn usable representations of characteristics from input. Neural networks are inspired by biological nervous systems and incorporate several nonlinear processing layers employing basic pieces running in parallel. Deep learning models may attain cutting-edge accuracy in object categorization; sometimes outperforming humans [15, 16]. Information enters a Deep Neural Network (DNN) from the input layer and travels through a number of hidden layers before reaching the output layer. Artificial deep neural networks (DNNs), which were first modelled after the human brain, allow computers to do cognitive tasks that humans are excellent at. When these cognitive phenomena were unaccounted for, cognitive scientists began studying biological cognition and its neurological foundation using DNNs as models, which sparked a contentious discussion among experts. Here, we consider the case from a scientific philosophy standpoint. We first contextualize DNNs as scientific models and then go over how DNNs can benefit cognitive research. We show that in addition to being able to predict and explain psychological events, through training DNA acquires the ability to perform certain functions and learn the strength of interactions between groups. The trained DNN is then used to perform the same operation on the new inputs [17, 18]. A deep neural network's design can be seen in Figure 4.

V. PROPOSED METHODOLOGY DESIGN

The suggested approach makes use of a deep-learning neural network. The system's performance is assessed using the KDD-CUP99 dataset. Figure 5 depicts the system's step-by-step flow. The process involves collecting a KDD-CUP99 dataset, cleaning the data, creating a deep-learning neural network model, and training it with three techniques [19].

A. The Knowledge Discovery in Databases (KDD) Dataset

The KDD dataset is first gathered from a reliable source, followed by further processing procedures. A KDD1999 dataset was created using several machine-learning methods and pattern recognition techniques. It was launched for the KDD Cup tournament in 1999. The KDD Cup 1999 standards database monitors network attacks and interference. The KDD dataset was used for testing and training.

B. Pre-Processing

Before training, the KDD dataset involves assigning protocol, attack, and flag values.

C. Deep Learning Neural Network Model:

Use acquired data to develop the recommended model.

D. Training of Neural Network

Simulating a DDoS attack requires training an efficient deep-learning neural network. In this phase, some deep neurons were trained to evaluate the default of the proposed algorithms and briefly check their accuracy.

E. Result:

The optimal training technique for detecting DDoS assaults was determined using the KDD Cup99 dataset.

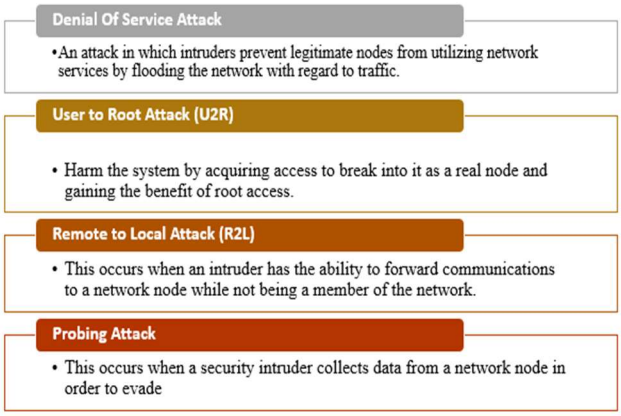

Figure 3: Distinct Groups for Attacks

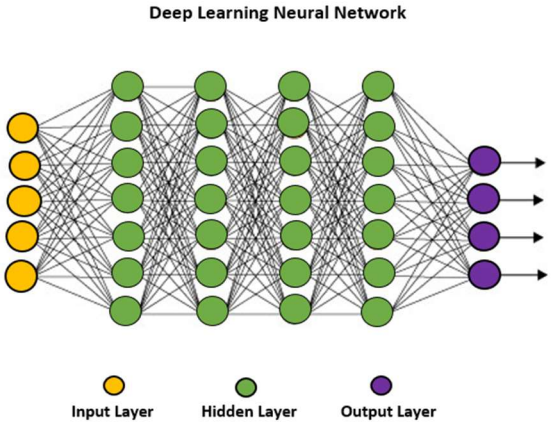

Figure 4: Deep Learning Neural Network

VI. VI. RESULT AND DISCUSSION

KDDCup99 is used to evaluate anomaly detection. It is the product of nine weeks of simulation on a local area network. The training in the dataset, with each tuple including 41 characteristics labelled with the name of the attacks. These are some attacks used with the KDDCUP99 dataset: TCP, UDP, ICMP, HTTP, SMTP etc. The KDD-CUP99 data set is used in this research work. That normal query and DDoS attack. KDDCUP99 can be accessed from MIT Lincoln Laboratory in Lexington, Massachusetts. That is US Department of Defense Research Center Of a record consists of multiple records, protocol type, service, flags,src_bytes, dst_bytes, etc. the final field demonstrates the attack. There are a few attack sorts such as Neptune, smurf, teardrop, etc. [20, 21]. The KDD-CUP99 information set contains both typical and ceaseless information. To create MATLAB R2023a congruous, typical Information areas are supplanted with persistent information. The typical information incorporates convention sorts; benefit sorts, banners and attack sorts [24]. Supported values for convention and benefit sorting are tcp=1, udp=2, icmp=3, http=4, and SMTP=5 etc. There are almost 65 different convention kinds in the information set. Up to ten mistake flags are present, and they are replaced with values such as S0=1, SF=2, S1=3, REJ=4, S2=5, RSTO=6, S3=7, RSTR=8, SH=9, NTH=10.

Attack used in Training.

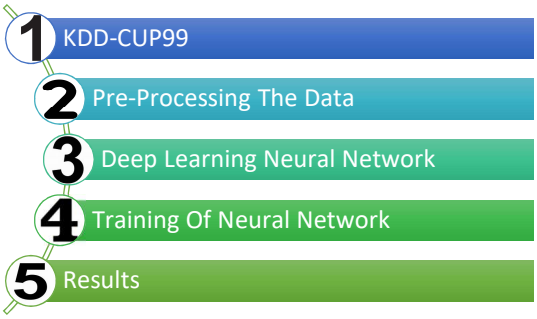

Figure 5: Experiment Steps Structure

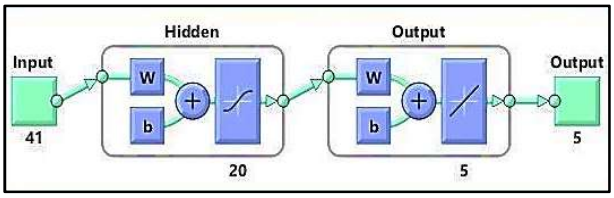

Figure 6: Deep Neural Network

DNS=0, Spoofed-Packet Flood=1, Ping of death=2, Syn=3, UDP=5, Pod=6, Port Sweep Attack=7, HTTP =8, Client Warez Attack =9, Teardrop Attack s=10.

Here, we have several cognitive system plans. Deep Neural networks with 20 neurons in the covered-up layer [22].

A. Deep Learning Neural Network

A deep neural network, one covered-up layer, 20 neurons, sigmoid exchange work, and an output layer. Attacks are classified into classes for ease of use [23]. As shown in Figure 6 Additional layers with 20 neurons in a deep neural network to improve prediction accuracy.

Three algorithms were employed in this study:

- *The Naive Bayes Training Algorithm.*
- *The K-Nearest Neighbor (KNN) Training Algorithm.*
- *Semi-Supervised K-Means Clustering Algorithm.*

A. Naive Bayes Training Algorithm

The Naive Bayes algorithm is a method used in machine learning for categorization that uses the posterior probability of Gaussian, Multinomial, and Bernoulli distributions to be computed. It is appropriate for sentiment analysis, text categorization, and real-time prediction. [24].

Figure 7 demonstrates the neural network's whole training. The performance is 1.6512e-06, the epoch value is 27 iterations, and the total duration is 27 min 20 sec.

Figures 8 depict the neural network's classification value of 94.3% and miss classification of 5.7%.

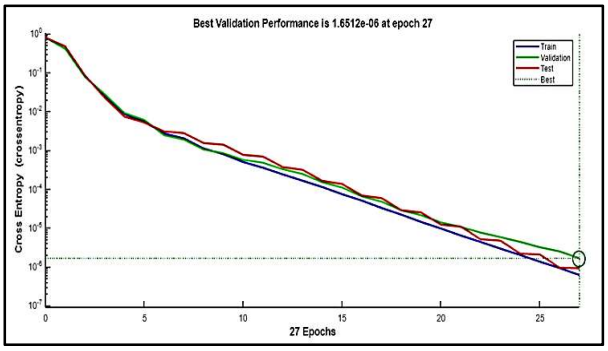

Figure 7: Performance of the Naive Bayes Algorithm in Testing

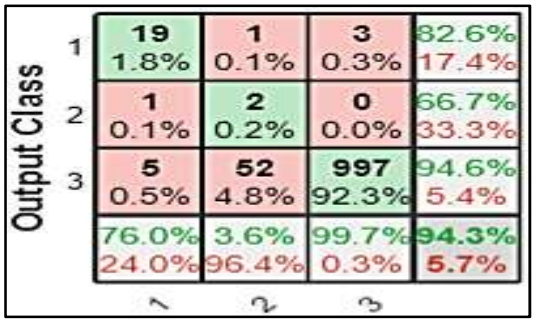

Figure 8: Confusion Matrix Naive Bayes Algorithm Training Algorithm

B. K-Nearest Neighbor (KNN) Training Algorithm

A new instance is added to the category that matches the current categories the most using the machine learning technique K-Nearest Neighbor, which is based on supervised learning. It may be used for regression and is used to group new data based on similarities. Being non-parametric, it makes no assumptions on the underlying data [25]. Once the neural network has finished training, Figure 9 displays the epoch 63 iterations, time 0:02:29, and validates the accuracy of 0.059504.

The neural network's classification value is 91.3% in the example shown as in Figure 10, while the miss prediction rateis 8.7%.

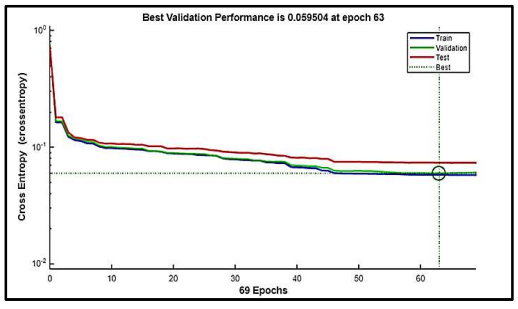

Figure 9: Validation Performance of K-Nearest Neighbor

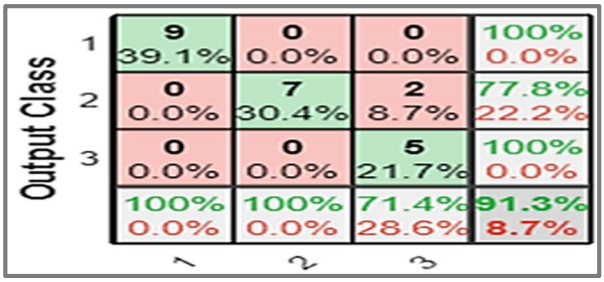

Figure 10: Confusion Matrix B.K-Nearest Neighbor (KNN) Training Algorithm

C. *Semi-Supervised K-Means Clustering Algorithm*

Using the supervised learning machine learning algorithm K-Nearest Neighbor, a new instance is added to the category that most closely fits the present categories. It is useful for regression and for grouping fresh data based on similarities. It makes no assumptions about the underlying data because it is non-parametric. [26]. Figure 11 shows the training, testing, and validation performance curve of the network, with the greatest validation performance of 0.027451 at 10 epochs.

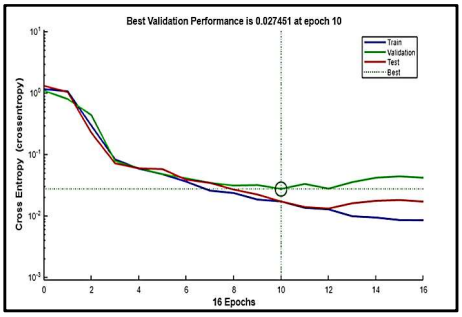

Figure 11: Validation Performance of Semi-Supervised K-Means Algorithm

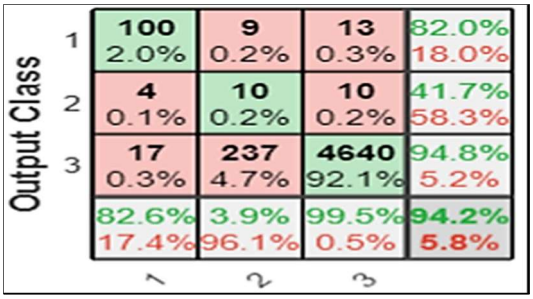

Figure 12: Confusion Matrix SEMI-SUPERVISED

The following Figure 12 displays the neural network's classification value, which is 94.2%, along with the 5.8% error detection rate.

Table 1 demonstrates the training of three distinct techniques using DNN. The result shows that, in terms of performance, the Naive Bayes Training Algorithm Outperforms two other chosen algorithms. In a shorter amount of time—17 minutes and 12 seconds—the training was finished with a 94.3% success rate (accuracy) and a 5.7% misclassification rate.

TABLE 1: Complete Technique Result

S.No.	***Algorithms***	***Success Rate***	***Misclassification***	***Epoch Value***
1.	Naive Bayes Training Algorithm	94.3%	5.7%	27
2.	K-Nearest Neighbor (KNN) Training Algorithm	91.3%	8.7%	63
3.	Semi-Supervised K-Means Clustering Algorithm	94.2%	5.8%	10

VII. CONCLUSION

Nowadays, internet consumers' primary concern is security. DDoS attacks pose a significant threat to internet users' security. DDoS attacks disrupt user access to services. This study utilized a recurrent neural network for training and detecting DDoS assaults. Three well-known methods were chosen: 1) Naive Bayes Training Algorithm 2) K-Nearest Neighbor (KNN) Training Algorithm, and 3) Semi-Supervised K-Means Clustering Algorithm. This research aimed to identify the best algorithm according to accuracy and training time. A deep learning neural network was trained to accurately evaluate and detect DDoS attacks. The results show that “The Naive Bayes Training Algorithm” algorithm gives good results in short training time with very good accuracy performance 94.3 % accuracy and a training time is 2 minutes and 29 seconds in comparison to the “K-Nearest Neighbor (KNN) Training Algorithm and “Semi-Supervised K-Means Clustering Algorithm. To evaluate the precision and detection of DDoS assaults, we trained a Deep Neural Network and compared the three techniques. The purpose of this work was to identify the optimal method the accuracy and training duration of the training are crucial factors to consider. DDoS attacks were recognized with a deep neural network. The study found that the "Naive Bayes Training Algorithm" approach worked effectively In

future, various techniques, models and neural networks may be used for machine learning. Different algorithms may be evaluated to determine which neural network or approach is best for detecting attacks with DDoS.

REFERENCES

[1] Lansky, Jan, Saqib Ali, Mokhtar Mohammadi, Mohammed Kamal Majeed, Sarkhel H. Taher Karim, Shima Rashidi, Mehdi Hosseinzadeh, and Amir Masoud Rahmani. "Deep learning-based intrusion detection systems: a systematic review." IEEE Access 9 (2021): 101574-101599.

[2] Sumathi, S., and N. Karthikeyan. "Detection of distributed denial of service using deep learning neural network." Journal of Ambient Intelligence and Humanized Computing 12, no. 6 (2021): 5943-5953.

[3] Rao, Gottapu Sankara, and P. Krishna Subbarao. "A Novel Framework for Detection of DoS/DDoS Attack Using Deep Learning Techniques, and An Approach to Mitigate the Impact of DoS/DDoS attack in Network Environment." *International Journal of Intelligent Systems and Applications in Engineering* 12, no. 1 (2024): 450-466.

[4] Sahosh, Z. H., Faheem, A., Tuba, M. B., Ahmed, M. I., & Tasnim, S. A. (2024). A Comparative Review on DDoS Attack Detection Using Machine Learning Techniques. *Malaysian Journal of Science and Advanced Technology*, 75-83.

[5] Reddy, P., Adetuwo, Y., & Jakkani, A. K. (2024). Implementation of Machine Learning Techniques for Cloud Security in Detection of DDOS Attacks. *International Journal of Computer Engineering and Technology(IJCET)*, *15*(2).

[6] Hnamte, V., Najar, A. A., Nhung-Nguyen, H., Hussain, J., & Sugali, M. N. (2024). DDoS attack detection and mitigation using deep neural network in SDN environment. *Computers & Security*, *138*, 103661.https://doi.org/10.1016/j.cose.2023.103661

[7] Shah, A., Rathod, D., Dave, D. (2021). DDoS Attack Detection Using Artificial Neural Network. In: Chaubey, N., Parikh, S., Amin, K. (eds) Computing Science, Communication and Security. COMS2 2021. Communications in Computer and Information Science, vol 1416. Springer, Cham. https://doi.org/10.1007/978-3-030-76776-1_4

[8] Kumar, D., Pateriya, R. K., Gupta, R. K., Dehalwar, V., & Sharma, A. (2023). DDoS detection using deep learning. *Procedia Computer Science*, *218*, 2420-2429.https://doi.org/10.1016/j.procs.2023.01.217

[9] Ahmed, S., Khan, Z. A., Mohsin, S. M., Latif, S., Aslam, S., Mujlid, H., ... & Najam, Z. (2023). Effective and efficient DDoS attack detection using deep learning algorithm, multi-layer perceptron. *Future Internet*, *15*(2), 76.https://doi.org/10.3390/fi15020076

[10] Al-Shareeda, M. A., Manickam, S., & Ali, M. (2023). DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison. *Bulletin of Electrical Engineering and Informatics*, *12*(2), 930-939.

[11] Mustapha, A., Khatoun, R., Zeadally, S., Chbib, F., Fadlallah, A., Fahs, W., & El Attar, A. (2023). Detecting DDoS attacks using adversarial neural network. *Computers & Security*, *127*, 103117.https://doi.org/10.1016/j.cose.2023.103117.

[12] Ahmim, A., Maazouzi, F., Ahmim, M., Namane, S., & Dhaou, I. B. (2023). Distributed denial of service attack detection for the Internet of Things using hybrid deep learning model. *IEEE Access*, *11*, 119862-119875.DOI: 10.1109/ACCESS.2023.3327620

[13] Leon, Miguel, Tijana Markovic, and Sasikumar Punnekkat. "Comparative Evaluation of Machine Learning Algorithms for Network Intrusion Detection and Attack Classification." In 2022 international joint conference on neural networks (IJCNN), pp. 01-08. IEEE, 2022.

[14] Kshirsagar, Deepak, and Sandeep Kumar. "A feature reduction based reflected and exploited DDoS attacks detection system." Journal of Ambient Intelligence and Humanized Computing 13, no. 1 (2022): 393-405.

[15] Pakmehr, A., Aßmuth, A., Taheri, N., & Ghaffari, A. (2024). DDoS attack detection techniques in IoT networks: a survey. *Cluster Computing*, 1-32.

[16] Sark Jatmika, M. O., Pratomo, A., Gunawan, W., Aljaber, F., & Budiarto, R. (2024, April). Investigating DDOS attacks on metro network. In *AIP Conference Proceedings* (Vol. 2987, No. 1). AIP Publishing.

[17] Sun, Maoran, Fan Zhang, Fabio Duarte, and Carlo Ratti. "Understanding architecture age and style through deep learning." *Cities* 128 (2022): 103787.

[18] Rao, Gottapu Sankara, and P. Krishna Subbarao. "A Novel Framework for Detection of DoS/DDoS Attack Using Deep Learning Techniques, and An Approach to Mitigate the Impact of DoS/DDoS attack in Network Environment." *International Journal of Intelligent Systems and Applications in Engineering* 12, no. 1 (2024): 450-466).

[19] Srivastava, A., Tiwari, S., Rawat, B. S., & Dhondiyal, S. A. (2024, June). DDoS Attacks Detection in IoT

Networks using Naive Bayes and Random Forest. In *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)* (pp. 1609-1612). IEEE.

[20] Salem A, A. A. (2024, February). DDos Attack Detection Method Based on Information Entropy and Naive Bayes. In *2024 International Conference on Electrical Drives, Power Electronics & Engineering (EDPEE)* (pp. 335-340). IEEE.

[21] Qamar, Roheen, Baqir Ali Zardari, Aijaz Ahmed Arain, Zahid Hussain, and Asadullah Burdi. "A Comparative Study of Distributed Denial of Service Attacks On The Internet Of Things By Using Shallow Neural Network." *Quaid-E-Awam University Research Journal of Engineering, Science & Technology, Nawabshah*. 20, no. 01 (2022): 61-73.

[22] Hemanth, D. J. "Intrusion Detection System Using Convolutional Neural Network on UNSW NB15 Dataset." Advances in Parallel Computing Technologies and Applications 40 (2021): 1.

[23] Nafea, A. A., Hamdi, M. M., saad Abdulhakeem, B., Shakir, A. T., Alsumaidaie, M. S. I., & Shaban, A. M. (2024, April). Detection Systems for Distributed Denial-of-Service (DDoS) Attack Based on Time Series: A Review. In *2024 21st International Multi-Conference on Systems, Signals & Devices (SSD)* (pp. 43-48). IEEE.

[24] Gautam, R., & Padmavathy, R. (2024). Distributed denial of service attack detection using machine learning classifiers. *International Journal of Ad Hoc and Ubiquitous Computing*, *46*(3), 123-149.

[25] Deb, D., Rodrigo, H., & Kumar, S. (2024, May). Performance Analysis of Machine Learning Algorithms on Imbalanced DDoS Attack Dataset. In *2024 IEEE World AI IoT Congress (AIIoT)* (pp. 0349-0355). IEEE.

[26] Naveenkumar, E., B. Dhiyanesh, R. Rajesh Kanna, P. S. Diwakar, M. Murali, and R. Radha. "Detection of Lung Ultrasound Covid-19 Disease Patients based Convolution Multifacet Analytics using Deep Learning." In *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, pp. 185-190. IEEE, 2022.