University of Sindh Journal of Information and Communication Technology (USJICT)
Volume 5, Issue 2, July 2021

ISSN-E: 2523-1235, ISSN-P: 2521-5582
Website: http://sujo.usindh.edu.pk/index.php/USJICT/

Detecting Distributed Denial of Service attacks using Recurrent Neural Network

Roheen Qamar[1], Baqir Ali Zardari[2], Aijaz Ahmed Arain[1], Fida Hussain Khoso[3], Fareed Ahmed Jokhio[4]

[1]Department of Computer Science, 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

[3]Department of Basic Science, Dawood University of Engineering & Technology Karachi, Pakistan

[4]Department of Computer System Engineering, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan

roheen.qamar04@yahoo.com[1], alizardari34@gmail.com[2], aijaz@quest.edu.pk[1], fidahussain.khoso@duet.edu.pk[3], fajokhio@quest.edu.pk[4]

Abstract: As the internet grows and diversity, attackers use various attacks to crash the servers and to stop specific sites. Multiple computers and multiple Internet connections are targeted by using distributed denial of service (DDoS) attacks. The aim of this paper is to identify the best algorithm among the selected algorithms (i.e., gradient descent with momentum algorithm, scaled conjugate gradient, and variable learning rate gradient descent algorithm. In this study, the recurrent neural network was trained to check the accuracy and detection of DDoS attacks. The intention of this training was to allow the system to learn and classify the input traffic into the category. The proposed system's training was composed of three separate algorithms utilizing recurrent neural networks. The MATLAB 2018a simulator was used for training purpose. Moreover, clean the Knowledge Discovery Dataset (KDD) during design and include the values of protocols, attacks, and flags. The neural network model was subsequently developed, and the KDD was trained using Artificial Neural Network (ANN). The results of DDoS attacks' detection were analyzed using MATLAB "ANN" toolbox. The success rate of the variable learning rate gradient descent algorithm was 99.9% accuracy and the short timing was 2 minutes and 29 seconds. The variable learning rate gradient descent algorithm gives better results than gradient descent with momentum and scaled conjugate gradient algorithms. In the state of the art, different algorithms have been trained in different neural networks and different KDD datasets by using selective DDoS attacks but in this research recurrent neural network was used for three different algorithms. In this research we have used a total 22 attacks for detection of DDoS attacks' accuracy.

Keywords: Distributed Denial of Service (DDoS) Attacks, Recurrent Neural Network (RNN), Knowledge Discovery Dataset (KDD), Artificial Neural Network (ANN).

I. INTRODUCTION

The flood attack is one of the major security issue of the Distributed Denial of Service (DDoS). To disturb the legitimate users, the DDoS flood attack involve in multiple tries. The number of security issues have been created due to the fast growth of Internet and computer networks. In recent years, the numerous attacks have been discovered on the networks. Consequently, cybersecurity [1] and security of network resources is very important by investigating potential attacks.

A bot is an effected computer controlled by the attacker remotely. The attacker setups these computers for forward transmissions (including spam and viruses) to other computers on the Internet. The botnet is a computer program also referred as zombie. It's a new type of malware; installed on affected computers that botmaster can remotely control in order to execute certain commands. The computer turns into a bot or zombie after the bot code is installed into compromised computers [2].

The major purpose of DDoS attacks is to hurt the victim either for specific reasons, to gain material or to fame. A high-capacitated computer that delivers all available operating system resources, can no longer handle authentic user requests, which are attacked at the application level. Synchronize attack (SYN) works with incomplete SYN messages when the victim floods. When the attacker attacks a random host port with IP packets including a user datagram called UDP attack.

On using ping command which sends malformed or over-sized packets the targeted computers or services are destabilized, crashed and frozen by the attack of another ping of death. Large packets of statistics are used by Teardrop Attack. It is fragmented by the transmission control protocol (TCP)/ internal protocol (IP) that could be built on the host. As the bundles of the attacks are delivered, the attackers manipulate these attacks by overlapping. The consumed incoming and outgoing bandwidth are attacked by the internet control message protocol (ICMP). Without waiting for replies this type of attack sends packets as quickly as possible.

In a smurf attack, the application is distributed to an intermediate IP network. This attack sends the server with the fake IP request. The attacker hacks clearly legitimate hypertext transfer protocol (HTTP), GET or POSTS applications for HTTP attack to attack a web server or application. The IP sweep attack is used when an attacker generates ICMP attack echo requests (pings) for various target addresses, then an IP sweep attack happens [3].

A. DDoS Architecture

The following are the elements of DDoS attack architecture as shown in Figure 1:

- Attacker: An unauthorized user, who selects the machine for crashing.
- Masters: These are designed by a unique program and control many slaves.
- Slaves: They are in-charge for generating packet streams which send to the server.
- Server: It is a system that an attacker destroys.

The reasons for DDoS attacks:

- Powerless programs / applications running on the machine or system.
- Software installation without security consideration.
- There are no checks or data analyses carried out [4].

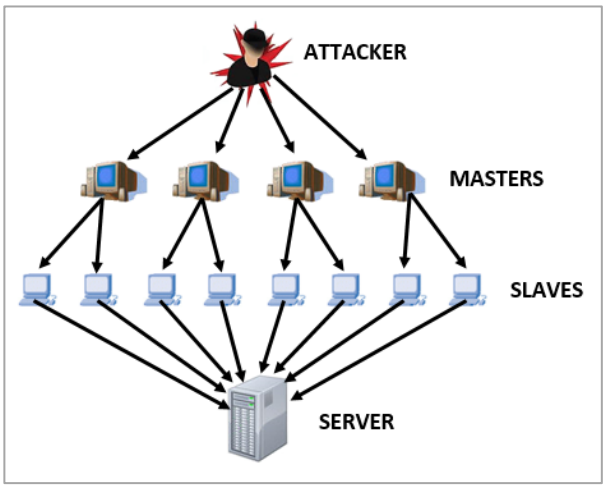

Figure 1. Scenario of DDoS Attack

B. Artificial Neural Network

Artificial neural network (ANN) is considered a nonlinear data modeling system, where models or patterns are placed in complex relations between inputs and outputs. Neural networks have more learning skills. They are widely used for more difficult tasks, such as handwriting and face recognition. The neural network is also known as "perceptron". It was introduced in the early 1940's. They have only become a major element of artificial intelligence in the last several decades [5]. Different types of artificial neural networks are currently being used in machine learning but this research used recurrent neural network (RNN) for the detection of DDoS attacks. Figure 2 shows the architecture of an artificial neural network.

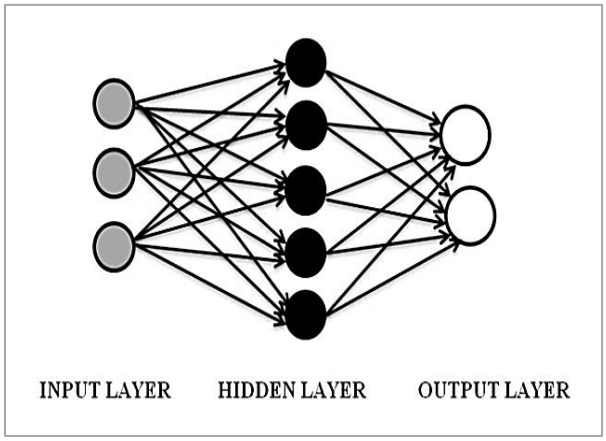

Figure 2. Architecture of Artificial Neural

There are three layers in the artificial neural network architecture:

1. Input Layer

The input layer of a neural network comprises a set of artificial input neurons. They transfer information from original neuron layers to the system for further processing. The workflow is initiated by the input layer for the neural network [5].

2. Hidden Layer

The hidden layer of the artificial neural network consists of between input and output layers, while the input and output of the artificial neurons are weighted by the number of inputs [5].

3. Output Layer

The final neurons' layer is an output layer that produces certain outputs in the program within an artificial neural network. The neurons in the output layer can be developed and treated differently, because they are the last "performer" nodes of the network [5].

C. Recurrent Neural Network

The network that involves backward links from output to the input and hidden layer is called a recurrent neural network. The recurrent neural networks often involve in deep learning and development of models and simulating the neural activity of human brains. An advanced artificial neural network (ANN) that includes a direct memory cycle is a recurrent neural network (RNN). The ability to build on previous network types with fixed-size input vectors. These input vectors are part of the recurrent neural networks. RNNs have an active field in image processing, language processing and even modeling applications that add characters to the text at a time [6]. Basically, you have an input that goes through a neural network and then you get an output. The layers between input and output are called secret layers, allowing the data to be manipulated accordingly as shown in Figure 3.

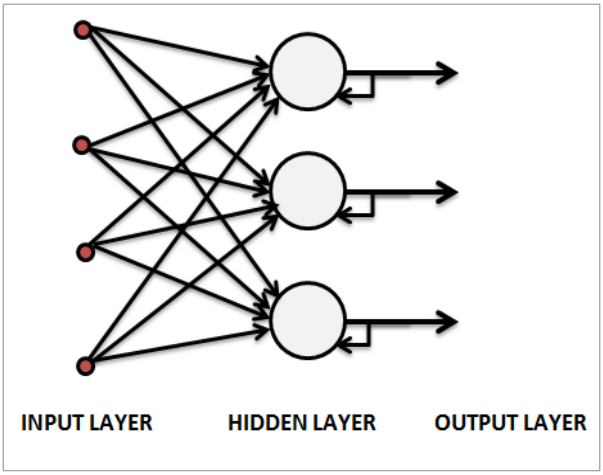

Figure 3. Recurrent Neural Network

D. Data Sets Description

In this section, few attacks have been presented, which can be caused by slow network performance, crash the system or make the service unavailable to the users. As the input vectors of the neural network, tested the input sets where knowledge discovery dataset (KDD) are used for instruction and validation. In the link files, the raw information set was processed. The 41 different characteristics were obtained for each association. Each link has been marked as ordinary or under a certain attack form. The 22 kinds of attacks can be categorized in four major classes as summarized in Table 1.

TABLE 1. FOUR MAJOR CLASSIFICATIONS OF THE ATTACKS

Classes / Categories	Major attacks
DoS	Neptune, Land, Back, Pod, Smurf, Teardrop
Probe	Port sweep, Nmap, Ipsweep , Satan
U2R	Perl, Rootkit, Load Module
R2L	Imap, Guess-passwd, Physpy, Warezmater, Warezclient, Multihop

1. Denial of Service (DoS)

The attacker requires a laptop and an internet connection to flood a specific system or resource. A device or memory resource by the attack of DoS which is an attacker and it is too busy or too complete to manage legitimate requests. It prevents legitimate users' access to network. An attacker attempts to avoid legitimate customers using a service, e.g., Neptune, Land, Back, Pod, Smurf, and Teardrop [7].

2. Probe

An attacker attempts to discover the target host data. For instance, by using the operating system to scan victims for knowledge of services. For the apparent purpose of circumventing its security control the information is gathered about a computer network by an operation. The port sweep, Nmap, Ipsweep and Satan are the types of available attacks [7].

3. User To Root (U2R)

An attacker has a local host account and attempts to receive root freedoms. The attacker used a buffer overflow attack. U2R is a class of attacks in which the attacker begins accessing the system's user account by sniffing passwords, dictionary attacks, or social engineering and is able to exploit certain weaknesses to get root access to the network [7].

4. Remote To Local (R2L)

An attacker has no local host account but tries to get it. When an attacker has the ability to send packets to a computer over a network it happens without having a user account of any particular computer. The attacker utilizes any security hole to gain local access as a user of the machine [7].

II. LITERATURE REVIEW

Tavallaee et al. [7] have proposed a new dataset NSL-KDD. It consists of selected records of the complete KDD dataset and it does not suffer from any mentioned shortcoming. The huge number of redundant records is the first important deficiency in the KDD dataset.

Having carried out a statistical review on this data collection. The authors addressed two important issues that have a major effect on the efficiency of the system analysis. The result shows very poor evaluation anomaly detection approaches. A new dataset i.e., NSL-ADD have been proposed by the

researchers to solve these problems. The selected records of the complete KDD dataset is consists of the proposed dataset. It is not suffered from any of the listed drawbacks.

Kumar and Selvakumar [8] proposed a framework which comprises on four primary modules: (i) information gathering module (ii) preprocessing (iii) grouping and (iv) reaction. The authors prepared a dataset by utilizing feed forward neural network. In any case, this neural system does not give great identification precision. The dataset prepared by utilizing the fake neural system and after that it tried with the RBP neural system to discover its identification exactness. Improving the efficiency of the RBP classifier is the objective of this paper.

Mane and Pawar [9] have identified various attacks with the support of supervised neural networks. Anomaly Intrusion detection system is used to detect various network attacks. The study consists of experimental neural networks which use only most relevant features of KDD 99 dataset (17 out of 41). To discover the intrusion signatures, the intrusion detection system is used. The system is intended to protect the system in connection with various network attacks such as DoS, U2R, R2L testing, etc. The IDS collects information from different networks and system sections.

Moradi and Zulkernine [10] introduced a neural intrusion detection network method for intrusion detection based on an off-line analysis strategy and Multi-Layer Perceptron (MLP). This research seeks to address a multi class issue that also detects the sort of assault via the neural network. Furthermore, in order to find the ideal neural network in relation to the amount of concealed layers, different neural network buildings are analyzed. In the training stage a technique for early stop validation is used to boost the neural network's generalization capacity.

Khanal and Lynton [11] have identified active DDoS attacks. However, this paper presents network connection failure during simulation in an effort to show how the network recovers during and after an attack. They present a simulation modelled a flood attack by sending a large number of TCP packets to the victim. The combined zombies managed to send over 8 MB worth of bogus traffic per second, more than enough to completely consume the victim’s available bandwidth. Because of this, packets were buffered at the server. Once the available buffers were completely filled, packets destined for the victim were dropped. This project offers a starting point for future work in distributed denial of service research. By presenting the in-depth result analysis.

Ali and Cotae [12] performed a research study of ANN as a machine learning solution for intrusion detection systems, denial of service attacks and distributed denial of service attacks. The proposed method has been used the Bayesian regularization (BR) back propagation and scaled conjugate gradient (SCG) back propagation algorithm. The network was trained and evaluated using a subset of the CICID2017 dataset that meets the real-world requirements.

Costa et al. [13] described a new IDS model for intrusion detection that is based on LSTM RNN. In the training phase, the LSTM RNN is able to learn the dataset features in great depth and conducts effective deep learning. Understanding the characteristics of network traffic involved in intrusions and distinguishing aberrant traffic from normal traffic requires this expertise. The detection of an IoT-botnet using a deep learning-based LSTM RNN (Long Short-Term Memory Recurrent Neural Network) model is explained in this research. The SVM (Support Vector Machine), LR (Linear Regression), and KNN (K-Nearest Neighbors) models are then used to compare the accuracy of this model. The model is trained and tested using the UNSW-NB15 dataset. There are nine different sorts of attack classifications in the dataset. This proposed model has a high level of accuracy. This may be expanded to include botnet detention in real time. Wire shark can collect real-time network data and identify IoT-Bot in a network.

Al-Islam et al. [14] examined various well-known DoS and DDoS attacks. The human brain is more accurate than mathematical computation in detecting these attacks, according to experience. As a result, I propose a technique for detecting these attacks that incorporates the human brain's representation, Recurrent Neural Networks (RNN). DoS and DDoS detection is difficult since they offer false data to IDS. The goal of an intrusion detection system (IDS) is to discern between true and false data in order to detect an assault. RNN is the most effective tool for this categorization. I solely consider the detection approach in this work. The detection produces posteriori probability as a result. Actions should be taken in accordance with the probability's range.

Secure data transmission is crucial in achieving all of the fundamental objectives of social multimedia networks, including dependability, scalability, Quality of Information (QoI), and Quality of Service (QoS). To fulfill the growing user demands and give more fast and actionable insights, a trust-based paradigm for multimedia analytics is widely desired. Software Defined Networks play an important role in this respect; yet, various constraints, such as runtime security and energy-aware networking, limit their ability to assist effective network control and management. As a result, a hybrid deep learning based anomaly detection strategy for suspicious flow identification in the context of social multimedia is developed in order to improve the dependability of SDN. It is made up of two modules) An anomaly detection module that uses an enhanced Restricted Boltzmann Machine and Gradient Descent based Support Vector Machine to detect aberrant activities, and (2) an end-to-end data delivery module that complies with SDN's demanding QoS criteria, such as high bandwidth and low latency. Finally, the suggested approach was tested on real-time and benchmark datasets to demonstrate its effectiveness and efficiency in terms of anomaly detection and data transmission, both of which are critical for social multimedia.

Furthermore, a large-scale analysis of the CMU-based insider threat dataset was performed to determine its performance in terms of detecting malicious actions including identity theft, profile cloning, and confidential data collecting, among others [15].

Kim et al. [16] created a DL-based intrusion model that focuses on denial of service (DoS) assaults in particular. We use the KDD CUP 1999 dataset (KDD) for the intrusion dataset, which is the most extensively used dataset for evaluating intrusion detection systems (IDS). DoS, user to root (U2R), remote to local (R2L), and probing are four types of attacks covered by KDD. Machine learning has been used in a number of KDD research to categories the dataset into the four categories or two categories, such as assault and benign. Rather of focusing on broad categories, we concentrate on specific attacks that fall into the same group. Unlike the other KDD categories, , there are enough samples in the DoS category to train each attack. We also use CSE-CIC-IDS2018, the most recent IDS dataset, in addition to KDD. CSE-CIC-IDS2018 includes more sophisticated DoS attacks than KDD. We concentrate on the DoS category in both datasets in this paper and create a DL model for DoS detection. We build our model using a Convolutional Neural Network (CNN) and compare it to a Recurrent Neural Network to see how well it performs (RNN). Furthermore, based on several studies, we recommend the best CNN design for improved performance.

In this paper, Rehman et al. have detected and identified DDoS attacks on the network. The DIDDOS is assessed utilizing the state-of-the-art CICDDoS2019 dataset and deep learning techniques such as GRU and RNN, as well as traditional machine learning algorithms like as NB and SMO. The DIDDOS was shown to be the most effective at detecting and identifying DDoS attacks in the experiments. Based on the results of the experiments, it is clear that our proposed approach provides promising performance in terms of accuracy, precision, recall, and F1-score. In the instance of an SSDP assault, the maximum accuracy attained was 99.91 percent, with an average of 99.7 for all other attacks. Furthermore, the precision, recall, and F1-score for SSDP assaults are 99.83 percent, 99.79 percent, and 99.79 percent, respectively. for all other types of assaults Furthermore, the precision, recall, and F1-score for SSDP assaults are 99.83 percent, 99.79 percent, and 99.69 percent, respectively. We want to use this dataset in an intrusion detection system in the future, and the network module can be updated to an intrusion prevention system to identify and block DDoS attacks.

Kumar et al. [18] worked on Convolutional Neural Networks and variants of Recurrent Neural Networks (i.e. Long Short-Term Memory, Bidirectional Long Short-Term Memory, Stacked Long Short-Term Memory, and Gated Recurrent Units) have been proposed in this paper as Deep Learning-based approaches to detect Distributed Denial of Service attacks. The Deep Learning techniques were tested using the Portmap.csv file from the CICDDoS2019 DDoS dataset. The data is pre-processed before being fed into the Deep Learning algorithms. The pre-processed dataset is used to train and test Deep Learning techniques. In compared to other Deep Learning-based algorithms, the RNN-based Stacked-LSTM Deep Learning approach gives the greatest results in identifying Portmap DDoS attacks, according to the reporting results.

New and inventive methods used by attackers to avoid installed security solutions, detecting distributed denial-of-service (DDoS) attacks remains a difficult task. In this paper, we propose an unsupervised machine learning (ML)-based strategy for detecting various forms of DDoS attacks by improving the performance of the K-means clustering algorithm using a hybrid feature selection and extraction method. We develop a hybrid method for extracting encoded features by progressively integrating an integrated feature selection (IFS) algorithm and a deep auto encoder (DAE), which can better differentiate benign from malicious network traffic clusters. The problem of detecting DDoS attacks is presented as a binary clustering of network flows. Despite the fact that K-means clustering is the most basic and frequently used technique, we examine its efficacy in detecting DDoS attacks before and after using the proposed hybrid method for feature selection and extraction. Our findings show that using the suggested hybrid method increases the performance of the K-means clustering model, making it comparable to state-of-the-art supervised ML and deep learning (DL)-based DDoS attack detection systems [19].

Khan and ashfaq [20] formed NIDS by using HCRNN, which is effective in cyber security. A CSE-CIC-DS2018 dataset was used to train the ID system framework. For the suggested ID system, we used a combination of classic classification approaches (LR, DT, XGB, etc.) and the HCRNN technique. After the CNN layers, we added recurrent layers to capture both spatial and temporal data more effectively. In this method, we aimed to successfully address the vanishing and expanding gradient difficulties, enhancing the ability to capture spatial and temporal correlations and learn efficiently from variable extent sequences. The suggested ID system based on DL classification was developed to integrate the advantages of both anomaly-based (AB) and signature-based (SB) techniques. The recommended and proposed ID system aids in the reduction of computing complexity. Resulting in improved intrusion detection accuracy and DR.

III. Design Of Proposed Architecture

The proposed system uses Recurrent Neural Network. The performance of the system is evaluated using KDD Cup dataset. Figure 4 shows step by step flow of the system. It includes stages like KDD dataset (data collection), cleaning

the data, neural network model and training of neural network by using three different algorithms [2,3].

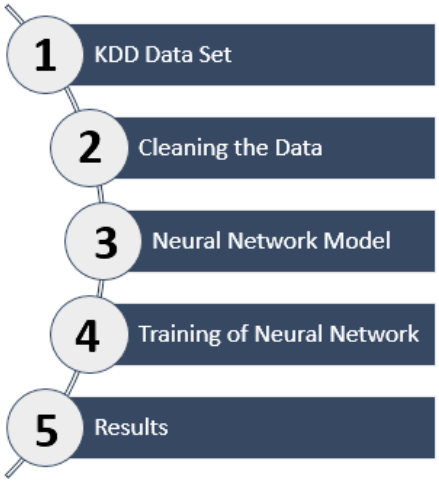

Figure 4. Proposed Design

1. Knowledge Discovery in Databases (KDD) Dataset:
First KDD dataset is collected from the trusted source in additional steps of processing. Recently, a wide range of pattern recognized and machine learning algorithms have been used to develop a KDD1999 dataset. It was launched for the KDD Cup competition in 1999. The KDD Cup 1999 standard database contains connecting records of attacks and interference in a network. The KDD dataset used for testing and training purposes.

2. Cleaning The KDD Data:
Before the training pre-processing KDD dataset is clean and assigns protocol, attack and flag values.

3. Neural Network Model:
We have to build up the proposed network model with the data collected after the collection of desired data.

4. Training of Neural Network:
Training of neural network is a very important feature of DDoS attack simulation. In this phase Recurrent neural network has been trained for analyzing the predefine behavior of proposed algorithms and compare the better result accuracy with short timing.

5. Result:
In this phase, the better training algorithm has been identified for the detection of DDoS attacks by using KDD data set.

IV. Result and Discussions

The purpose of the training is to make the system able to learn and classify the input traffic into desired category. The training of the proposed system has been composed of three different algorithms using recurrent neural network. The MATLAB 2018a simulator has been used for training purpose. During the design, cleaning the KDD dataset and give the values of protocols, attacks and flags. Afterwards, the neural network model has been developed and delivers training the KDD dataset using ANN. After training, the results of DDoS attacks' detection have been analyzed using ANN tool box of MATLAB. Here assign the values in "Protocol type" TCP=1, SMTP=2, HTTP=3, UDP=4, URP_I=5, FTP_DATA=6, FINGER=7, FTP=8, DOMAIN=9, NTP_U=10, "Flag" with corresponding values S0=0, RSTR=1, S1=2, REJ=3, S2=4, SO=5, SH=6, RSTO=7, SH=8, S1=9, OTH=10. The "Attacks" in the dataset have been categorized as normal=0, warezclient=1, back=2, smurf=3, teardrop=4, ipsweep=5, multihop=6, neptune=7, ftp_write=8, nmap=9, warezmaster=10, pod=11, buffer_overflow=12, and so on.A layer Recurrent Neural Network (RNN) has been used for entire experiment as shown in Figure 5.

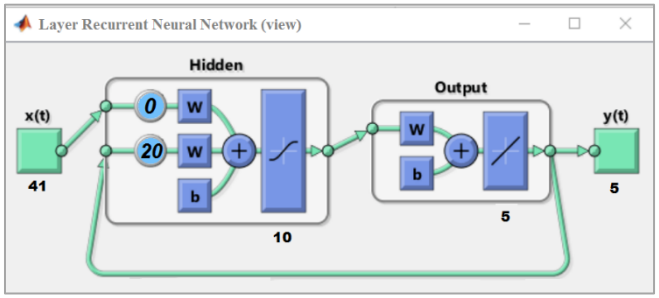

Figure 5. Artificial Neural Network

In this research, three algorithms have been used:
1) Gradient descent with momentum algorithm.
2) Scaled conjugate gradient algorithm.
3) Variable learning rate gradient descent algorithm.

A. Gradient Descent with Momentum Algorithm

A strategy to refine the machine learning operations is called gradient descent algorithm. In order to optimize a problem, the gradient descent algorithm is designed to adjust the input weight of neurons in artificial neural networks. It identifies minimum or global minimum level. The algorithm gradient descent involves reducing the prediction error or gap between the theoretical values and the observed values. It also involves for adjusting the input weights in the course of master learning. Momentum is a method that helps to speed up the vectors of gradient in the correct direction and to converge faster. It is one of the best known optimization algorithms and it is trained with several state-of-the-art models [21].

Figure 6 shows the neural network training state plot. It also shows validation check at epoch 1000 time 15 min 20 sec and performance 0.0218 and validation check value is 0. The performance of RNN shows that validation goes to optimizing the threshold. The Figure 6 shows the performance curve which produced during training, testing and validation of the network. We get the best validation performance 0.022325 at 1000 epochs.

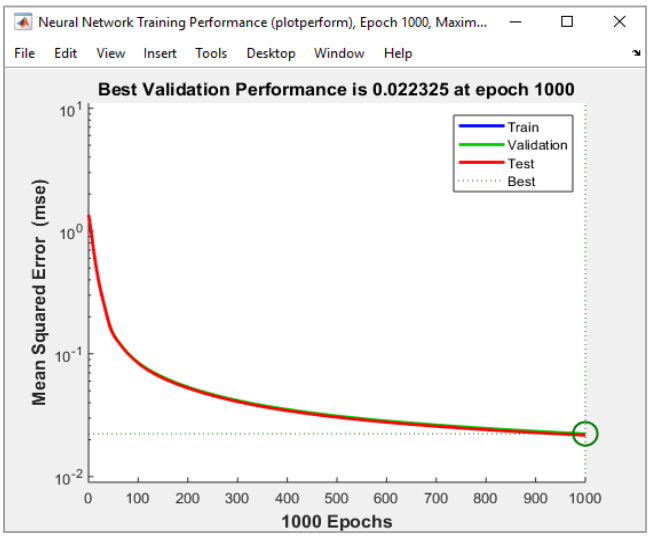

Figure 6. Neural network training state plot

Figure 7 shows the classification value fit net with shallow neural network which is 95.5% and miss classification 4.5%.

Figure 7. Confusion Matrix of Gradient Descent with Momentum Algorithm

B. *Scaled Conjugate Gradient Algorithm*

Implementing a supervised algorithm with a linear convergence rate (Scaled Conjugate Gradient). The algorithm is based on an optimization class known as conjugate gradient methods in numerical analysis [22].

The complete training of neural network as shows in Figure 8. The epoch value is 907 iterations, total time 27 min 20 sec, and performance is 0.00011399.

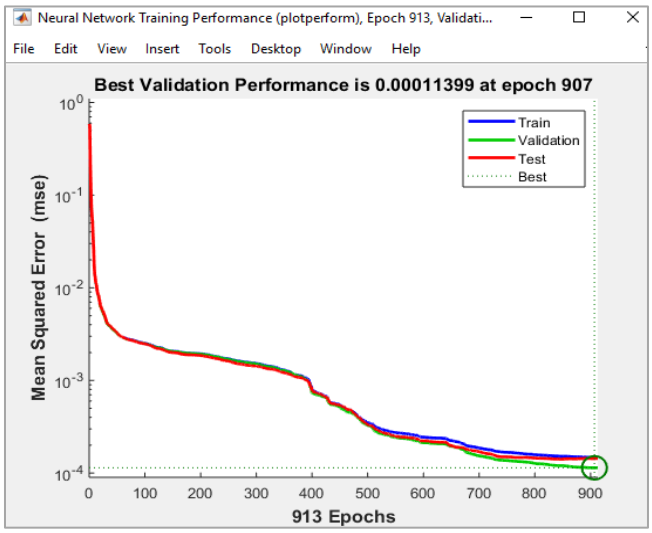

Figure 8. Validation Performance of Scaled Conjugate Gradient Algorithm

Figure 9 shows the classification value fit net with RNN which is 100% and miss classification 0.0%.

Figure 9. Confusion Matrix Scaled Conjugate Gradient Algorithm

C. *Variable learning rate gradient descent algorithm*

Gradient descent is an iterative optimization algorithm in the first order for the minimum function. Deep learning neural networks are trained using a stochastic gradient optimization algorithm. The learning rate is a hyper parameter that determines how much to modify the model in response to the predicted error every time the weights of the model are adjusted. The amount of weights that are changed during training is referred to as the step size or the "learning rate" [22]. After complete training of neural network, it shows the epoch 129 iterations, time 0:02:29, validation performance is 0.0075627 as shown in Figure 10.

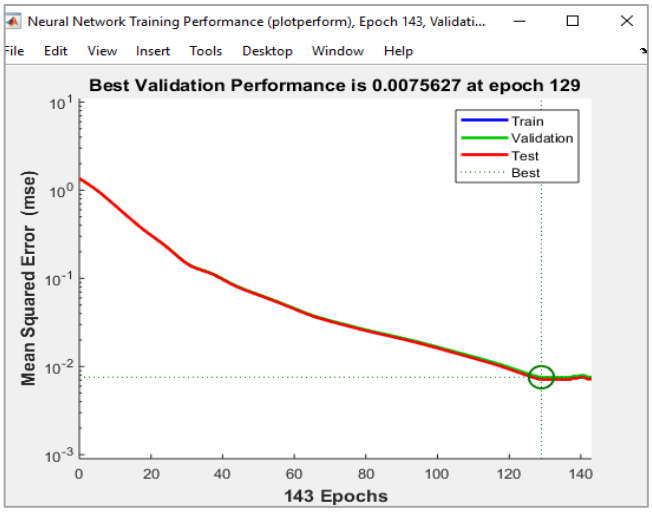

Figure 10. Validation Performance of Gradient Descent

Figure 11 shows the classification value of neural network which is 98.9% and miss classification 1.1%.

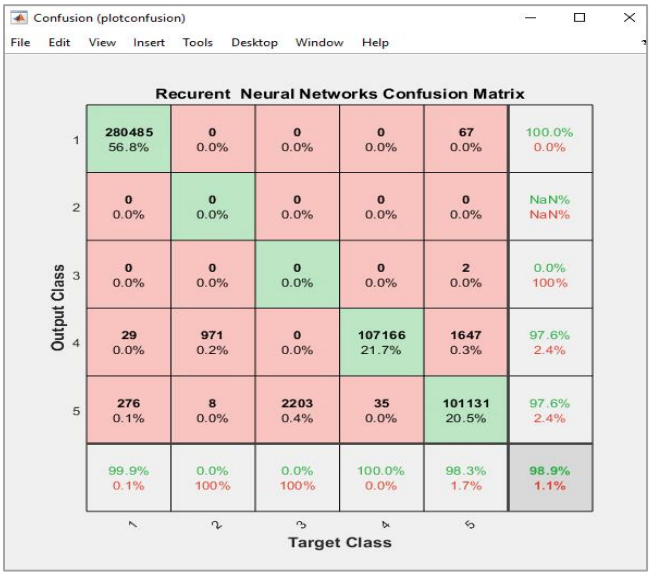

Figure 11. Confusion Matrix of Variable Learning Rate Gradient Descent Algorithm

Table 2 shows the RNN training of three different algorithms. The result shows that Variable Learning Rate, Gradient Decent algorithm gives better results as compared to two other selected algorithms. The success rate (accuracy) is 99.9% and training done in less time, i.e., 2 minutes and 29 seconds.

TABLE 2. SUCCESS RATES AND TIMING OF ALL STAGES

S#	Algorithm	Success Rate	Timing
1.	Gradient Descent with Momentum	95.5%	15:20
2.	TrainSCG: Scaled Conjugate Gradient	100%	27:20
3.	Variable Learning Rate, Gradient Descent	99.9%	02:29

V. CONCLUSIONS

Now-a-days security is a major issue of internet users. Where there are many serious security thread for internet users, there are distributed denial of service (DDoS) attacks. DDoS attack actually do not allow the access services to the users. In this research study, the recurrent neural network has been used for training and detection of DDoS attacks. Three well-known algorithms have been selected, i.e., i) gradient descent with momentum algorithm, ii) scaled conjugate gradient, and iii) variable learning rate gradient descent algorithm.

The aim of this research was to identify the best algorithm according to accuracy and training time. The recurrent neural network was trained to check the accuracy and detection of DDoS attacks. The result shows that the "Variable Learning Rate, Gradient Descent" algorithm provides better results in a short training duration with good precision performance 99.9 % accuracy and training time is 2 minutes and 29 seconds as compared to "Scaled Conjugate Gradient" algorithm and "Gradient Descent with Momentum" algorithm. In future, various techniques, models and neural networks may be used for deep learning and machine learning. Domain Name System (DNS) amplification attack [23] is also biggest DDoS may be compare and analyze in future. The other algorithms can also be compared and identified which neural network or technique is better suited for detecting DDoS attacks.

REFERENCES

[1] Brohi, A., Butt, P., Sheikh, S., Maher, A., & Mahesar, H. (2019). Study of the Governing issues for Implementation of Cyber Security system and Digital Morals in Pakistan. Sindh University Research Journal-SURJ (Science Series), 51(01), 25-30.

[2] Ye, J., Cheng, X., Zhu, J., Feng, L., & Song, L. (2018). "A DDoS Attack Detection Method Based on SVM in Software Defined Network. Security and Communication Networks," 2018.

[3] Kumar, V. P. (2011). "ANALYSIS OF DDoS ATTACKS IN DISTRIBUTED PEER TO PEER NETWORKS''. Journal of Global Research in Computer Science, 2(7), 10-16.

[4] Mukhopadhayay, I., Polle, S., & Naskar, P. (2014). Simulation of denial of service (DoS) attack using matlab and xilinx. IOSR Journal of Computer Engineering (IOSR-JCE), 16(3), 119-125.

[5] Iftikhar Ahmad, I., Abdullah, A. B., & Alghamdi, A. S. (2009, October). Application of artificial neural network in detection of DOS attacks. In Proceedings of the 2nd international conference on Security of information and networks (pp. 229-234). ACM.

[6] Bediako, P. K. (2017). Long Short-Term Memory Recurrent Neural Network for detecting DDoS flooding attacks within TensorFlow Implementation framework.

[7] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). "A detailed analysis of the KDD CUP 99 data set". In 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications (pp. 1-6). IEEE.

[8] Kumar, P. A. R., & Selvakumar, S. (2011). Distributed denial of service attack detection using an ensemble of neural classifier. Computer Communications, 34(11), 1328-1341.

[9] Mane, V. D., & Pawar, S. N. (2016). "Anomaly based ids using backpropagation neural network. International Journal of Computer Applications", 136(10), 29-34.

[10] Moradi, M., & Zulkernine, M. (2004, November). A neural network based system for intrusion detection and classification of attacks. In Proceedings of the IEEE International Conference on Advances in Intelligent Systems-Theory and Applications (pp. 15-18).

[11] Khanal, S., & Lynton, C. (2013, October).” Packet Simulation of Distributed Denial of Service (DDoS) Attack and Recovery”. In International Telemetering Conference Proceedings. International Foundation for Telemetering.

[12] Ali, O., & Cotae, P. (2018, November). Towards DoS/DDoS Attack Detection Using Artificial Neural Networks. In 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 229-234). IEEE.

[13] Costa, Jenny, Nandini Fal Dessai, Shivani Gaonkar, Shailendra Aswale, and Pratiksha Shetgaonkar. "IoT-Botnet Detection using Long Short-Term Memory Recurrent Neural Network", International Journal of Engineering Research & Technology (IJERT), 9(08), pp. 531-536.

[14] Al Islam, ABM Alim, and Tishna Sabrina. "Detection of various denial of service and Distributed Denial of Service attacks using RNN ensemble." In 2009 12th International Conference on Computers and Information Technology, pp. 603-608. IEEE, 2009.

[15] Garg, Sahil, Kuljeet Kaur, Neeraj Kumar, and Joel JPC Rodrigues. "Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective." IEEE Transactions on Multimedia 21, no. 3 (2019): 566-578.

[16] Kim, Jiyeon, Jiwon Kim, Hyunjung Kim, Minsun Shim, and Eunjung Choi. "CNN-based network intrusion detection against denial-of-service attacks." Electronics 9, no. 6 (2020): 916.

[17] S ur Rehman, Saif, Mubashir Khaliq, Syed Ibrahim Imtiaz, Aamir Rasool, Muhammad Shafiq, Abdul Rehman Javed, Zunera Jalil, and Ali Kashif Bashir. "DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU)." Future Generation Computer Systems 118 (2021): 453-466.

[18] Kumar, Krishan, and Sunny Behal. "Distributed Denial of Service Attack Detection using Deep Learning Approaches." In 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 491-495. IEEE, 2021.

[19] Marvi, Murk, Asad Arfeen, and Riaz Uddin. "An augmented K-means clustering approach for the detection of distributed denial-of-service attacks." International Journal of Network Management (2021): e2160.

[20] Khan, Muhammad Ashfaq. "HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System." Processes 9, no. 5 (2021): 834

[21] Ahmad, I., Ansari, M. A., & Mohsin, S. (2008, April). Performance comparison between backpropagation algorithms applied to intrusion detection in computer network systems. In Proceedings of the 7th WSEAS International Conference on Applied Computer and Applied Computational Science as ACM guide (pp. 47-52).

[22] Riadi, I., & Muhammad, A. W. (2017). Network Packet Classification using Neural Network based on Training Function and Hidden Layer Neuron Number Variation. Network, 8(6).

[23] Atan, A., Noor, M., & Ismail, M. (2016). DNS Amplification Attack Detection via Flexible Flow (sFlow). Sindh University Research Journal-SURJ (Science Series), 48(4D).