ISSN: 2581-3404 (Online) **IF: 5.445 (SJIF)**
International Journal of Innovative Research in Technology and Management, Volume-6, Issue-2, 2022.

PRP-Based Cascaded Feed-Forward Network for Detection and Prevention of DDoS Cyber Attacks

Rupali Jain[1], Chinmay Bhatt[2]
CSE, SRK University, Bhopal, India[1, 2]
reshuji675@gmail.com[1] , chinmay20june@gmail.com[2]

Abstract: *Researchers are facing an insurmountable challenge with cyber attacks. The Federal Communications Agency of the Marshall Islands was taken offline by hackers in 2022 thanks to a distributed denial of service attack. In this study work, a PRP (Polak–Ribière–Polyak) with cascaded feed forward networks was presented for the purpose of detecting DDoS cyber attacks. The PRP algorithm offers improved learning efficiency in addition to improved accuracy. When compared to various earlier weight optimizer approaches based on artificial intelligence as well as deep learning techniques, the suggested PRP algorithm demonstrates superior performance in terms of the outcomes it produces. Utilize MATLAB 2020 for the process of putting the given method into action. For the sake of carrying out the suggested approach, this body of study makes use of the data set that was produced by the Canadian Institute of Cyber Security in 2017 (CICIDS 2017). Accuracy, precision, selectivity, sensitivity, and confusion matrix are all areas in which the suggested technique performs admirably. The approach that has been described demonstrates an accuracy of 98.60%, and the other parameters are discussed in the section that discusses the simulation and the results.*

Keywords: DDoS, Cyber Attacks, Neural Networks, Feed Forward Network.

Introduction

The Internet has become an indispensable tool for human life in this epoch at every moment of life internet aids us. Hence to provide security for the internet become vital. In the proportion of advancement fear of unlawful activities has also been increasing rapidly. An attack on the basic pillars of security confidentiality, integrity, and availability is a sequence of activities having the aim of weakening computer network security. System attacks like external and internal attacks, attacks based on the network like a collection of information, Denial of Service by heavily requesting a particular target, and so on. There is no system which is made perfectly safe and secure because of few limitations, hence the attacker finally finds a loophole in the system to intrude, to analyze the network data for the probable intrusions (attacks), an IDS has become the principal component of computer security to bolster existing defenses.

1.2 Type of attacks

There are different type of attacks are happened in the cyber attack world. In the below section it shows the different attacks.

1.2.1 Anomaly based intrusion detection system (AIDS)

This model is created by using machine learning statistical and knowledge-based methods, any difference between the model's behavior and observed behavior is considered as an anomaly.

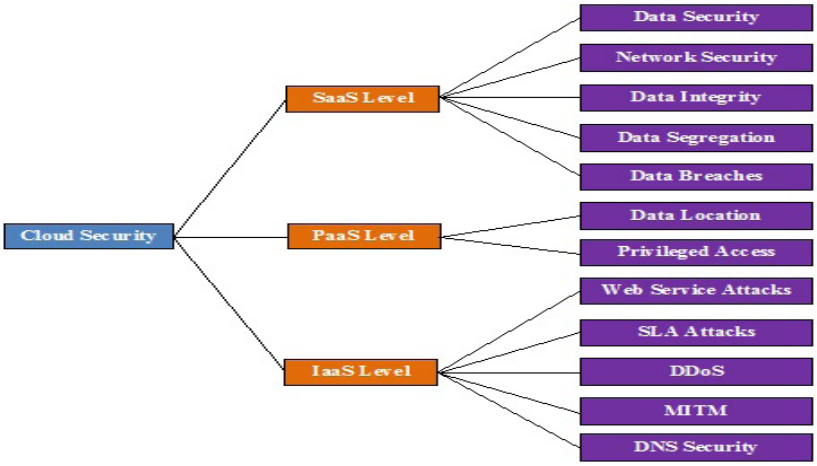

Figure 1: Type of Attacks in Clouds.

1.3 Machine learning based IDS detection

Machine learning is broadly classified into supervised and unsupervised. Supervised counts on the significant information in labeled data, lack of labeled data are a limitation for this method.

ANN - It has the strong fitting ability and is capable of dealing with non-linear data, it is susceptible to becoming stuck in the local optimum, and training is time taking via this approach, use of activation function and loss functions could be improvement measures.

KNN It applies to massive data, is very conducive for non-linear data, quickly trains the model, and is robust to noise, it takes a long testing time and is very sensitive to parameter k. It could reduce comparison time by using trigonometric inequalities and optimized parameters by using PSO (Particle swarm optimization) [14], balancing of the dataset could be done by SMOTE (synthetic minority oversampling technique) [15].

Naive Bayes It can learn incrementally, robust to noise, On attribute-related data, its performance is not up to the mark, importing of latent variable could be done to relax the independent variable [16].

SVM It has strong generation capabilities and learns useful information from the small training set, It does not perform well on big data and is very sensitive to the kernel function. For further improvement, optimization can be done by using particle swarm optimization [17].

Decision tree It has strong interpretation and select features automatically, balancing of data with SMOTE and introduction of latent variables may improve the performance [18].

K-Means It is simple and has strong scalability and can be fitted into big data, it can be trained rapidly [19].

Ensemble and Hybrid classifiers Some classifiers are weak in performance and do not perform as expected hence better approach comes into the frame by joining weak classifiers, which gives far better results than earlier, this approach is called the ensembling of classifiers. Ensemble method trained various classifiers and then by voting final output is selected.

II. Literature Review

***Afsaneh Banitalebi Dehkordi , et.al.* (2021),** In this research work According to the researchers, SDNs are the recent in network improvements because they are flexible, reduce operational costs, as well as provide protection against DDoS attacks. DDoS attacks of high and low volume can be detected using suggested here is a blend of statistics and machine learning. An entropy-based as well as classification-based collection method is used. Experimental tests on various datasets show that the entropy-based sections with static threshold do not

produce accurate findings when using the developed model that has been evaluated and analysed. Good outcomes for dynamic threshold come at the expense of a large false positive rate (FPR). To address this issue, a variety of classification techniques are run, and so more accurate results are generated [1]. ***Liu_et.al,* (2021)** In this research work analyzer suggested an impactful as well as real-time DDoS detection method for LAN and WAN environments that is both effective and real-time. To start, researchers drew a three-dimensional architecture based on network traffic characteristics (SIP and DIP). Comparing the traditional per-item-state mode of backups as well as compressibility with this sketch framework, it was found that this framework was more efficient in both concepts. With multidimensional sketch structures, network information can be stored in a more efficient way. By comparing it to a SIP sketch, this structure effectively improves the detection effects of LDDoS attacks. An enhanced behaviour divergence measurement technique was then used to measure the differences in behaviour between the normal sketch and the attack sketch. The energy percentage of input divergences was calculated using a reordered daub 4 wavelet transform. Maintaining a stable traffic baseline as well as successfully distinguishing between DDoS attack traffic and normal traffic is made possible by this approach. To achieve a dynamic threshold mechanism, we developed a more efficient exponential weighted moving average (EWMA). The dynamic threshold is more in line with the real network environment and the inherent dynamic of the network because it is based on actual changes in network traffic. In addition, we suggested the freezing mechanism for calculating the normative dynamic threshold. We can conclude that the freezing mechanism effectively reduces false positive and false negative rates by avoiding the threshold polluted by attack traffic. Furthermore, the proposed LDDM has a good time feasibility because each component's run time is computed. Finally, the analysis shows that LDDM is superior to other methods in terms of accuracy as well as TPR, as well as lower FPR and FNR for more concealed as well as low-rate DDoS attacks. Meanwhile, they demonstrated that LDDM is flexible enough to work in a variety of network configurations [2].

Kushwah_et.al,* (2021),** In this research work researchers contend for Many kinds of data can be accessed via the Internet using cloud technology. The smooth operation of this software depends on the availability of web services. The availability of cloud services can be disrupted by DDoS attacks. Cloud servers DDoS attack detection is suggested using machine learning by the researchers. SaE-ELM with crossover adaptation is the first version of this device to be developed as an upgraded model. For a given situation, the implemented application is able to access the mutation strategy, crossover rate, and crossover operator that is most appropriate. The suitable number of hidden neurons is automatically determined by the researchers. The model's ability to learn is enhanced by these features. The DDoS attack detection system is then built using this design. Based on current datasets such as NSL KDD, ISCX IDS, UNSW-NB15 as well as CICIDS 2017, researchers evaluated the explained system's performance. KD-DTest+ and KDDTest-21 were the most accurate, followed by ISCX IDS 2012, UNSW-NB15 as well as CICIDS 2017 with 98.90percentage reliability, with 98.90%, 89.17 percent accuracy as well as 99.99 percent precision, respectively[3].Snehi_et.al,*(2021),** In this research work authors presented analysed the most devastating DDoS and IoT-DDoS attacks, as well as the elements of today's Cyber–Physical Device, architectural features, as well as security problems. A layer between perception as well as the cloud, Fog Computing has been suggested as a method of improving performance and performing the assigned duties on behalf of Cloud. DDoS/IoT-DDoS detection and reduction have been analysed. Next but not least, an uncertainty as well as gap evaluation was carried, as well as the narrow down method was used to identify general gaps or vulnerabilities in the possible solutions. Using that research study, they've attempted to summarise the vulnerability analysis that can serve as a foundation for future DDoS/IoTDDoS defence solutions for future technologists and researchers. DDoS attacks are just one of a number of cybersecurity risks that the vulnerability research examines. Provided the wide range of options[4].***Wang, et.al. (2020),*** In this presented research work, the main purposes is to improve the availability of robust machine learning-based detection

methods, According to the MLP model, researchers don't take into account the fact that functionality might be removed as well as that traffic can be unpredictable. Authors demonstrated problem, which is not widely addressed by the community, through implementing and testing in the machine learning phased case. MLP-based detection method against the DDoS attack through combing with sequential feature selection and feedback mechanism. According to the results, on the one hand, presented method had comparable detection performance on the popular benchmark data NSL-KDD compared with some related works. The main contributions of this work presented an easily feasible and interactive method to combine feature selection with MLP model designed a feedback mechanism to perceive detection errors based on the recent detection results[5].***Perez-Diaz, et.al (2020),*** This research work presented, a flexible modular architecture is shown in this study that can identify and mitigate LR-DDoS assaults in SDN environments. Six machine learning (ML) models are used to train our intrusion detection system (IDS), including J48, Random Tree, REP Tree, Random Forest, Multi-Layer Perceptron, as well as Support Vector Machines (SVM). Despite the difficulties of identifying LRDoS assaults, our technique achieves a detection rate of 95 percent, according to the assessment results [06].

III. Proposed Method

A. Distributed Denial of Service (DDoS)

Internet resources and services are made unavailable to their intended users by denial of service (DoS) attacks. Flooding the victim machine with external communication requests is a common DoS attack tactic, and it renders the device unable to reply to valid traffic.

B. Proposed Work

In this section discuss the proposed method. The key objective of a Distributed Denial of Service (D-DoS) attack is to compile multiple systems across. The Internet with agents and form botnets of networks.

C. Training

On*q*-Polak–Ribière–Polyak conjugate gradient algorithm

This section discusses the proposed solution for the detection and identification of DDOS attacks on clouds. **On*q*-Polak–Ribière–Polyak conjugate gradient algorithm** Consider the following unconstrained nonlinear optimization problem:

$$(P)\ \min f(x) \qquad (1)$$

Where $f : R^n \to \mathbb{R}$ is a continuously q-differentiable function. The numerical optimization algorithms of general objective functions differ mainly in generating the search directions. In the conjugate gradient algorithms, a sequence of iterates is generated with a given starting point $x^0 \in R^n$ by the following schema:

$$x^{k+1} = x^k + p^k,\ p^k = a_k d_q^k, \qquad (2)$$

for all $k \geq 0$, where x^k is the current iterate, d_q^k is a descent direction of f at x^k and $a_k > 0$ is the step-length. Note that the descent direction $d^k q_k = -g^k q_k$ leads to the q-steepest descent method. In the case q^k approaches,

$$(1,1,\ldots,1)^T \qquad (3)$$

as $k \to \infty$, the method reduces to the classical steepest descent method [7]. The search direction $d^k q$ is guaranteed to have a descent direction due to the following:

$$(g_{qk}^{k})^{T} d^{k}{}_{qk} < 0. \quad (4)$$

The directions $d^{k}{}_{qk}$ are generated in the light of classical conjugate direction methods as:

$$a_{k} d_{q}^{k}{}_{k} = \begin{cases} -g^{k} q_{k} k = 0 \\ -g^{k} q_{k} + \beta_{k} q^{-PRP} d^{k-1} q^{k-1} k \geq 1 \end{cases} \quad (5)$$

where $\beta_{k}{}^{q-PRP} \in R$ is modified from a scalar quantity β^{k} in the PRP method and presented as follows:

$$\beta_{k}{}^{q-PRP} = \frac{(g^{k}{}_{qk})^{T} (g^{k-1} - g^{k-1})}{\left\| g^{k-1}_{qk-1} \right\|^{2}}. \quad (6)$$

D. Training of D-DoS attack detection

In the machine learning process, training is an important part of the proposed attack detection. For the training first required the data set of previous attack. For the implementation of proposed method, we use (Canadian Institute of Cybersecurity (CICIDS2017)) [31]. This data set is available Kaggle website.

Steps of Training by ***Polak Ribiere Polyak (PRP)***

1. Start
2. Select Data set,
3. Load training data % train data tr label
4. Apply Labeling on data,
5. for i = 1:length(reduce)
6. val = tr_label2(i);
7. t(i,val) = 1;
8. end
9. **%Apply Training Using Polak Ribiere Polyak (PRP)**
10. net1 = cascade forward net(size(x,2),'traincgp')
11. net1.train Param epochs = 30; % Number of iterations
12. net1.train Param goal = 1e-5; %
13. net1.train Param.min_grad = 1e-6;%
14. net1 = train(net1,x',t'); % Apply Cascaded feed forward
15. Perform(net,t,y) % Performance Calculation
16. Accuracy = match * 100 / length(reduce)
17. Modified Data Unique id Selected Features
18. Test net unique id selected feature % Training Data
19. End

E. Testing of D-DoS Attack Detection

Now discuss the testing for proposed CFFNN[21] based polak ribiere polyak (PRP). The DDoS attack classify benign attack, DoS Hulk, and DoS slow loris.

Testing of Cyber DDoS Attack

1. Start
2. [a,b,exc data]= xlsread('data-set');% Read data set
3. Load Final Test % Unique id elected feature

```
4. for j = 1:30 % Unique features cal.
5. rw = t_data(j);
6. Lookup =unique_id{selected_feat(j)};% Save features
7. s = find(rw==lookup); % find unique
8. t_data2(j) = s;
9. End
10. for y = net1(t_data2'); % Apply CFFNN
11. detected = unique_id{69}(loc); % Unique 69 feature
12. end
13. if (strcmp(req_cat,'BENIGN')) % Detection attack
14. actual(pos) = 1 ;
15. elseif(strcmp(req_cat,'DoS Hulk')) % Detection attack
16. actual(pos) = 2 ;
17. Else,
18. actual(pos) = 3; % DoS slow loris,
19. End,
20. detect(pos) = loc;,
21. End,
22. % Performance Parameters Calculation,
23. mat,selectivity, sensitivity, specificity, accuracy,
24. End
```

IV. Simulation & result

In this section we are describing out the implementation detail and designing issues for our proposed research work. By searching we have observed that for our proposed work the MATLAB 2020 is well known platform to perform suggested approach

Data set

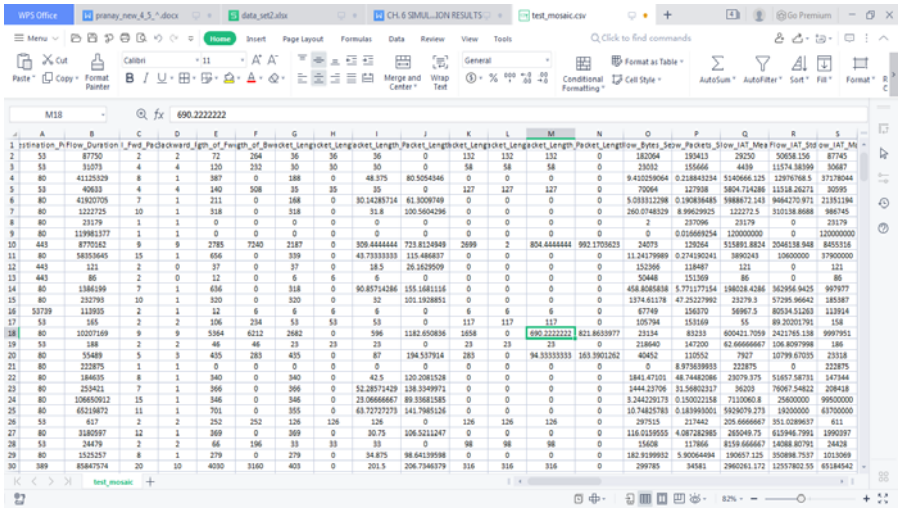

Figure 2: Data Set in Excel

ISSN: 2581-3404 (Online) **IF: 5.445 (SJIF)**

International Journal of Innovative Research in Technology and Management, Volume-6, Issue-2, 2022.

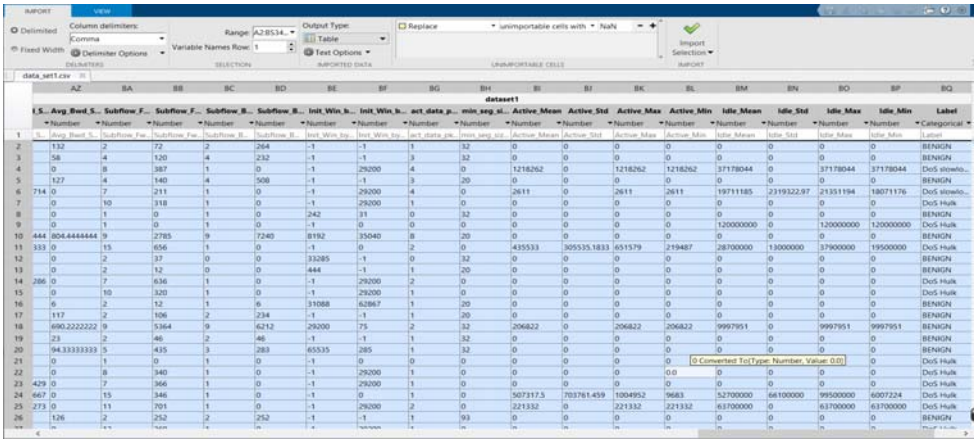

Figure 3: Data Set in MATLAB

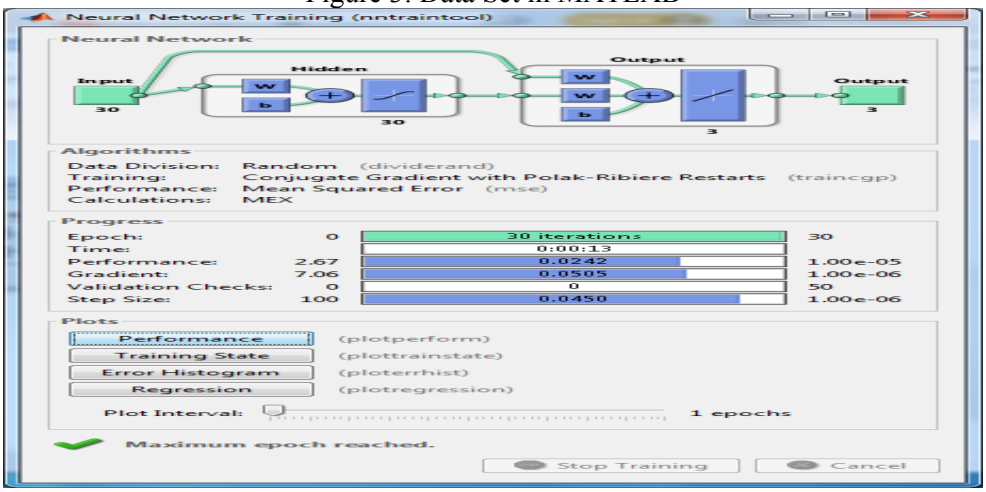

Figure 4: NN simulation model

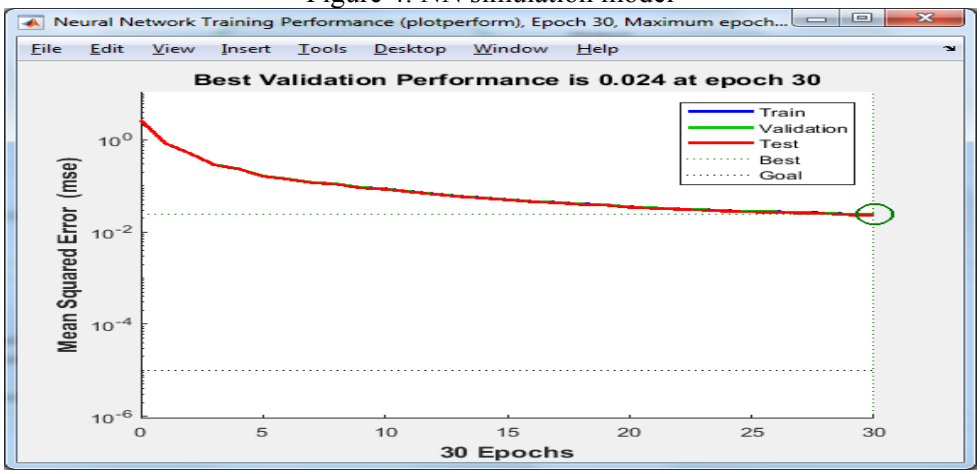

Figure 5: Output of training validation performance

ISSN: 2581-3404 (Online) **IF: 5.445 (SJIF)**
International Journal of Innovative Research in Technology and Management, Volume-6, Issue-2, 2022.

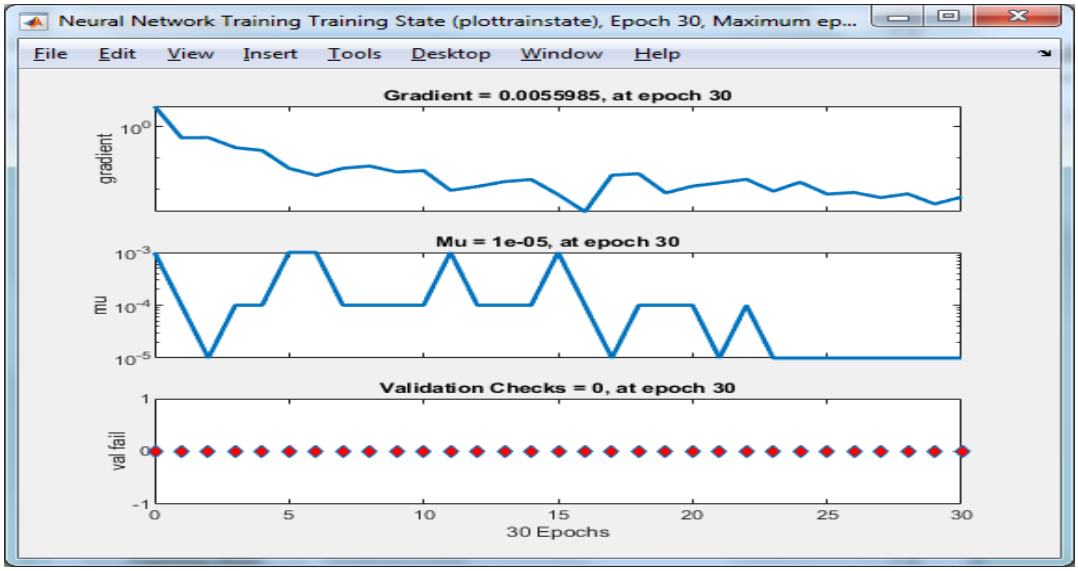

Figure 6: shows the neural network training states

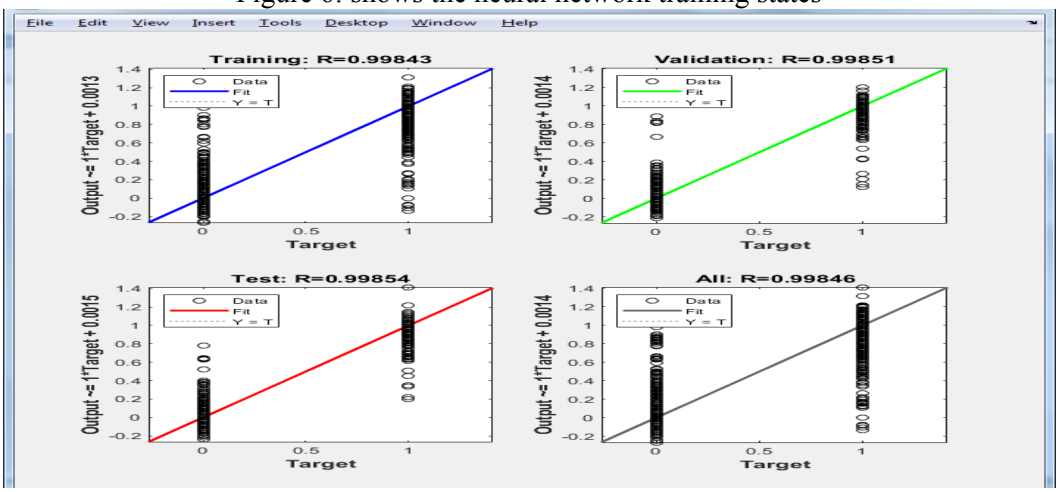

Figure 7: shows the result outcomes of training, validation and test

TABLE -II. Experimental Results

Proposed Accuracy (Acc)	**99.12**
Acc. hybrid	98.6070
True Positive	318 274 94
False Negative	0 4 3
False Positive	3 3 1
True Negative	372 412 595

V. Conclusion

The most of this work is analysis the various attacks of cloud computing, additionally discuss the various attacks on clouds and issues with cloud computing. In the last few year cloud computing is increases speedily and its application on different sectors. Each and every thing having two faces, one is positive and second is negative, cloud computing security threats are increases day to day.As a result of a denial of service (DDoS) attack, a targeted system is unable to provide regular services to its legitimate customers. In this proposed work presented modified feature selected based neural network for efficient DDoS attack detection. The implementation of proposed work is done in MATLAB 2020 software. MATLAB is well known academic as well as industrial research software this work. The proposed method design and simulated in the R2020 MATLAB. There are different type of DDoS attack are present in internet.

References:

[1] Afsaneh Banitalebi, MohammadReza Soltanaghaei, and Farsad Zamani Boroujeni. "The DDoS attacks detection through machine learning and statistical methods in SDN." The Journal of Supercomputing 77.3 (2021): 2383-2415.

[2] Liu, Xinqian, et al. "Low-rate DDoS attacks detection method using data compression and behavior divergence measurement." Computers & Security 100 (2021): 102107.

[3] Kushwah, Gopal Singh, and Virender Ranga. "Optimized extreme learning machine for detecting DDoS attacks in cloud computing." Computers & Security 105 (2021): 102260.

[4] Snehi, Manish, and Abhinav Bhandari. "Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks." Computer Science Review 40 (2021): 100371.

[5] Wang, Meng, Yiqin Lu, and Jiancheng Qin. "A dynamic MLP-based DDoS attack detection method using feature selection and feedback." Computers & Security 88 (2020): 101645.

[6] Perez-Diaz, Jesus Arturo, Ismael AmezcuaValdovinos, Kim-Kwang Raymond Choo, and Dakai Zhu. "A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning." IEEE Access 8 (2020): 155859-155872.

[7] Jia, Yizhen, et al. "Flowguard: An intelligent edge defense mechanism against IoT DDoS attacks." IEEE Internet of Things Journal 7.10 (2020): 9552-9562.

[8] Singh, Jagdeep, and Sunny Behal. "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions." Computer Science Review 37 (2020): 100279.

[9] Virupakshar, Karan B., et al. "Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud." Procedia Computer Science 167 (2020): 2297-2307.

[10] Singh, Maninder Pal, and Abhinav Bhandari. "New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges." Computer Communications 154 (2020): 509-527.

[11] Dong, Shi, Khushnood Abbas, and Raj Jain. "A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments." IEEE Access 7 (2019): 80813-80828.

[12] Agrawal, Neha, and Shashikala Tapaswi. "Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges." IEEE Communications Surveys & Tutorials 21.4 (2019): 3769-3795.

[13] Wang, An, et al. "Delving into internet DDoS attacks by botnets: characterization and analysis." IEEE/ACM Transactions on Networking 26.6 (2018): 2843-2855.

[14] Yang, Kun, Junjie Zhang, Yang Xu, and Jonathan Chao. "Ddos attacks detection with autoencoder." In NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, pp. 1-9. IEEE, 2020.

[15] Wani, Abdul Raoof, Q. P. Rana, U. Saxena, and Nitin Pandey. "Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques." In 2019 Amity International conference on artificial intelligence (AICAI), pp. 870-875. IEEE, 2019.

[16] Dayal, Neelam, and Shashank Srivastava. "An RBF-PSO based approach for early detection of DDoS attacks in SDN." In 2018 10th International Conference on Communication Systems & Networks (COMSNETS), pp. 17-24. IEEE, 2018.

[17] Li, Qian, Linhai Meng, Yuan Zhang, and Jinyao Yan. "DDoS attacks detection using machine learning algorithms." In International Forum on Digital TV and Wireless Multimedia Communications, pp. 205-216. Springer, Singapore, 2018.

[18] Hsieh, Chang-Jung, and Ting-Yuan Chan. "Detection DDoS attacks based on neural-network using Apache Spark." In 2016 international conference on applied system innovation (ICASI), pp. 1-4. IEEE, 2016.

[19] Buragohain, Chaitanya, and Nabajyoti Medhi. "FlowTrApp: An SDN based architecture for DDoS attack detection and mitigation in data centers." In 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), pp. 519-524. IEEE, 2016.

[20] Xiao, Peng, Zhiyang Li, Heng Qi, Wenyu Qu, and Haisheng Yu. "An efficient ddos detection with bloom filter in sdn." In 2016 IEEE Trustcom/BigDataSE/ISPA, pp. 1-6. IEEE, 2016.