International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Mitigating Economic Denial of Sustainability (EDoS) in Cloud Environment using Genetic Algorithm and Artificial Neural Network

Swati Nautiyal, C Rama Krishna, Shruti Wadhwa

Abstract: ***Economic Denial of Sustainability (EDoS) is a latest threat in the cloud environment in which EDoS attackers continually request huge number of resources that includes virtual machines, virtual security devices, virtual networking devices, databases and so on to slowly exploit illegal traffic to trigger cloud-based scaling capabilities. As a result, the targeted cloud ends with a consumer bill that could lead to bankruptcy. This paper proposes an intelligent reactive approach that utilizes Genetic Algorithm and Artificial Neural Network (GANN) for classification of cloud server consumer to minimize the effect of EDoS attacks and will be beneficial to small and medium size organizations. EDoS attack encounters the illegal traffic so the work is progressed into two phases: Artificial Neural Network (ANN) is used to determine affected path and to detect suspected service provider out of the detected affected route which further consist of training and testing phase. The properties of every server are optimized by using an appropriate fitness function of Genetic Algorithm (GA) based on energy consumption of server. ANN considered these properties to train the system to distinguish between the genuine overwhelmed server and EDoS attack affected server. The experimental results show that the proposed Genetic and Artificial Neural Network (GANN) algorithm performs better compared to existing Fuzzy Entropy and Lion Neural Learner (FLNL) technique with values of precision, recall and f-measure are increased by 3.37%, 10.26% and 6.93% respectively.***

Key words : Artificial Neural Network, Cloud Computing, EDoS attack, Genetic algorithm.

I. INTRODUCTION

Cloud computing is now one of the most researching area among researchers. It provides services to the users such as storage, accessing data from anywhere in the world. The organizations that provide the above-mentioned services are known as a cloud service provider and usually charge for cloud computing services on the basis of usage. Convenience, payout, flexibility, scalability and other peculiarities of this paradigm have attracted interest in placing the services of large corporations on the cloud. Nevertheless, responding to security threats and events is becoming the major concern of the cloud computing [1]. Its elasticity characteristic permits us to extend the assigned servers and provide multiple inquiries for our service. The use of cloud computing platforms that are rich with resources based on the requirement, known as 'pay per use' or utility computing [2]. In this computing, the traditional DDoS attack on the server has been transformed into a financial issue and creates a new attack named as economical denial of sustainability (EDoS) attack [3]. In other sense, EDoS attack makes the cloud network difficult to sustain financially. Some of the researchers are thinking that traditional DDoS attack and new form of DDoS that is EDoS attack are identical. However, some tried to reduce EDoS attack, its impact and influence on cloud environment. In this paper, we have reviewed various EDoS mitigation techniques and proposed a new reactive intelligent technique that uses GA along with ANN for mitigating the EDoS attack, which we named as Genetic and Artificial Neural Network (GANN) algorithm.

A. Distributed Denial of Service (DDoS)

DDoS attack is a destructive effort that makes a server or a network resource out of reach to genuine users. This occurs due to overloading the server/network by sending large number of requests. In this attack, an attacker initiated by obtaining the control of one computer and serves it as DDoS expert node [7]. In this way, DDoS attacker gains admission to enter into network and work as per the instructions provided by the DDoS expert node by sending number of requests to the destination server. This process results in overloading the destination server, hence, deny the further requests coming from the genuine user [8].

B. Economic Denial of Sustainability (EDoS)

In EDoS attack, the attacker brilliantly and deliberately moves to cloud computing auto scaling feature. This leads to an increase in utilization of computing resource of a destination user and results in huge resource costs as well as the security price provided to the destination cloud user [9]. This constant effort towards the utilization of cloud computing services by the target cloud user ends with a huge financial loss to the consumer. Therefore, economical expediency of cloud users is not sustainable which is described in Fig. 1 [10].

Manuscript published on 30 August 2019.
*****Correspondence Author(s)
Swati Nautiyal, PG Scholar, Department of Computer Science and Engineering, NITTTR, Chandigarh, India.
C. Rama Krishna, Department of Computer Science and Engineering, NITTTR, Chandigarh, India.
Shruti Wadhwa, Department of Computer Applications, Post Graduate Govt. College, Chandigarh, India

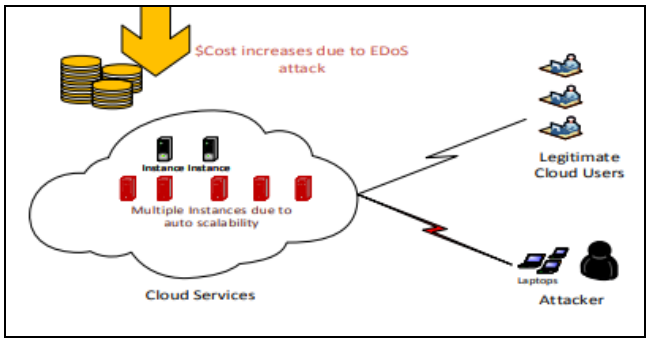

Fig. 1: Billing effect of cloud user due to EDoS attack [10]

DDoS attack focuses to cease all the services provided by the service provider. Thus, in DDoS attack, the attacker interrupts maximum server resources in a short interval. The purpose of such type of attacks is to completely discontinue the services or remarkably affect the quality of the service (QoS). On the contrary, EDoS attack is typically more intelligent and effective. It targets an individual by gradually push the illegal data towards the genuine user for a longer duration. EDoS concentrates on maximizing the financial costs of cloud-based consumers through cloud-based resources. The EDoS's traffic domain is somewhat different than the DDoS attack domain. The EDoS attack affects cloud computations in terms of performance as well as in terms of price model. EDoS may also lead to hike in cost of energy bill by consuming fraudulent resources. Table 1 shows the difference between EDoS and DDoS attack.

Table 1: DDoS Vs EDoS Attack

DDoS attack	EDoS attack
Degrade/block cloud services	Makes cloud resource economically unsustainable
The attacker period is very short	The attacker period is long
The attacker occurs above the EDoS attack zone	The attacks appear between normal data traffic and DDoS attack region

II. RELATED WORK

In this section, the previous work done by various researchers in the field on cloud computing to detect and protect cloud environment from EDoS attack is discussed.

Waters et al. [12] utilized a client –puzzle scheme to lessen the effect of EDoS attack on application as well as on network layer. This mechanism works as per user demand. A crypto puzzle is created and verified by the user. Brute force approach has been used to prove the authenticity for acquiring service. The system requires high cost when the mechanism is used in real time application.

Sqalli et al. [13] proposed a security mechanism against EDoS shield. This mechanism identified the malicious request to the server and denies the fraudulent request but it cannot secure the server from IP spoofing. Al-Haidari et al. [14] presented a Welch technique along with a queuing model. This model consists of different constraints such as throughput, end to end delay etc. to analyze the consequence of EDoS attack on cloud computing and also used to remove the warm-up period. But the system suffers from various drawbacks such as the computation time is more as the simulation length is five times more than the length of warm up period. To reach its steady state it require more time. Chowdhury et al. [15] has been used Game theoryto detect EDoS attack. This scheme generate game scenario between EDos attacker and defender. Best value has been found out using Nash equilibrium which blocks the EDoS attacker. The technique of solving games involving mixed strategies is very complicated especially in the case of large payment matrices. The stability of the system is maintained by the value of Poisson distribution that must be less than 1. W.Shruti et al. [16] firewall as a security mechanism has been used, which rejects the attack traffic before billing is triggered. This reduces the negative impact of EDoS attack which taking place on cloud services using hybrid filtering technique. Here, the data is protected when the firewall have a control on the entire perimeter. Bhingarkar et al. [17]Fuzzy entropy mechanism has been based on the fuzzy logic properties that used feedback mechanism to find the attack in the system Lion algorithm is an nature inspired optimization algorithm which is used to find out the EDoS attack according to their nature based on neural network. But the disadvantage of this system was that for the feedback mechanism, the pre-define-rule set is used and the chances of error generate became high with increment in simulation.

III. PROPOSED GENETIC AND ARTIFICIAL NEURAL NETWORK (GANN) TECHNIQUE

This section describes the proposed technique named as GANN technique which is a two way mechanism that takes the economic consumption of the nodes as the input. In this, mainly two techniques are used named as Genetic Algorithm (GA) and Artificial Neural Network (ANN). GA is an optimization algorithm, which is used to optimize the properties (energy consumed by each server) of the server. ANN is used to find and detect the faulty server. The phase diagram of the proposed technique is explained in Fig. 2.

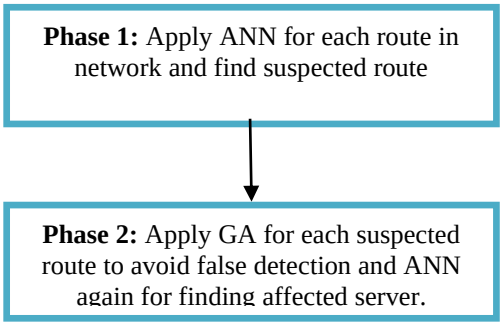

Fig. 2: Phase Diagram

Phase 1

In EDoS attack, the attacker continuously request bulk resources, so the various paths get affected due to this illegal traffic. Therefore, in phase 1, ANN is applied for finding the affected paths between source and destination server. The detail description is provided in the following section.

Artificial Neural Network (ANN) to detect affected route: An ANN is a computational model in which the functions depend on biological neural networks. The optimized data is sent to the input layer neurons that are forwarded to the output layer through the hidden layer [19]. In this paper, the cost consumption by each path is taken as input to find the affected path between source and destination server. Sigmoid function has been used as activation function to produce output. The input provided to the neural network is the number of transaction paths formed by the server along with the economic consumption. In hidden layer, input data is multiplied by the weight function and summed up the data obtained by all the input neurons. After obtaining difference between input data and output data, the value is fed back to the hidden neuron. This value adjusts the hidden neurons value until error value is minimized and we will obtain desired output.

ANN is further comprises of two phases: training and testing. In first phase, ANN is used to train the system on the basis of cost utilized by the servers for each route. The ANN is trained as per the number of paths along with the economic consumption of each route. The trained data becomes a test data by utilizing supervised learning process. The Levenberg Marquardt technique is used for classification. The ANN structure is shown in Fig. 3.

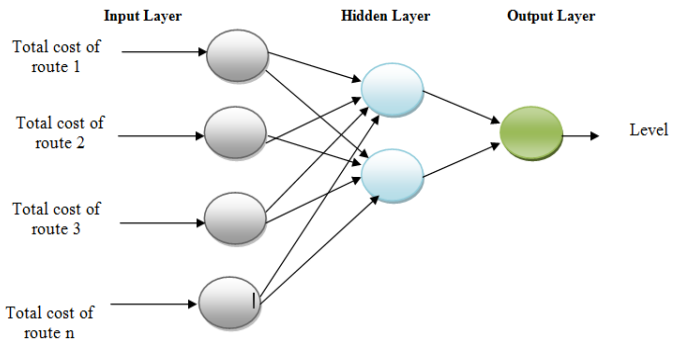

Fig. 3: ANN Structure for GANN Technique

Phase 2

The path between the source and the destination server can be overcrowded with the legal traffic rather than affected by the attackers' requests. Therefore, in this phase, Genetic Algorithm is utilized to optimize various properties of the server and to avoid false detection of affected paths because out of the extracted faulty path, some may fall into false selection. Hence, GA is applied over here. Once GA reduces the faulty paths, again ANN is applied to see the faulty node out of the faulty paths. Each path may have same or different nodes which are faulty.

Genetic Algorithm (GA) to avoid false path detection: GA is an optimization algorithm that works on the basis of natural selection process obtained from biological evolution [18]. In this paper, Genetic Algorithm has been used to optimize the properties of the node which is considered in the route and to reduce the faulty route. In population initialization, we initialize a group of all possible coded solutions for a given problem. Here, we initialize the properties of the route in terms of cost consumption, co-ordinates of servers and threshold value. Fitness function is termed as a function to which input is the solution and the suitable solution is generated as an output. The initialized population is evaluated using this fitness function to check whether the given solution is considered as acceptable or not. The formula used for fitness function is defined below:

$$\text{Fitness}(\text{server}) = \begin{cases} 1, energyconsumption > threshold \\ 0, otherwise \end{cases} \quad (1)$$

Where, 1 denotes the attacker server, 0 represents the normal server

For further selection, P_{val} and $Threshold_{val}$ parameters are used. Crossover function is applied to select the best property of server to find out the affected and non-affected path as per fitness function. In mutation phase, GA categorized the server property with some changing feature to segregate the input data in affected or non-affected list. GA determined the properties of each node that forms the affected route.

Threshold of ECR is given by,

$$ECR = \frac{\sum_{i=1}^{server} EC(i)}{Totalnumberofserver} \quad (2)$$

The GA algorithm is defined in the following:

Algorithm 1: Pseudocode of Genetic Algorithm to avoid false path detection

Required Input: Properties of Server & Fitness/objective Function

Obtained Output: Affected Path with optimized server features

1 $Fitness\ Function = \begin{cases} Ture; & if\ P_{val} < Threshold_{val} \\ False; & Otherwise \end{cases}$

2 Find Rows and Columns of server features

3 Initialize GA parameters – Iterations (T)

– Population Size (P)

– Crossover function

– Mutation function

– Selection function

(P_{val} and $Threshold_{val}$)

4 Optimized Properties = [] // *initialize empty variable*

5 Affected Path = [] // *initialize empty variable*

6 for range of Row (i)

7 for range of Column (j)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$P_{Val} = Server\ Properties\ (i, j)$

$Threshold_{Val} = \frac{\sum_{i=1}^{F} \text{Server feature (i,j)}}{Lengthof Server\ features}$

$Fitness\ Function = Fit\ Fun\ (P_{Val},\ Threshold_{Val}))$

$Optimized\ feature = GA\ (Fitness\ Function, Initialize\ Parameters)$

end
If optimized server feature not lies in range of real properties list
Affected Path = Current server (i, j)
end
end
Return: Optimized Properties and Affected Path
end

A route consists of number of servers and to find the affected server among them, the ANN is again applied on previously found affected path. Here, the energy consumption of each server is taken as input for finding the affected server in previously found affected path. Again, sigmoid function and Levenberg Marquardt technique has been used for classification. The ANN algorithm is defined in the following:

Algorithm 2: Pseudocode of ANN to find affected server

Required Input: Optimized Properties as training data (T), affected network Path (G), & ANN Neurons (N)
Obtained Output: Affected Server

Setup the network with fundamental parameters
– Number of Epochs /iteration (E) // *Iterations used by ANN*
– Total ANN Neurons (N)
– Training constraints MSE
–Algorithm used: Levenberg Marquardt
– Training Data Division: non linear
for range of T do
if T ∈ 1st group of server features then
G (1) = Features of training data for the server // *genuine server*
else
G (2) = Auxiliary Features of training data // *affected server*
end
end
Call ANN using Training data (T) and Group (G)
ANN-Network = Newff (T, G, N)
If ANN-Network required tuning for training of system then set
Net = Train (Net, Training data, Group)
In Classification Phase:
Test server feature = Optimized feature of current server
Affected Server = simulate (Net, Test server feature)
Return: // Affected Server
end

IV. RESULTS AND DISCUSSION

The proposed reactive technique named as GANN technique is conducted in MATLAB tool. This section describes the test results and comparative analysis which are evaluated on the basis of evaluation metrics.

Test Results

To determine the efficiency of the proposed work three parameters namely PDR (packet delivery ratio), throughput and economy consumption are measured in the presence of EDoS attack and after applying the proposed GANN technique. Table 2 represents the considered parameters and values of these parameters before and after applying the proposed GANN technique to the modeled cloud network. From Table 2, the efficiency of the cloud network improves by applying proposed GANN technique.

Table 2: Parameters To Determine Efficiency Of Proposed GANN Technique

Parameters	With EDoS attack	After Prevention of EDoS attack
PDR (%)	19.35	40.9
Throughput	62.2	91.3
Economy consumption (Rs)	1670	1513

i. *Analysis based on PDR:* Fig. 4 represents the packet delivery ratio (PDR) measured in the presence of EDoS attack and when an prevention algorithm GANN have been applied. The vertical line represent the PDR values for 10 numbers of iterations after prevention algorithm and with EDoS attack in cloud server

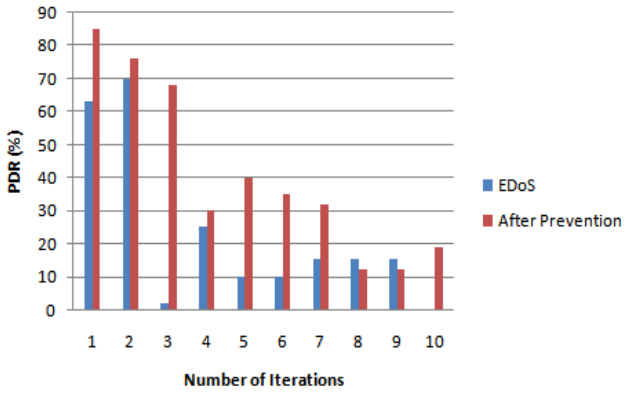

Fig. 4: PDR after applying proposed GANN technique

From Fig. 4 it is clear that when EDoS appear in the cloud server, the performance of cloud decreases compared to the PDR values obtained after applying the prevention mechanism. The values of PDR are listed in Table 3 .The average value of PDR obtained in the presence of EDoS attack and after preventing the cloud server from EDoS attack are 0.1935 and 0.409 respectively. Thus the PDR of cloud server using GANN has been increased by 0.2155, which has index of 52.6%.

Table 3: PDR after applying proposed GANN technique

Number of iterations	PDR with EDoS attack	PDR after Prevention of EDoS attack
1	0.63	0.85

2	0.7	0.76
3	0.02	0.68
4	0.25	0.3
5	0.01	0.4
6	0.01	0.35
7	0.015	0.32
8	0.15	0.12
9	0.15	0.12
10	0	0.19

ii. *Analysis based on throughput:* Fig. 5 depicts the values of throughput measured with EDoS attack and after preventing the cloud server from EDoS attack. From Fig. 5, it is clear that when prevention algorithm (GANN) are applied in the network, the throughput or the capacity of the destination server to accept the packet within the defined interval has been increased by 29.1 compared to the presence of EDoS attack.

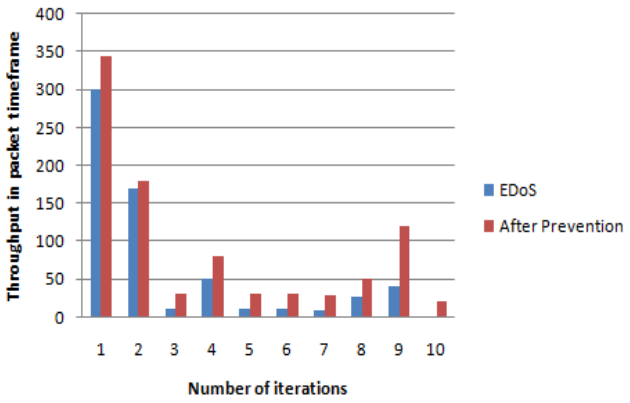

Fig. 5: Throughput after applying proposed GANN technique

The values of throughput are listed in Table 4. The average value of throughput obtained for the proposed work with EDoS attack and with GANN technique are 62.2 and 91.3 respectively.

Table 4: Throughput After Applying Proposed GANN Technique

Number of iterations	Throughput with EDoS attack	Throughput after Prevention of EDoS attack
1	300	345
2	170	180
3	10	30
4	50	80
5	10	30
6	9	30
7	8	28
8	25	50
9	40	120
10	0	20

iii. *Analysis based on economy consumption:* Fig. 6 represents the economy consumption or the bill provided to the cloud server users on the basis of usage of server. From Fig. 6, the billing cost has been reduced by utilizing prevention mechanism. The values of economy consumption are listed in Table 5. The average cost measured in the presence of EDoS attack and when the attack has been removed are Rs 1670 and Rs 1513 respectively. Thus it is clear that the billing cost has been reduced by 157 Rs while utilizing the prevention algorithm.

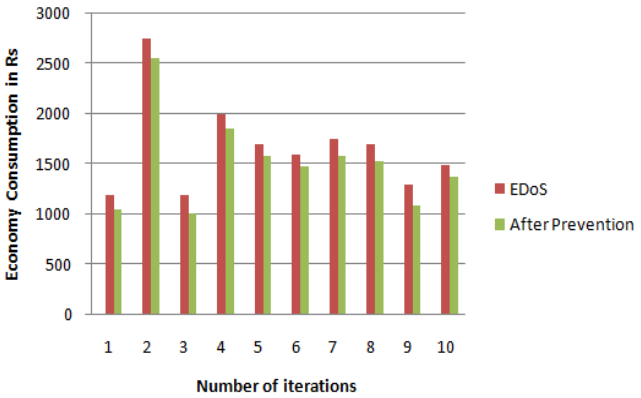

Fig. 6: Economy consumption (Rs) after applying proposed GANN technique

Thus it is clear that the billing cost has been reduced by 1.38% while utilizing the prevention algorithm.

Table 5: Economy Consumption (Rs) After Applying Proposed GANN Technique

Number of iterations	Economy consumption with EDoS attack	Economy consumption after Prevention of EDoS attack
1	1200	1050
2	2750	2560
3	1200	1010
4	2000	1860
5	1700	1590
6	1600	1480
7	1750	1580
8	1700	1530
9	1300	1090
10	1500	1380

Methods used for comparison

This section describes comparison of the performance of the proposed GANN technique with existing Fuzzy Entropy and Lion Neural Learner (FLNL) technique. In the existing work, Lion Neural Learner has been used along with the concept of fuzzy entropy. For classification purpose Lion Neural Learner has been used. The parameters such as precision, recall and F-measure have been measured. The comparison is performed to determine the accuracy or the betterment of the designed network compared to FLNL technique.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

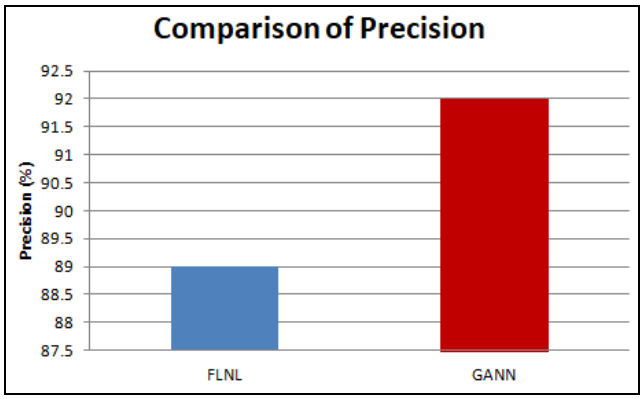

Fig. 7: Comparison of Precision

i. *Analysis based on precision:* Fig. 7 represents the comparison of average precision values measured for the proposed and existing work. Here FLNL has integrated fuzzy entropy with Lion Neural Learner to prevent the server from the EDoS attacker. In our work, genetic algorithm with neural network has been used to prevent the network from the EDoS attacker. From Fig. 7 GA with NN perform better compared to existing FLNL algorithm.

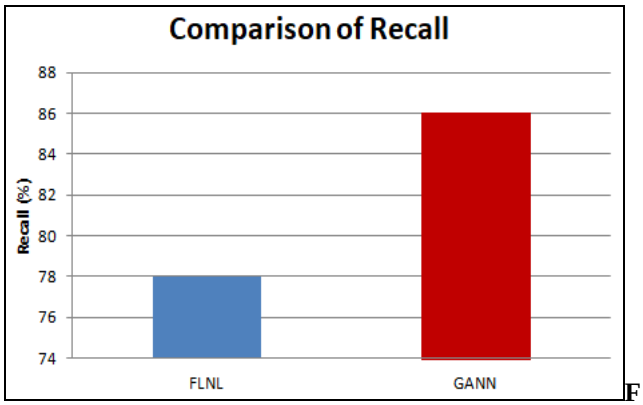

Fig. 8: Comparison of Recall

ii. *Analysis based on recall:* Fig. 8 depicts the comparison of recall parameter measured for proposed GANN technique and existing work. Fig. 8 shows that the when GA with NN is used in the proposed cloud environment the recall has been increased by 10.26%.

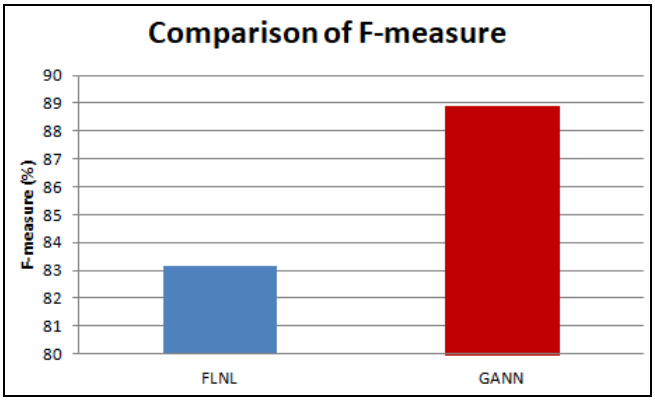

Fig. 9: Comparison of F-measure

iii. *Analysis based on F-measure:* Fig. 9 shows the comparison of F-measure which is computed while designing a prevention system to protect the cloud server from EDoS attack. F-measure defines the harmonic means of precision as well as recall. F-measure obtained for the proposed GANN technique is higher than the existing work.

Discussion

The experimental results comparison of proposed GANN technique with existing FLNL technique has been discussed for different parameters such as Precision, Recall and F-measure. The comparison values are listed in the Table 6.

Table 6: Comparison of Proposed Work with Existing Work

FLNL Technique			GANN Technique		
Precision (%)	Recall (%)	F-measure (%)	Precision (%)	Recall (%)	F-measure (%)
89	78	83.13	92	86	88.89

The values of precision, recall and F-measure observed for the proposed work as compared to the existing work are increased by 3.37%, 10.26%, 6.93% respectively which proves that the proposed approach performs better than the existing FLNL technique.

V. CONCLUSIONS

Cloud Computing serves a wide range of services to their users. Different security techniques are present for prevention of EDoS attack but these methods have not provided remarkable security. Therefore, we proposed a new cloud security model named as GANN to protect the server from EDoS attack. Three algorithms are used in a hierarchy. Firstly, ANN is applied to determine the number of suspected transaction path in cloud network. Secondly, to determine the number of affected route an objective function of GA has been designed. At last, ANN is again trained and tested on the basis of the affected number of transaction paths and hence discovered the affected service provider. The evaluation metrics such as PDR, throughput and energy efficiency are considered. From the test analysis, it has been observed that the performance of cloud server has been increased when GANN has been implemented in the network.

The throughput of the network has been increased by 29.1% while using prevention algorithm. To evaluate the level of performance of proposed GANN algorithm as compared to existing FLNL algorithm the parameters such as precision, recall and F-measure are utilized which is increased by 3.37%, 10.26% and 6.93% respectively and proved that the proposed GANN technique is better than the existing FLNL technique.

REFERENCES

1. Q. Zhang, L. Cheng and R. Boutaba. Cloud computing: state-of-the-art and research challenges, Journal of internet services and applications, vol.1, pp.7-18, 2010.
2. S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing, Journal of network and computer applications, vol. 34, issue 1, pp. 1-11, 2011.
3. K. Bhushan and B. B. Gupta(2018). Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment, Journal of Ambient Intelligence and Humanized Computing, vol. 10, issue 5, pp. 1985-1997, May 2019.
4. A. Shawahna, M. Abu-Amara, A. Mahmoud, and Y. E. Osais. EDoS-ADS: An Enhanced Mitigation Technique Against Economic Denial of Sustainability (EDoS) Attacks, IEEE Trans. on Cloud Computing, 2018

5. S. Bulla, B. B. Rao, K. G. Rao, and K. Chandan. An experimental evaluation of the impact of the EDoS attacks against cloud computing services using AWS, International Journal of Engineering & Technology, vol. 7, pp. 202-208, 2018.
6. P. Daffu and A. Kaur. Energy Aware Supervised Pattern Attack Recognition Technique for Mitigation of EDoS Attacks in Cloud Platform, International Journal of Wireless and Microwave Technologies, vol. 1, pp. 42-49, 2018
7. Q. Yan and F. R. Yu. Distributed denial of service attacks in software-defined networking with cloud computing, IEEE Communications Magazine, vol.53, no.4, pp. 52-59, 2015.
8. O. Osanaiye, K. K. R. Choo and M. Dlodlo. Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. International Journal of Network and Computer Applications, vol.67, pp. 147-165, 2016.
9. M. Ficco and M. Rak. Economic denial of sustainability mitigation in cloud computing. in Organizational Innovation and Change Springer-Cham, pp. 229-238, 2016.
10. F. Z. Chowdhury, L. B. M. Kiah, and M. M. Ahsan. Economic denial of sustainability (EDoS) mitigation approaches in cloud: Analysis and open challenges. In Proc. 2017 IEEE Conf. Electrical Engineering and Computer Science (ICECOS), August 2017, pp. 206-211.
11. A. S. Bhingarkar and B. D. Shah. A survey: Securing cloud infrastructure against EDoS attack. in Proc. International Conference on Grid Computing and Applications (GCA), p. 16, January 2015.
12. B. Waters, A. Juels, J. A. Halderman and E. W. Felten. New client puzzle outsourcing techniques for DoS resistance, in Proc. 11th ACM conference on Computer and communications security, pp. 246-256, October 2004.
13. M. H. Sqalli, F. Al-Haidari and K. Salah. EDoS-shield-a two-steps mitigation technique against edos attacks in cloud computing, in Proc. 2011 IEEE 4th International Conference on Utility and Cloud Computing (UCC), 2011, pp. 49-56.
14. F. Al-Haidari, M. Sqalli and K. Salah. Evaluation of the impact of EDoS attacks against cloud computing services, Arabian Journal for Science and Engineering, vol.40, no.3, pp. 773-785, 2015.
15. F. Z. Chowdhury, M. Y. Idris, M. L. M. Kiah, and M. M. Ahsan. EDoS eye: A game theoretic approach to mitigate economic denial of sustainability attack in cloud computing. in Control and System Graduate Research Colloquium (ICSGRC), 2017 IEEE 8th (pp. 164-169). IEEE.
16. W.Shruti, K. C. Rama, S. Poonam. Prevention of EDoS attack using hybrid filtering technique (EDoS Guard). I J C T A. 9(40).519-526, 2016.
17. S. Bhingarkar and D. Shah. FLNL: Fuzzy entropy and lion neural learner for EDoS attack mitigation in cloud computing. International Journal of Modeling, Simulation, and Scientific Computing, vol. 9, no. 6, 2018.
18. K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan. A fast and elitist Multiobjective genetic algorithm: NSGA-II. IEEE transactions on evolutionary computation, vol.6, no.2, pp.182-197, 2002.
19. S. Dreiseitl and L. Ohno-Machado (2002). Logistic regression and artificial neural network classification models: a methodology review, Journal of biomedical informatics, vol.35 (5-6), pp. 352-359, 2002.

AUTHORS PROFILE

Ms. Swati Nautiyal received her B.E. Degree in Computer Science and Engineering from Sant Longowal Institute of Engineering and Technology (SLIET), Punjab, India in 2015. She is pursuing her Master of Engineering in Computer Science and Engineering from National Institute of Technical Teachers' Training & Research (NITTTR), Chandigarh under Panjab University, Chandigarh, India. Her areas of research interest include Computer Networks and Cloud Computing.

Dr. Rama Krishna received B.Tech. from JNTU, Hyderabad, M.Tech. from Cochin University of Science & Technology, Cochin, and Ph.D from IIT, Kharagpur. He is Senior Member, IEEE, USA. Since 1996, he is working with Department of Computer Science & Engineering, National Institute of Technical Teachers' Training & Research (NITTTR), as Professor. His areas of research interest include Computer Networks, Wireless Networks, Cryptography & Cyber Security, and Cloud Computing. To his credit, he has more than 80 research publications in referred International and National Journals and Conferences. He is a member in Advisory/Technical committees of many national and international journals and conferences and also chaired many technical sessions. He is reviewer of various journals of IEEE, ACM, Elsevier and Springer. He has more than 22 years of experience in organizing more than 100 training programmes in the upcoming areas of CSE and IT for the faculty of engineering colleges, polytechnics and industry professionals. He is instrumental in launching various initiatives at NITTTR Chandigarh towards paperless office under 'GO GREEN' initiative.

Ms. Shruti Wadhwa, received her B.Tech. from PTU, M.Tech. from National Institute of Technical Teachers' Training & Research (NITTTR), Chandigarh. She is working with Department of Computer Applications, Post Graduate Government College, Chandigarh. Her areas of research interest include Computer Networks, Web Security, Cyber Security, and Cloud Computing, Virtualization & Artificial Intelligence. To her credit, she has more than 5 research publications in referred International and National Journals and Conferences. She also delivered expert lectures on Campus Wide Network Security & Implementation of IPv6 at College of Engineering & Management, Kolaghat and on Malware & Network Attack Analysis using Packet Sniffing, Mitigation of Network and DoS attack & on various routing protocols in National Institute of Technical Teachers' Training & Research (NITTTR), Chandigarh. She has more than 3 years of experience in teaching and organizing various training programmes in the areas of CSE and IT for the faculty of engineering colleges, polytechnics and students.