International Journal of Engineering Sciences & Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

RESEARCHERID
THOMSON REUTERS

[Kumari *et al.*, 10(1): January, 2021]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

OPTIMIZED NEURAL NETWORK USING CUCKOO SEARCH BASED INTRUSION DETECTION AND PREVENTION SYSTEM IN CLOUD COMPUTING ENVIRONMENT

Kajal Kumari[*1] & Poonam Choudhary[2]

[*1&2]Sirda institute of Engineering and Technology, Mandi (H.P) HPTU, Himachal Pradesh

DOI: Will get Assigned by IJESRT Team

ABSTRACT

Nowadays, Cloud Computing is the preferred choice of IT organizations as it provides dynamic and pay-per-use based services to its clients. The main problem of the cloud computing is security and privacy of data which occurs because of its open and distributed structural design. Thus, it becomes essential to design an intrusion detection system (IDS) to provide security to the system. IDS help to protect cloud ecosystem from the malicious activities of the attacker. In this research work, IDS is designed to detect malicious node by using an optimization technique along with the concept of AI (Artificial Intelligence).The Cuckoo Search (CS) algorithm is used as an optimization technique and it is a meta-heuristic approach which is inspired by the behavior of birds and CS algorithm operates on the healthiness function. After the feature optimization, different types of feature are categorized based on the node's nature into two types namely normal and attackers. On the basis of extracted features, train the proposed system using ANN (artificial neural network) as classifier to classify the attackers which affect the networks in cloud environment. ANN is a multiclass classifier which is used to solve multi-class problems and due to this reason ANN is used in proposed work with CS optimization algorithm. In this research work, ANN is used to distinguish between attacker nodes and genuine nodes based on their optimized feature sets. Thus, instead of passing data to the attacker node, the node passes the data to the genuine node and hence, the system is protected. By using the above motioned concept in cloud computing the possibility of results improvement become high because only genuine node involving in the data transmission process. To know the performance of the system, the QoS (Quality of service) parameters such as PDR (Packet delivery ratio), energy consumption rate and total delay with and without prevention algorithm are measured. The development of proposed ARS is done in the MATLAB 2016a software with the help of various toolboxes like data acquisition, artificial intelligence, optimization and curve fitting.

Keywords: IDS (Intrusion Detection System), CS (Cuckoo Search) algorithm, ANN (Artificial Neural Network), QoS (Quality of service) and Cloud Computing.

1. INTRODUCTION

Cloud computing is a novel business model in the world of computing [1]. As per the National Institute of Standards and Technology "Cloud computing is defined as the model enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [2]. A cloud computing environment is depicted in Figure 1. Cloud computing is used to provide different services such as databases, servers, software, networking, storage etc. through Internet. These services are provided by cloud service provider and the user has to pay as per usage [3].

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

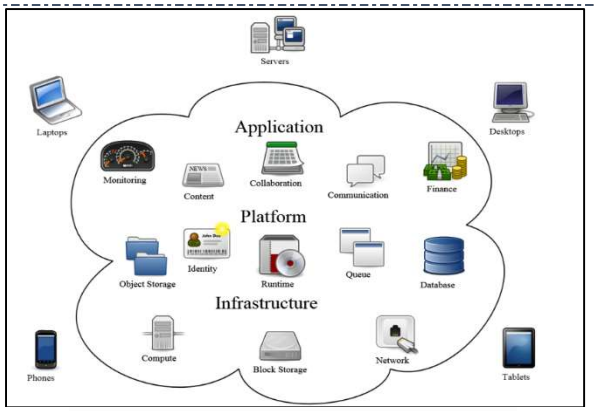

Figure 1: Cloud Computing Environment [4]

Cloud Computing Services are available in three flavors:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

They are sometimes referred to as cloud computing stacks because they are built on top of each other.

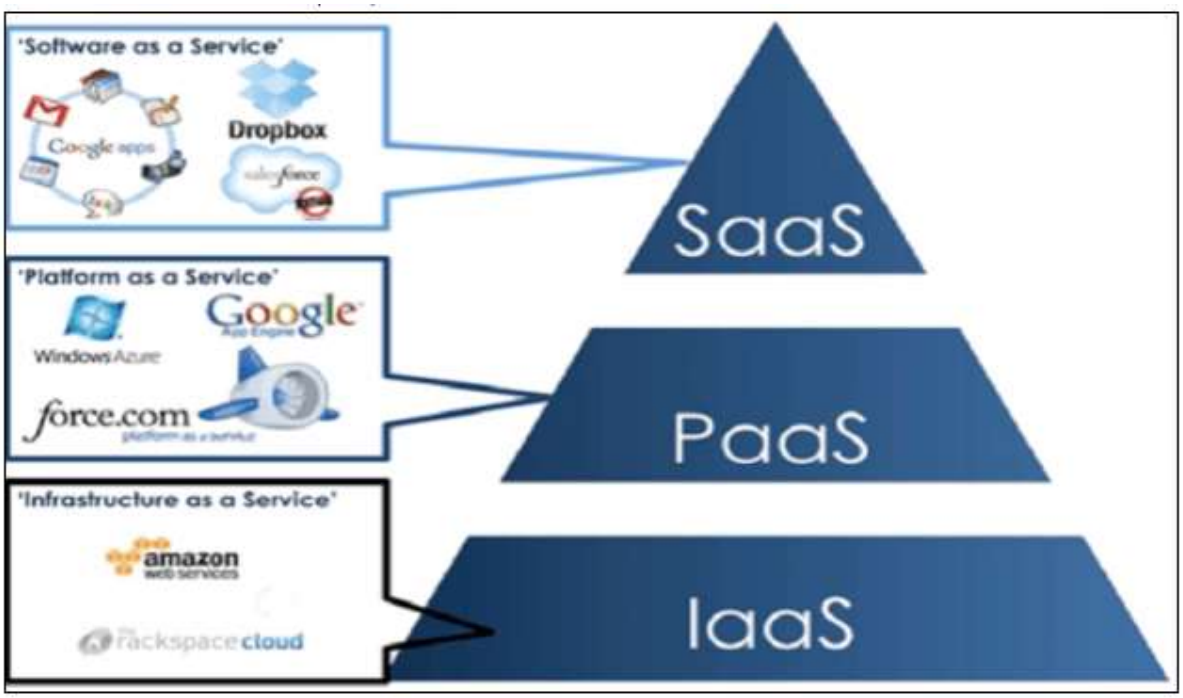

Figure 2: Cloud Computing Services [5]

Figure 2 represents the three main services along with the functions performed by these services. IaaS is used to provide virtualized infrastructure as per requirement, PaaS is used to create and deploy application for end users and SaaS is used to provide services such as email, MS office etc. that can be accessed anywhere. IAAS, PAAS and SAAS are used to provide infrastructure, platform and services to the cloud users respectively [6].

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IaaS: It is used to provide cloud infrastructure, for instance servers, networks, operating systems and storage. Customers can access the service as a pay-per-use model instead of purchasing servers, software and network devices. Rackspace and Go-daddy are example of IaaS [7].

PaaS: PaaS services are used to present software tools as well as hardware that are mainly used by the application designer over the network. The software and hardware are hosted upon the infrastructure which is provided by the cloud vendor [8].

SaaS: SaaS provides subscription-based service and there is no need of any licensing. Each user's software is compatible with others because all have the same version of software. Sometimes it is called 'on-demand software' and has previously been called 'software services' by Microsoft. A large number of SaaS applications can be run with the help of internet browser without any setup or download requirements and in some exceptional cases add-ins are used. SaaS removes the need to install and run applications on standalone PCs due to the web delivery model composition [9].

There are mainly four general deployment models present in cloud environment namely; Private, Public, Hybrid and Community Cloud. But, cloud network faces some issues and security challenges. As cloud computing utilizes several techniques/technologies like databases, networking, load balancing and virtualization etc., security challenges related to these technologies and mechanisms are also relevant for cloud computing.

- Data Availability
- Data Integrity
- Data confidentiality
- Data privacy
- Data leakage
- Malicious attacks
- Account Hijacking

In the last couple of years, the network revolution has ultimately come into existence. The capabilities and convenience are immense; unluckily, the threats and capabilities of malicious attacks are equal. Even though, the IDS (Intrusion Detection Systems) are thoroughly different in the methods and employ to collect and analyze the data, most of them rely on a comparatively universal architectural framework that comprises of the following components:
Sensors: Sensors are used to collect information through the source.
Knowledge Base: Pre-process the collected information such as signature, filtered data, profile etc. and store into the database.
Detector: It is used to process the data taken from the sensor devices which is used to identify the malicious activities.
Configuration: It is used to provide the information about the IDS state.
Response Component: This device is used when intrusion is identified in the system. It may be provided in the form of alarm or human action.

Basically, the working of IDS is based on the wireless network mechanism. So, the main motivation behind the improvement in the IDS mechanism for cloud environment is to provide a better secure along with the failure detection capacity by utilizing the ANN as a classifier in the network where Cuckoo Search Algorithm (CS) is used to optimize the ANN and the major contributions are listed as:

- We presents a brief analysis of the existing IDS for cloud environment.
- We perform route discovery process and optimize route using CS algorithm.
- We also apply classification algorithm over the optimized data based on artificial neural network.
- To validate the performance by comparing proposed technique with existing techniques in terms of energy consumption, delay and PDR (Packet Delivery Rate).

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

In this section, we provide a brief introduction about the proposed IDS mechanism and the main focus of research is to introduce a hybrid routing mechanism with intrusions such as Black hole or Distribute Denial of Service (DDoS) and the rest of paper is organized as: in Section 2 existing work related to the IDS are analyzed where, the material and methods are discussed in Section 3 with experimental set up of IDS scenario. In the Section 4, simulation results are discussed and the conclusion with the future possibilities is discussed in the Section 5.

2. RELATED WORK

Lots of hybrid routing mechanism proposed by the researchers in the previous ten years in the area of IDS, so, to find out the existing problems to designed a secure routing for IDS by focusing on the routing failures issues. ***Mishra et al. [5]*** have proposed an intrusion detection scheme based on machine learning approach to provide security in the cloud environment. Authors have mainly concentrated on two issues; detection of attack and speed of detection. Naive Bayes and neural network have been used for detecting intrusion in the network. Different attacks such as DoS, probe, U2R and R2 L have been considered and the detection rate for all these attacks have been determined. For DoS attack the detection rate is high i.e. approximately 99.90% whereas for U2L attack the detection rate is small i.e. approximately 80.02%. ***Deshpande et al. [6]*** have presented a Host-based intrusion detection model for cloud computing environment. The main drawback of this model is that the intrusion detection rate is low as no classification algorithm has been used. ***Aishwarya et al. [7]*** have proposed a TCP (transmission control protocol) to secure the devices from Distributed DoS attack. This can be done through SYN (Synchronization) cookie, only positive ACK (Acknowledgment) received user allows to enter in network. In first layer, filtering technique is used and the server distinguishes the real and spoofed users by some set of rules. In second layer SYN packet is used out of which only genuine packets are allowed. Also, MAC (message authentication code) is used for authentication of client. In cloud computing, the computation time has been reduced by using filtering mechanism. ***Haidar et al. [8]*** have proposed IDS with the help of ANN, which provides network security. Under this, ANN architecture is used which helped in improving intrusion detection rate of the system. The assessment was carried out for multiple network attacks, like DDoS, from remote to user, from user to root and probing attacks. ***Nie et al. [9]*** have proposed the detection system for an efficient anomaly as well as the network traffic measurement system, using the Bayesian network structure, the relationship between network traffic occurrences was determined. The subsequent strategy was used to produce probability distribution of network traffic. GEANT network were used to gather data and the observational evaluation was carried out to evaluate the effectiveness of the proposed framework, which is about 89% approximately. ***Seth et al. [10]*** have presented an integrated approach used by IDS model using key feature selection process that has been modified by using gray wolf optimization and K-NN classification algorithm. The optimization algorithm helps to decrease the features from the dataset and hence reduce the computing space with resources. The performance on the basis of features selection has been measured and it is found that the proposed model performed well. ***Moustafa et al. [11]*** have presented Collaborative anomaly detection framework to find cyber-attacks in cloud environment with the drawback that it can only be worked for homogeneous systems. ***Priyanka et al. [12]*** have presented a secure cloud network by using the concept of ANN and SVM approach. The research has mainly focused on detecting BHA (Black Hole Attack) in cloud. The authors have used AODV as a route discovery mechanism, which has been optimized using firefly algorithm. Firefly algorithm has used to identify multiple best possible routes. The ANN has been used to select the best routes among those multiple routes. ANN takes decision on the basis of node's energy consumption, collision rate and distance. The performance has been analyzed on the basis of throughput, end to end delay, and PDR (Packet Delivery Ratio).

From the above work performed by various researchers, it has been observed that the IDS for the cloud still needs improvement. With technology, the intruders have found smart ways to hide and to make maximum harm to the system at the same time. There is a need of adaptive IDS and this need gives birth to the problem statement of this research work

3. MATERIAL & METHOD

In this section, we explain the used methodology and algorithms that is to design an optimized neural network using cuckoo search based intrusion detection and prevention system in cloud computing environment and the model is shown in the Figure. 3

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

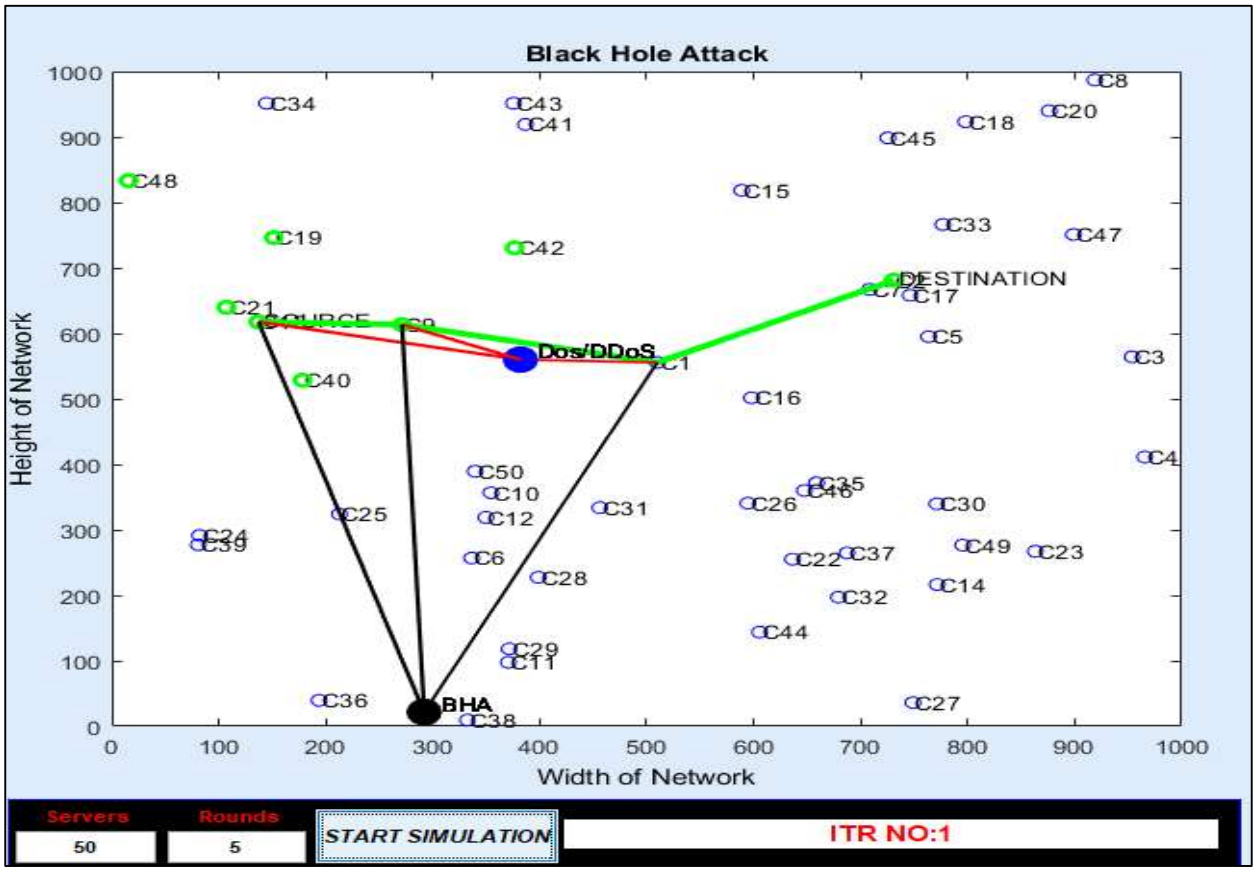

Figure 3: Proposed IDS

In this research, an IDS for cloud environment has been presented based on Cuckoo search and ANN approach. Various attacks such as DoS/DDoS, Black hole and Gray whole attacks have been identified. Initially, the route between the source server and the destination server is optimized using CS algorithm on the basis of fitness function. Fitness function is defined as followed to find out the appropriate servers for communication.

$$Fitness = \begin{cases} F_s\ (True)\ if\ F_s \geq F_t \\ F_t (\text{False})\ otherwise \end{cases}$$

Affiliation: CS is used to identify the best route between the source and the destination server. CS is meta-heuristic technique developed by Xin-She Yang and Deb in the year of 2009 that is used to solve the complex problems. It is stimulated by natural behavior of cuckoos, specifically, the obligatory breeding parasitism of some species of cuckoo by placing their eggs in the nests of other host birds for increase their probability. For defining CS algorithm three set of rules are used that are listed below:

- Every cuckoo can lay an egg at the same time step and transfers it into an individually selected nest.
- The higher quality of eggs will be transferred to produce further generations,

The total number of host nest is stable, and the likelihood of an egg laid by a bird can be detected through host bird (0, 1). Here, host can either remove those eggs or leave the nest and can create a totally new hive [13]. CS is meta- heuristic technique which is used to identify the best route between the source and the destination server.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

The algorithm of the proposed work is written as:

Algorithm: CS

Input: Properties of server which are consider in route
Output: Best servers

1. Produce initial cuckoo population for n number of servers
2. Compute average energy consumption (Avg EC) of all servers
3. For each Server s, if $EC_s \geq$ Avg EC, EC_s = Avg EC
4. **While (t < ITR)//** t: number of counts
5. Select a cuckoo randomly
6. Evaluate fitness of the selected cuckoo on the basis of energy consumption
7. Find best solution (*Bsol)* based on fitness function (If two cuckoos have same fitness then consider *Bsol* on the basis of delay and PDR)
8. **End (While)**
9. **Return:** *BSol*
10. **End (CS)**

Step 1 is used for the generation of population according to the number of servers. Compute the average energy consumption of all servers in step 2. In step 3, for each server if energy consumption is greater than or equal to average energy consumption then energy consumption of server becomes average energy consumption. Steps 4-8 are repeated for finding the best solution according to the fitness function.

ANN: ANN is a data processing algorithm inspired by neurons that are the essential elements of the human brain [14]. The architecture mainly consists of processing elements denoted by servers. In the ANN architecture, several processing units are joined with each other and hence resolve the particular problem. In this work, ANN is used to classify the normal and intrusion servers on the basis of the properties of servers that had been analyzed by using the CS algorithm.

Input: Best servers
Output: Selected attacker server

1. **Initialize ANN on the basis of:**
   - Epochs (E)
   - Neurons (N)
   - Number of hidden layers
   - Training data (T)
2. **For each set of T's**
3. Group(G)=Categories of Training data ∈ terms of attacker ∧ genuine node
4. **End**
5. Based on T and G initialize ANN using, Net = Newff (T, G, Neurons)
6. Train the cloud system, Net = Train ()
7. Classify = simulate (Net, Properties of cloud server)
8. **If categorize = True**
9. Normal Server = Simulated cloud Server
10. **Else**
11. Attacker/Affected Server = Simulated cloud Server
12. **End**
13. **Return:** Attacker Servers
14. **End**

To train the designed IDS model, above written ANN algorithm is used where we consider the optimized server properties as an input data. In step 1, we call the ANN in MATLAB using the initialization steps with epochs (iterations), number of neurons, number of layers and training data. After that in step 2 to 4, we divide the total training data based on the group (G) and then in step 5, initiate the ANN with the simulator using the "newff" command with the help of the training data (optimized server properties) and types of server (normal or affected

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

= Group (G)). In the step 6, we train the model using "train" function and after that in step 7, we classify the servers using trained structure (Net) and in step 8 to 12, we check the server's nature to find out the normal or affected/Attacker server in the network. At the last step 13, ANN algorithm returns the server with their properties.

4. RESULTS AND DISCUSSION

MATLAB is used to simulate the proposed work and experiment is conducting using UNSW- NB-15 dataset. The performance of the proposed work has been validated on the basis of delay, PDR and energy consumption for three different types of attacks (i) DoS/DDoS Attack (ii) BHA and (iii) GHA

DoS/DDoS Attack: Users are unable to access the information and facilities during DoS attack. DDoS is an advanced version of DoS. Targeted server is disrupted due to flooding of large number of spam messages by many computers and intended users are unable to use the network resources.

Black Hole Attack (BHA): In this attack, the attacker or malicious node advertise all other nodes by claiming itself an optimum route for all other nodes to pass data packets through itself. Later on, the packets received by attacker-node are dropped; instead of normally forwarding those packets.

Gray Hole Attack (BHA): This attack is a sophisticated type of black hole attack in which the source or destination of packets depends on a malicious node dropping only chosen packets and forwarding the others. Another type of gray hole can be malicious for a certain period by dropping all packets and later switching to usual behavior. Trust-based mechanisms are defeated by this attack making the detection of malicious node more difficult to achieve.

TABLE I: Computed Parameters Before and After Prevention of DoS /DDoS Attack

Number of Iterations	Delay (ms)		PDR		Energy Consumption(mJ)×106	
	Before Prevention	After Prevention	Before Prevention	After Prevention	efore Prevention	ter Prevention
1	45	42	0.91	0.98	0.94	0.92
2	46	45	0.90	0.97	0.96	0.91
3	40	38	0.89	0.99	0.84	0.83
4	51	49	0.88	0.96	1.1	1.08
5	35	32	0.87	0.95	1.21	1.18
6	40	38	0.85	0.98	1.35	1.31
7	44	41	0.82	0.97	1.47	1.41
8	39	37	0.80	0.96	1.59	1.48
9	41	38	0.75	0.98	1.65	1.55
10	35	31	0.72	0.99	1.82	1.61

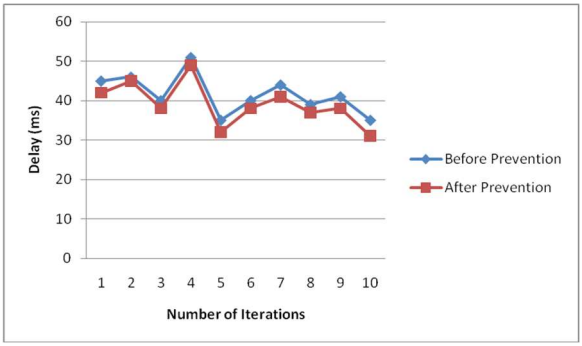

Figure 4: Delay (MS) before and after prevention of Dos/DDoS Attack

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

The performance of the cloud network after simulation of designed network before and after prevention from DoS / DDoS Attack is shown in Figure 4. Ten different iterations are used with different number of nodes. Ten different iterations are used with different number of nodes. Each iteration consists of 50 numbers of servers through which the data transfer has been considered and the network is run 10 times as indicated by the number of iterations. For each iteration, the results are executed and noted. Delay of designed network is reduced by using the concept of DDoS prevention mechanisms as compared with presence of attacker.

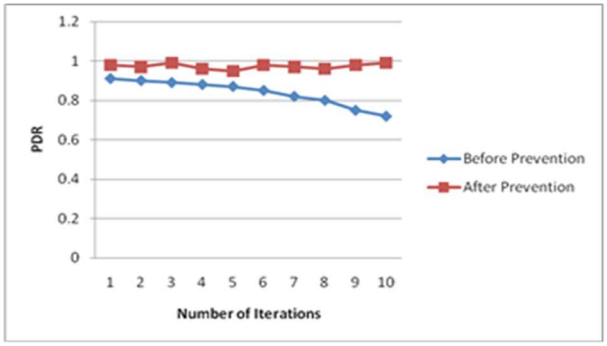

Figure 5 PDR before and after prevention of Dos/DDoS Attack

The PDR of the proposed work is depicted in Figure 5 before and after prevention the minimum and maximum value of PDR obtained are 0.72 to 0.91 and 0.95 to 0.99 respectively.

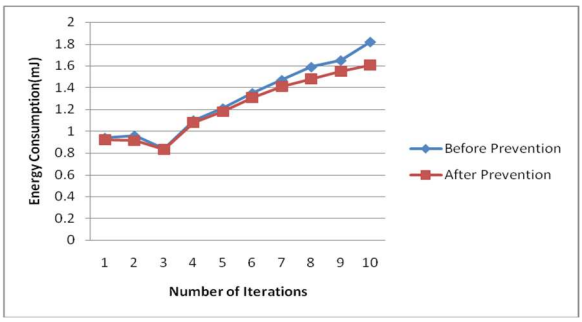

Figure 6 Energy Consumption before and after prevention of Dos/DDoS Attack

TABLE II Computed Parameters Before and After Prevention of Black Hole Attack

Number of Iterations	Delay (ms)		PDR		nergy Consumption(mJ)×106	
	Before Prevention	After Prevention	Before Prevention	After Prevention	Before Prevention	After Prevention
1	44	40	0.94	0.99	0.98	0.89
2	45	44	0.92	0.98	0.96	0.87
3	38	37	0.90	0.97	0.82	0.82
4	48	45	0.89	0.98	1.14	0.97
5	32	30	0.88	0.99	1.25	1.06
6	39	36	0.87	0.98	1.41	1.01
7	40	40	0.89	0.97	1.51	0.98
8	38	36	0.87	0.98	1.59	1.28
9	40	37	0.82	0.99	1.62	1.32
10	34	29	0.79	0.97	1.84	1.49

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

In Figure 7, delay of designed network is reduced by using the concept of BHA prevention mechanisms as compared with presence of attackers. The minimum and maximum values of delay before prevention and after prevention obtained are 32 to 48ms and 29 to 45ms respectively.

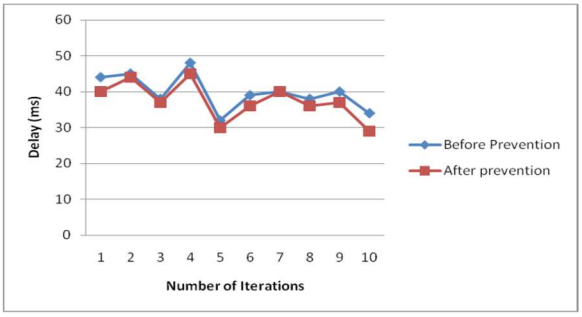

Figure 7 Delay (ms) before and after prevention of BHA Attack

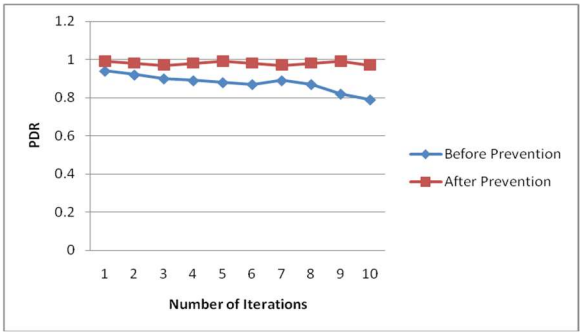

Figure 8 PDR before and after prevention of BHA Attack

From Figure 8, it is clear that the PDR after prevention from BHA is higher than that of PDR obtained before prevention from BHA. The minimum and maximum values of PDR obtained before and after prevention are 0.79 to 0.94 and 0.97 to 0.99 respectively.

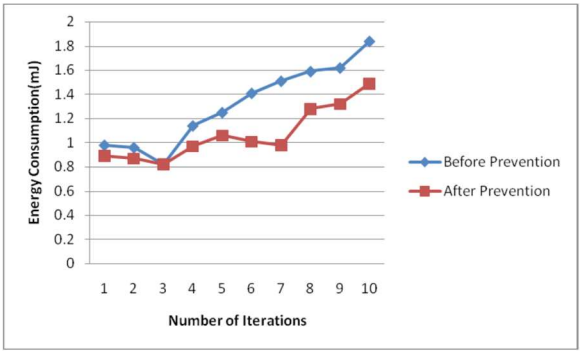

Figure 9 Energy Consumption before and after prevention of BHA Attack

From Figure 9, it is clear that the energy consumed by the cloud server increases due to the increment in iterations. The minimum and maximum value analyzed before and after prevention of BHA are 0.82 to 1.84×106mJ and 0.82 to 1.49×106mJ respectively.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

TABLE III Computed parameters before and after prevention of Gray hole attack

Number of Iterations	Delay (ms)		PDR		Energy Consumption(mJ)× 10 6	
	Before Prevention	After Prevention	Before Prevention	After Prevention	Before Prevention	After Prevention
1	41	38	0.92	1.00	0.96	0.75
2	42	35	0.91	0.99	0.95	0.72
3	35	34	0.88	0.98	0.79	0.82
4	42	39	0.89	0.99	1.11	0.85
5	30	29	0.87	0.99	1.18	0.97
6	37	34	0.90	0.98	1.38	0.99
7	36	34	0.91	0.98	1.44	1.07
8	34	33	0.89	0.97	1.49	1.18
9	38	33	0.85	0.99	1.58	1.08
10	32	27	0.87	0.96	1.75	1.62

The result with GHA is depicted in Figure 10. From the figure, it is seen that the delay after prevention of GHA is less compared to the delay measured before prevention of GHA. The minimum and maximum delay produced by the number of cloud servers used during the communication for ten numbers of iterations before and after prevention of GHA are 30 to 42 ms and 27 to 39 ms respectively. Thus, there is a reduction has been obtained while removing GHA from the cloud network.

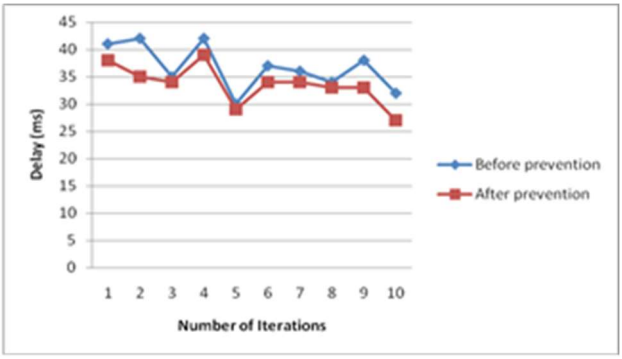

Figure 10 Delay before and after prevention of GHA Attack

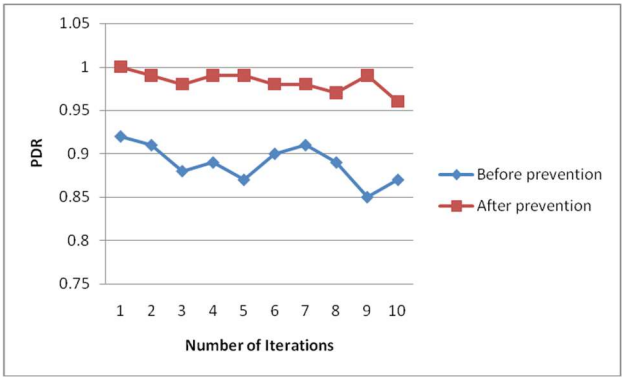

Figure 11 PDR before and after prevention of GHA Attack

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Figure 11 shows, the packet is delivered successfully to the desired server during the communication process before prevention of GHA and after prevention of GHA. So, it is clear that the successful delivery rate of packet after prevention of GHA is higher compared to the packet rate delivered in the presence of GHA. The minimum and maximum values of PDR before and after prevention of GHA are 0.85 to 0.92 and 0.96 to 1.0 respectively.

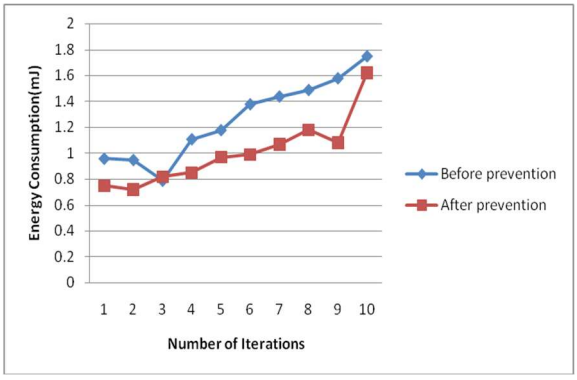

Figure 12 Energy Consumption before and after prevention of GHA Attack

Figure 12 represent the minimum and maximum values of energy consumed by the cloud network before and after prevention of GHA is 0.79 to 1.75× 106mJ and 0.72 to 1.62×106mJ respectively. Thus, the reduction has been obtained while preventing cloud network from GHA.
Comparison of existing Work with proposed work

In [17], a secure cloud network from Black Hole Attack using Firefly with Neural Network approach has been presented. The performance has been examined on the basis of PDR, delay and throughput. The comparison of the existing [17] work with proposed work has been presented in the table 4 and Figure 13 respectively.

TABLE IV Comparison in Term of PDR and Delay

Number of Cloud Servers	Delay (ms)		PDR	
	Proposed Work (ANN with CS)	Existing Work (ANN with Firefly)	Proposed Work (ANN with CS)	Existing Work (ANN with Firefly)
10	42.64	48.66	0.972	0.943
20	40.24	46.52	0.976	0.949
30	38.76	45.91	0.981	0.958
40	37.89	43.26	0.986	0.963
50	34.71	41.74	0.987	0.971
60	32.73	39.76	0.991	0.983

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

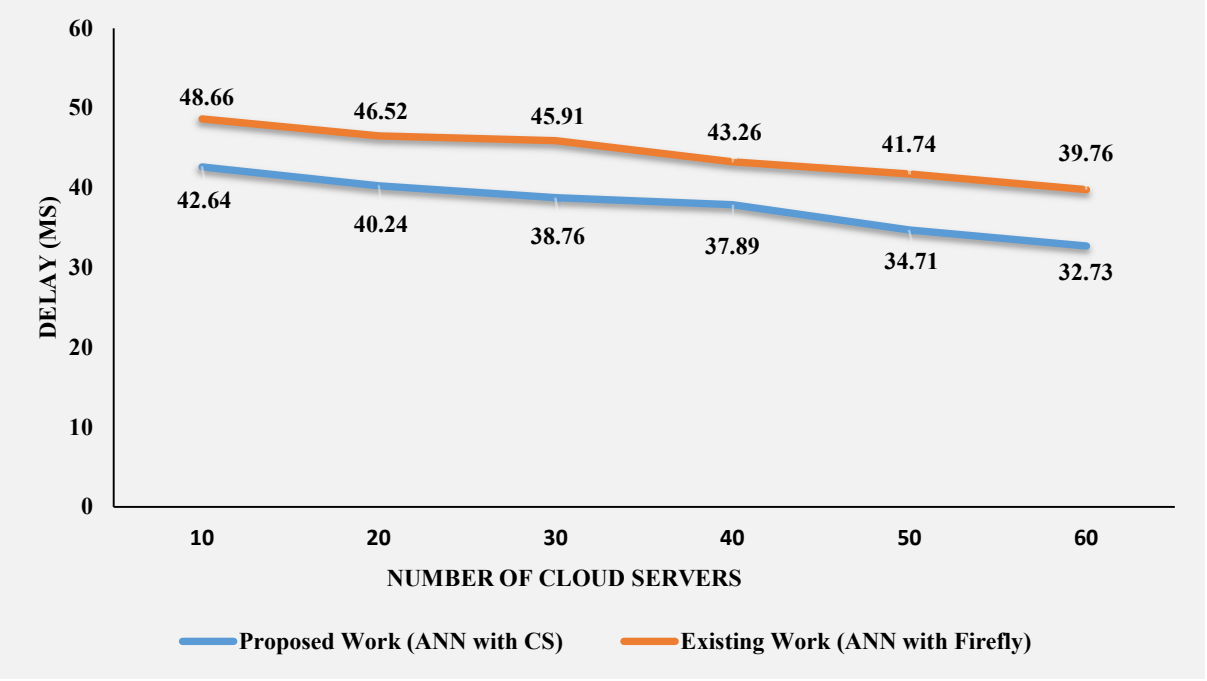

Figure 13: Comparison of PDRs

On the basis of comparative analysis of proposed work with exiting work, we concluded that some disadvantages of the proposed IDS model and they are written as:

Packet delivery rate is up to mark but need more attention the on transmission delay by optimizing the route based on the clustering approaches.

If the transmission delay is more, then also energy consumption rate by servers increases and in this work, we observed this limitation of developed system.

For any communicating model, security is a major factor that can gives a secure platform for users in a secured cloud environment. A secure IDS model secures its clients from lots of attackers or intrusions like DDoS, BHA, GHA and many more types of attackers they are sufficiently dangerous to take all the communicating data in the system. So, proposed mode have some disadvantages but, also the proposed IDS is very useful is lots of manners like:
Applicable to design an anti-spyware and anti-virus applications.
Can used to develop a firewall that helps to protect the network from unauthorized access.
In the design of a Virtual Private Networks (VPN), it is also useful that can give a safe access in cloud.

5. CONCLUSION AND FUTURE WORK

The efficiency of cloud services is diminished by attack. Also, the trust between cloud users and their providers is affected by the attacks which results in loss of data, poor services etc. Therefore, to enhance the service and reduce the loss of packets, a combination of CS with ANN algorithm as new IDS for cloud environment has been presented. The training of ANN has been performed by providing an optimized route, which is obtained after the CS algorithm applied in the cloud network. The optimized route has been identified based upon a designed fitness function. The simulation results have shown that the proposed IDS has performed much better as compared to the existing work and a significant enhancement in delay and PDR has been obtained. During experimental analysis we have considered DoS/DDoS, GHA and BHA attacks and the performance of proposed work has been analyzed on the basis of Delay, PDR and Energy Consumption. By preventing DoS/DDoS, BHA and GHA in the Cloud using proposed technique, up to 11%, 15% and 17 % reduction in delay is observed respectively. There is an

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

improvement of up to 38%, 23 % and 16% in Packet delivery ratio while dealing with DoS/DDoS, BHA and GHA attacks respectively. Using proposed algorithm, up to 12%, 35% and 32% energy consumption has been reduced by preventing DoS/DDoS, BHA and GHA attacks respectively.

REFERENCES

[1] Yamini, B.; Selvi, D.V., "Cloud virtualization: A potential way to reduce global warming," Recent Advances in Space Technology Services and climate Change (RSTSCC) International Conference in Chennai, pp.55-57, 2010.
[2] Seth, Jitendra Kumar, and Satish Chandra. "An Efficient Hybrid Intrusion Detection System in Cloud." 653-666, 2018.
[3] Mehibs, S. M., &Hashim, S. H. "Proposed Network Intrusion Detection System Based on Fuzzy c Mean Algorithm in Cloud Computing Environment". Journal of University of Babylon, 26 (2), pp 27-35, 2018.
[4] Pandeeswari, N., & Kumar, G, "Anomaly detection system in cloud environment using fuzzy clustering-based ANN, "Mobile Networks and Applications, vol.21, No. (3), pp. 494-505, 2016.
[5] Mishra, P., Pilli, E. S., Varadharajan, V., &Tupakula, U, "Efficient approaches for intrusion detection in cloud environment," In Computing, Communication and Automation (ICCCA), IEEE International Conference on, pp. 1211-1216, 2016.
[6] Deshpande, P., Sharma, S. C., Peddoju, S. K., &Junaid, "S. HIDS: A host-based intrusion detection system for cloud computing environment". International Journal of System Assurance Engineering and Management, 9(3), 567-576, 2018.
[7] Aishwarya, R., & Malliga, S, "Intrusion detection system-An efficient way to thwart against Dos/DDos attack in the cloud environment," In Recent Trends in Information Technology (ICRTIT), IEEE International Conference on Recent Trends in Information Technology, Chennai, pp. 1-6, 2014.
[8] Haidar, G. A., &Boustany, C, "High perception intrusion detection system using neural networks," Ninth IEEE International Conference on Intelligent, and Software Intensive Systems (CISIS), pp.497-501,
[9] Nie, L., Jiang, D., & Lv, Z, "Modeling network traffic for traffic matrix estimation and anomaly detection based on Bayesian network in cloud computing networks, "Annals of Telecommunications, vol.72, pp.5-6, 297-305.
[10] Seth, Jitendra Kumar, and Satish Chandra. "An Efficient Hybrid Intrusion Detection System in Cloud." 653-666,2018.
[11] N. Moustafa, G. Creech, E. Sitnikova and M. Keshk, "Collaborative anomaly detection framework for handling big data of cloud computing," Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, pp.1-6, 2017.
[12] Priyanka, Kumar. S, Kaur. A, "Prevention of Black Hole Attacks in Virtualized Cloud Network Using Trust- Aware Energy Efficient AODV Routing with Firefly Based AI Technique," International Journal of Recent Technology and Engineering (IJRTE), vol.8, no.2, 2019.
[13] Gandomi, A. H., Yang, X. S., & Alavi, A. H, "Cuckoo search algorithm: a metaheuristic approach to solve structural optimization problems," Engineering with computers, Vol.29, No.1, pp.17-35, 2013.
[14] Zhang, Z, "Artificial neural network, "In Springer, Cham Multivariate Time Series Analysis in Climate and Environmental Research, pp. 1-35, 2018.
[15] Witkowski, M.; Brenner, P.; Jansen, R.; Go, D.B.; Ward, E., "Enabling Sustainable Clouds via Environmentally Opportunistic Computing," IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), pp.587-592,2010.
[16] Cavdar, D.; Alagoz, F., "A survey of research on greening data centers," IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, pp.3237-3242,2012
[17] Userwei Ding, Xiaolin Qin, Liang Liu, Taochun Wang, "Energy efficient scheduling of virtual machinesin cloud with deadline constraint", Future Generation Computer Systems, pp.62-74, 2015.
[18] Xiaomin Zhu, Laurence T. Yang, Huangke Chen, Ji Wang, Shu Yin and Xiao cheng Liu, "Real-Time Tasks Oriented Energy-Aware Scheduling in Virtualized Clouds", IEEE, Transactions on cloud computing, vol.2, issue 2, pp-168-180, 2014.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

[19] Deshpande, P., Sharma, S. C., Peddoju, S. K., &Junaid, "S. HIDS: A host-based intrusion detection system for cloud computing environment". International Journal of System Assurance Engineering and Management, 9(3), 567-576, 2018.