ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 3, pp: (273-281), Month: July - September 2020, Available at: www.researchpublish.com

A SECURE INTRUSION DETECTION SYSTEM USING COA WITH ANN FOR CLOUD COMPUTING ENVIRONMENT

[1]DHEERAJ KUMAR, [2]RAJAN SACHDEVA

[1]Research Scholar (M.Tech), [2]Head of Department Computer Science

Guru Gobind Singh College of Modern Technology (GGSCMT), Kharar

Sahibzada Ajit Singh Nagar, Punjab 140301, India

Abstract: **Cloud computing is the recent fashionable approach used to provide computing services such as storage, database, network, software, analytics and more over the internet. As the communication has been performed through wireless link, therefore, the security of cloud data should becomes a major concern. To resolve this problem, IDS (Intrusion Detection System) is designed for cloud system using Artificial Neural Network (ANN) with Cuckoo Search (CS) approach. In the beginning, the CS algorithm is used to choose the cloud server's best features. The CS algorithm is used to refine the path between the source server node and the destination server node. Therefore, when intruder joins the network, its properties are correlated with the properties that are contained in the database. If the properties are not matched then, it is detected as intruder otherwise; normal server and starts communication. ANN is equipped based on structured properties such as site co-ordinates, distance between servers and energy consumed by the system. Furthermore, the built model's output is ultimately calculated and correlated with the existing work.**

Keywords: **Network, Artificial Neural Network (ANN), Intrusion Detection System (IDS), Cuckoo Search (CS).**

I. INTRODUCTION

Presently, in the IT world, cloud computing is the fastest growing computing method. It provides various services to their users such as comfort, on demand; Shared computing resources like as networks, servers, storage, and applications. The computing network is influenced by a number of threats and a safety environment has been implemented to secure the information. A research will be done by a number of authors to enhance the security level [1]. Security is a major concern for decision-making in the cloud computing space. When security standards are promulgated by the provider or the buyer needs the higher level security standards, so it becomes necessary to address the security issues in cloud services. The cloud computing is about providing information on the benefits of preventing malicious software attacks like DDoS. Solutions offered by a trusted cloud computing service will detect DDoS attacks and respond effectively to ensure 24/7 availability. It can also provide solutions that protect users' credentials against theft. In addition, without a secure platform, hackers can access transaction information, manage data, and return fake data to harm cloud computing clients [2].

Of all the network security challenges, this research has focused on the DDoS attack, which is an extension of DoS (Denial-of-Service) attack. DoS Attack and its distributed version seek to make a service unavailable to intended users by unloading a DdoS attack, system or network source. Although the experts working in the network security have devoted grate effort in order to solve this problem, DDoS attacks have been on the rise, and have been increasingly affected the computing services in recent times [3].

Existing DDoS attack protection solutions have been presented by a number of researchers such as (Bhushan and Gupta, 2019 [4]; Saxena and Dey, 2019[5] and Velliangiri & Premalatha; 2019 [6]) have contained a network that is completely controlled by enterprise network managers. Therefore, network administrators were able to place certain hardware components on the network to detect or reduce DDoS attacks. However, these assumptions are no longer work in the new network computing paradigm [7-9].

Therefore, to resolve the problem of security, a nature inspired approach named as Cuckoo Search (CS) in addition to machine learning approach has been presented. The combination of CS with ANN approach makes the Intrusion detection system (IDS) more robust. The training data has been prepared by applying CS approach, which again enhance the training speed by obtained a set of database. Also, the CS approach helps ANN structure to bias signal in less time and hence increase the speed of detecting intruder in cloud environment [10].

II. RELATED WORK

Deshpande et al. (2018) implemented a host-based intrusion detection framework in cloud computing including its comparative analysis and implementation. The approach only analyzes specific system call traces, and not all, the failed system call trace. With this feature, early detection of intrusions for reduced computational burden may be possible. The model described provides security as a service (SaaS) within the Cloud system infrastructure layer. The results of implementation indicate an average sensitivity of intrusion detection of 96% [11].

Hajimirzaei et al. (2019) presented a novel intrusion detection method (IDS) on the basis of integrating Multilayer Perceptron (MLP) and Artificial Bee Colony (ABC) along with Fuzzy Algorithms. The normal and abnormal network traffic packets are defined by the MLP, while the ABC algorithm conducts the MLP training by optimizing the weight and bias values of the linkages. The suggested approach is tested with the CloudSim simulator and the NSL-KDD dataset. Mean absolute error (MAE), root mean square error RMSE has been considered as criteria for evaluation with obtained RMSE is 0.1217 and MAE is 0.0286 [12].

Alzahrani et al. (2018) provided approach to detect attacks involving known as well as unknown DDoS attack. Two different methods utilized for identification of intrusion named as anomaly- based combining with artificial neural network (ANN) and signature-based strategy. The proposed hybrid model produces enhanced accuracy (99.98%) to detect DDoS attack as compare to separately signature-based (97.52%) and neural based gives (98.10%) accuracy. Amazon public datasets has been utilized to perform this work [13].

Yang et al. (2018) propose SDN architecture for the detection and protection of machine learning based DDoS attacks. This system consists of 3 sections which are module for the collection of traffic, module for DDoS attack detection and module for the distribution of flow chart. Traffic collection module collects traffic characteristics for traffic detection preparations. SVM has been used to classify DDoS traffic. The results of the experiment on the KDD99 dataset demonstrate the efficacy. This platform allows for real-time online identification of DDoS attacks and the necessary security strategies. This design of the system doesn't rely on other hardware and has good portability [14].

Verma et al. (2019) implemented an adaptive hybrid approach to the collection and classification of incoming traffic attributes. The suggested method consists of three subsystems, named as (a) pre-processing subsystem, (b) adaptive selection subsystem for attributes and (c) the subsystem for identification and prevention. The work uses the NSLKDD dataset which helps in evaluating the approach proposed. The combination of Mean Absolute Deviation technique with Random Forest Classifier (MAD-RF) is concluded to outperform the other combinations. The result shows that MAD-RF outperforms reduction of dimensionality, conventional methods of selection of attributes. The results show that the chosen MAD-RF combination achieves the highest accuracy of 98%, 98.066% detection rate, and 98.34% precision [15].

Wang, Z., & Zhu, Y. (2017) proposed a centralized host-based IDS architecture to minimize the resource utilization. By used the logstash tool to collect device logs from each virtual machine, and centrally store them in an elastic search cluster. After that, all of these logs are evaluated in the detection centre and reports are sent to each virtual machine. All of these logs are processed in the detection centre and findings are sent to each virtual machine. Our architecture has been tested in the Open stack platform. The results demonstrate good performance in reducing CPU and memory utilization [16].

III. PROPOSED WORK

The IDS is Proposed in cloud environment on the basis of CS approach along with artificial neural network. In this work, we have mainly focused on the DDoS attack as an intruder. To optimize the route among source and destination server, CS algorithm is utilized as per the fitness function Fitness function on the basis of which route has been optimized is written below:

$$Fitness\ function = \left\{ \begin{matrix} P_s(True) & if\ \ P_s \geq P_t \\ P_t(False) & otherwise \end{matrix} \right\} \qquad (1)$$

Here, the property of servers and the threshold values on the basis of which intruder has been detected is represented by equation (1). Based on the best selection of servers, ANN has been trained by categorizing the properties into two classes that is intruder nodes and normal nodes. The trained features of servers are stored into the database for future use. **D**uring the testing process, the attacker server and normal server can be easily classified. To measure the performance of cloud system QoS (Quality of Service) parameter as well as detection accuracy of system is analyzed.

Also, the description of CS with ANN has been provided below:

3.1 CUCKOO SEARCH (CS)

Cuckoo Search (CS) was developed by Xin-she Yang and Suash Deb in 2009 as an optimization algorithm. It is inspired by the host of several cuckoo species that often lay their eggs in the nests of many other (other) host birds. Certain host birds that overlap immediately to invasive cucumbers. Some cuckoo species, such as New World parasitic barracuda, have adapted so that female parasitic cuckoos often imitate the colour and pattern of eggs of a variety of host species very closely. Dewey quest idealizes this breeding behaviour and can therefore be extended to different optimization problems and it appears that the program will outperform other heuristics. If the egg is present in the nest, it is a novel solution. The key objective is to make the most of the new and potentially better solution by eliminating the wrong solution in the nest. Typically, an individual nest has a single egg, and the algorithm becomes more complicated if the nest has more than one egg. The solution can then be found using the following steps, written below:

1. Put one egg at a time for each cuckoo and place the eggs in a randomly selected nest;

2. The best egg quality nest will continue to the next generation;

3. The number of available host nests is set and the host bird discovers with the eggs laid by the Cuckoo a probability of P (0,1).If the solution is obtained then the discovered solution do not go for farther search [17].

The image of the cuckoo bird and its eggs in the nest is shown in Figure 3 and the step descriptions are shown below:

Figure 1: Cuckoo bird with their egg

3.2 ANN

The ANN classifier is biologically inspired algorithm. The working strategy of this algorithm is based on the interlinked nodes as well as units. These nodes or units are termed as artificial neurons that on some manner similar to the neurons of biological nervous system. The signal can be processed through the connectivity of neurons that are equivalent to the synapses present inside the brain.

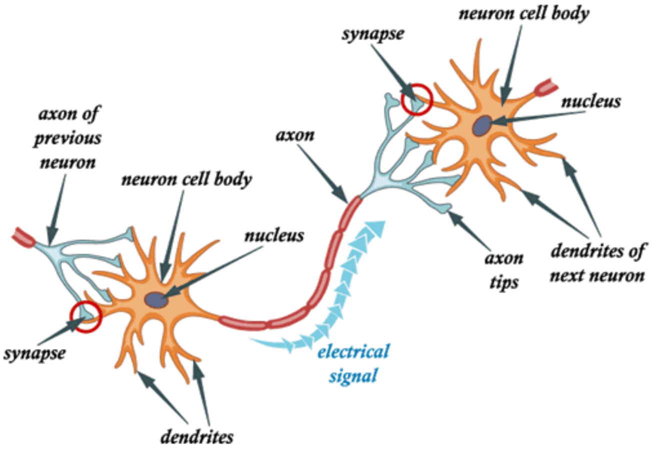

Figure 2: Biological structure of neural network

Figure 2 demonstrates a binding neuronal cell to another neuron. The cell consists of a cell nucleus, with dendrites that serve as connecting wires to attach to other neurons. A neuron has one axon that can effectively transfer electrical currents to other connecting cells in most cases. The neuronal connections are formed using synapses located at the axon end [18].

Figure 3, shows a typical neural network consists of input layer, hidden layer and output layer with connections.

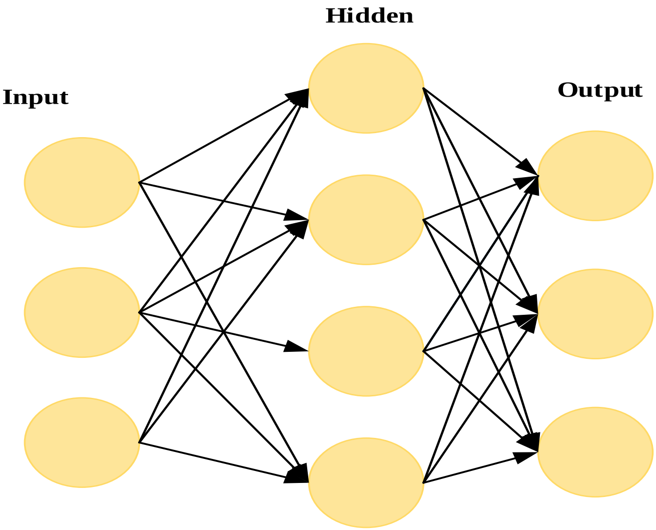

Figure 3: Artificial Neural Network

ANN has been employed to offer solutions for resolving social networking, medical diagnosis, speech recognition, computer vision, games play and machine translation problems. The neurons are connected using different patterns so that feedback from some neurons is used as the input of other neurons and results in a weighted graph network.

i. The architecture of this network has three layer input layer, hidden layer (it can be more than one) and the output layer. It also known as the Multilayer perceptron (MLP) due to this multiple number of hidden layers.

ii. The hidden layer can be called the distillation layer which distils some of most important pattern from the inputs and forward it to the next layer. Because of this layer network becomes faster and efficient through identifying the important data only.

iii. Output layer is the last layer of neurons producing the program's outputs.

One of the specialties of neural networks is that the hidden unit’s factors. The network which implemented a neural network in it actually has the ability to extract higher order statistics by adding one or more hidden layers [19].

IV. EXPERIMENTAL RESULTS

Matrix Laboratory (MATLAB) tool has been used to evaluate the performance of the proposed cloud network, which is protected against DDoS. MATLAB version 2016 a have been used with a core i3 version having RAM of 16 GB. Following results are executed after the simulation of work.

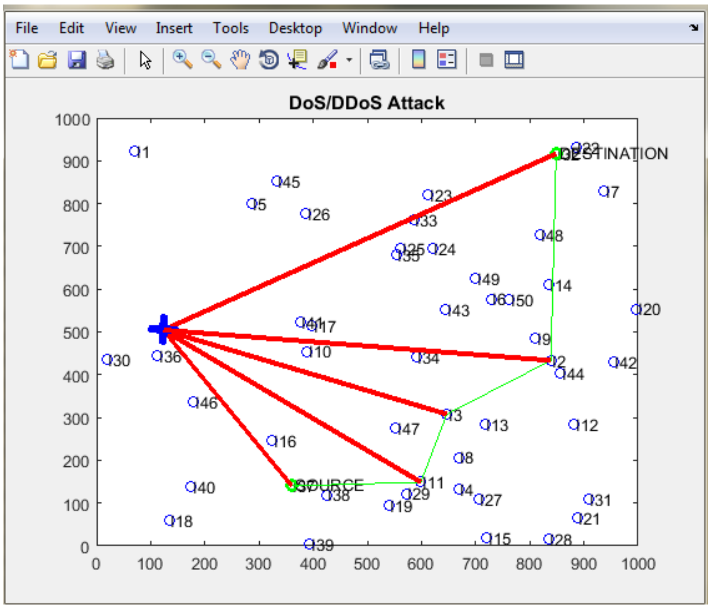

Figure 4: Intruder in the Cloud Network

The scenario with intruder occurs in the network is shown in Figure 4. The intruder affected the entire communicating nodes as depicted in the above figure. Node 38 is behaving as a source service, with node 22 as a destination server. As shown in Figure 2, Q 36 acts as an attacker node and hence affects the entire communicating nodes along with the source and the destination node. The experiment has been perfumed in two scenarios (i) Without any Prevention Algorithm and (ii) With Prevention Algorithm. The parameters observed for the two different scenarios are given below.

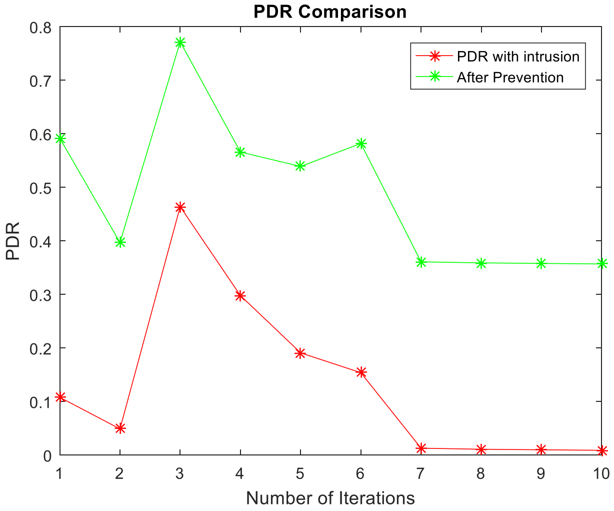

Figure 5: PDR with and without Prevention Algorithm

The values of PDR analyzed after preventing the cloud network against the intruder along with the intruder is represented by the green line and the black line respectively. From the graph, it is clearly seen that the PDR using nature inspired approach with machine learning has performed better and hence provide better PDR values for the entire 10 number of iterations. The average values analyzed for 10 number of iteration with intruder and without intruder are 0.1307 and 0.488 respectively. It has been observed that PDR has been increased with higher rate while utilizing prevention algorithm.

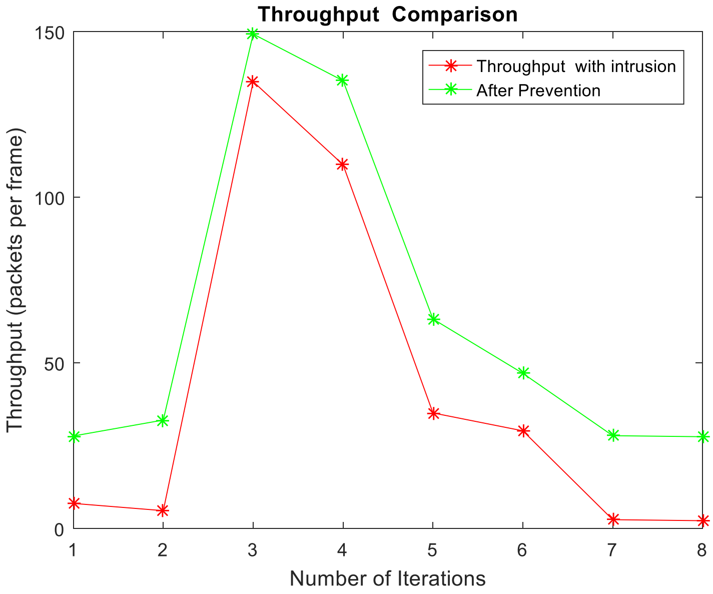

Figure 6: Throughput with and without Prevention Algorithm

Figure 6 illustrated the throughput analyzed in the presence and after the detection of intruder. The figure shows that using a preventive algorithm the rate of data transmission in the cloud network increases in contrast to the presence of intruder. The transmission values obtained after simulating the designed network in the presence and after the detection of intruder are represented in red and pink line respectively. The average value of throughput measured with and without prevention algorithm are 33.17 packets/timeframe and 57.2 packets/timeframe respectively. Thus, it has been find out that about 54.09 %.

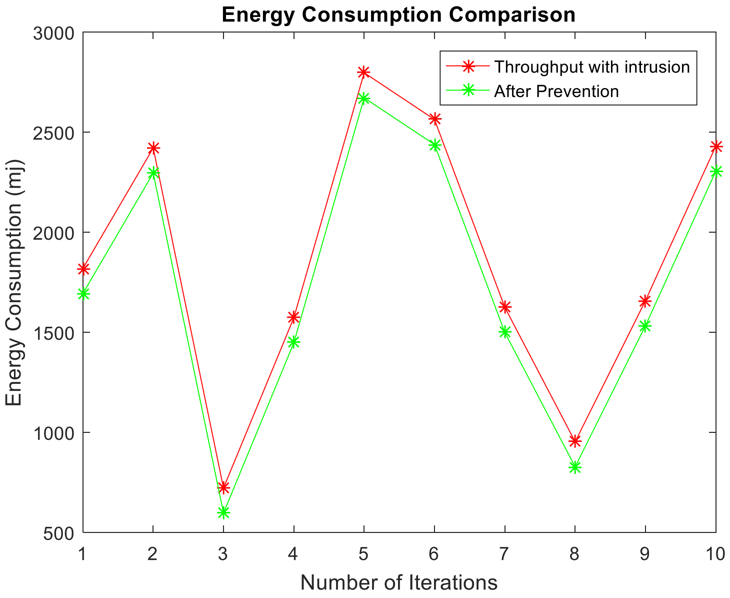

Figure 7: Energy Consumption with and without Prevention Algorithm

Figure 7 demonstrates the energy consumption values measured while the services are provided to the user. The energy is consumed by each user while communicating with each other. The case when the intruder exists in the network, the probability of consuming energy is high as the intruder starts dropping information. In this research, the energy that have been observed with and without intrusion are 1855.34 mJ and 1730.54 mJ respectively. Thus there is a reduction of about 6.73 %.

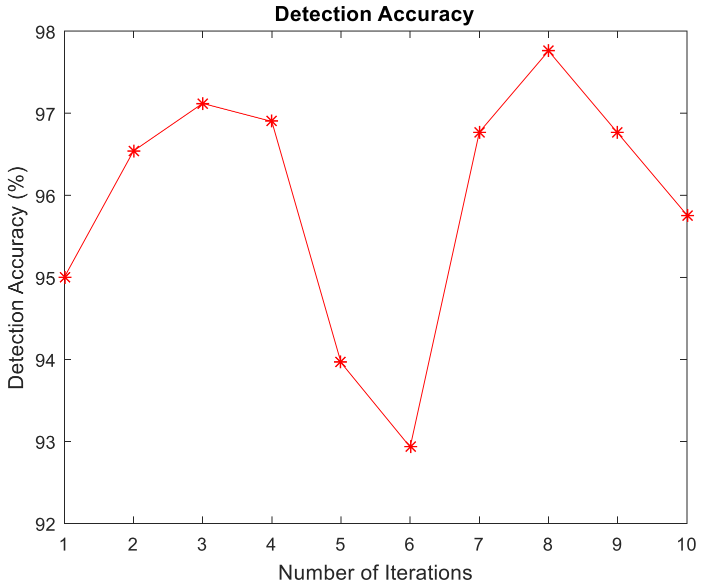

Figure 8: Detection Accuracy with and without Prevention Algorithm

Detection is the foremost parameters, which represents the efficiency of the design intrusion detection system. From the figure 8, it is clear that the detection accuracy is constant upto five iterations and then starts decreasing. The detection accuracy is high because the ANN can segregate the intruder server from the genuine server effectively. The average detection rate measured for the proposed system is about 99.89 %, which represents the designed system accurately identified the intruder and hence protect the cloud system from the malicious user.

To show the betterment of the designed IDS system comparison with the previous work has also been presented, which is proposed by Ghosh et al.in 2019 [20]. In the existing work, Cuckoo Search (CS) along with · Particle swarm optimization (PSO) are used in hybridization in order to trained the IDS on the basis of extracted features. Pre-processing and normalization steps have been performed on the KDD dataset and the features are selected using CS along with PSO algorithm. The detection accuracy upto 75.5 % has been obtained. Figure 9 represents the comparison graph plotted between proposed work and existing work performed by Ghosh et al. (CS-PSO) in 2019. From the graph it is shown that by utilizing optimization algorithm along with classification technique the detection accuracy enhanced by 20.2 %.

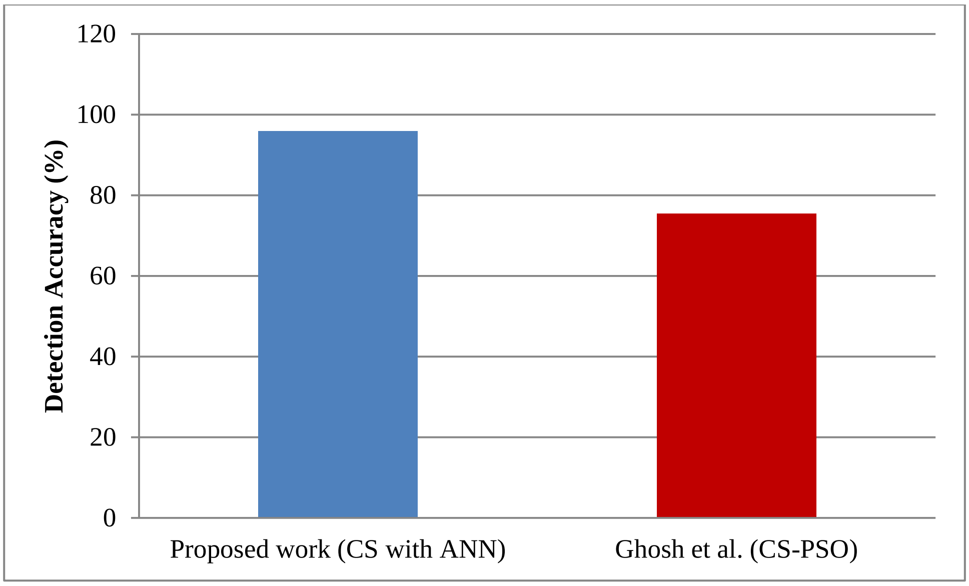

Figure 9: Comparison of proposed with Ghosh et al. (CS-PSO)

V. CONCLUSION

In this research, IDS for the cloud server has been designed to provide protection for cloud data by using optimization along with classification algorithm. The CS algorithm is used to optimized the features of severs on the basis of its fitness function. The ANN algorithm is trained as per the optimized server properties and a list of genuine server and the intruder server is created, which is stored into its database. So that the application attributes are compared with the stored values during the testing process and, if the values suit the attacker domain data, it is otherwise marked as an attacker object. The findings are analyzed for both situations. So that the application attributes are compared with the stored values during the testing process and, if the values suit the attacker domain data, it is otherwise marked as an attacker object. The findings are analyzed for both situations. From the experiment it has been observed that the intruder is identified effectively using prevention algorithm and the detection accuracy of about 98.89 % has been obtained.

REFERENCES

[1] Modi, C., Patel, D., Borisanya, B., Patel, A., & Rajarajan, M. (2012, October). A novel framework for intrusion detection in cloud. In *Proceedings of the fifth international conference on security of information and networks* (pp. 67-74).

[2] Wang, B., Zheng, Y., Lou, W., & Hou, Y. T. (2015). DDoS attack protection in the era of cloud computing and software-defined networking. *Computer Networks*, *81*, 308-319.

[3] Chonka, A., Xiang, Y., Zhou, W., & Bonti, A. (2011). Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of Network and Computer Applications*, *34*(4), 1097-1107.

[4] Bhushan, K., & Gupta, B. B. (2019). Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. *Journal of Ambient Intelligence and Humanized Computing*, *10*(5), 1985-1997.

[5] Saxena, R., & Dey, S. (2019). DDoS attack prevention using collaborative approach for cloud computing. *Cluster Computing*, 1-16.

[6] Velliangiri, S., & Premalatha, J. (2019). Intrusion detection of distributed denial of service attack in cloud. *Cluster Computing*, *22*(5), 10615-10623.

[7] Geneiatakis, D., Portokalidis, G., & Keromytis, A. D. (2011, December). A multilayer overlay network architecture for enhancing IP services availability against DoS. In *International Conference on Information Systems Security* (pp. 322-336). Springer, Berlin, Heidelberg.

[8] Liu, X., Yang, X., & Lu, Y. (2008, August). To filter or to authorize: Network-layer DoS defense against multimillion-node botnets. In *Proceedings of the ACM SIGCOMM 2008 conference on Data communication* (pp. 195-206).

[9] Mittal, P., Kim, D., Hu, Y. C., & Caesar, M. (2011). Mirage: Towards deployable DDoS defense for Web applications. *arXiv preprint arXiv:1110.1060*.

[10] Morein, W. G., Stavrou, A., Cook, D. L., Keromytis, A. D., Misra, V., & Rubenstein, D. (2003, October). Using graphic turing tests to counter automated DDoS attacks against web servers. In *Proceedings of the 10th ACM conference on Computer and communications security* (pp. 8-19).

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

[12] Hajimirzaei, B., & Navimipour, N. J. (2019). Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm. *ICT Express*, *5*(1), 56-59.

[13] Alzahrani, S., & Hong, L. (2018, July). Detection of distributed denial of service (DDoS) attacks using artificial intelligence on cloud. In *2018 IEEE World Congress on Services (SERVICES)* (pp. 35-36). IEEE.

[14] Yang, L., & Zhao, H. (2018, October). DDoS attack identification and defense using SDN based on machine learning method. In *2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN)* (pp. 174-178). IEEE.

[15] Verma, P., Tapaswi, S., & Godfrey, W. W. (2019). An Adaptive Threshold-Based Attribute Selection to Classify Requests Under DDoS Attack in Cloud-Based Systems. *Arabian Journal for Science and Engineering*, 1-22.

[16] Wang, Z., & Zhu, Y. (2017, June). A centralized HIDS framework for private cloud. In *2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)* (pp. 115-120). IEEE.

[17] Singh, D. A. A. G., Priyadharshini, R., & Leavline, E. J. (2018). Cuckoo Optimisation based Intrusion Detection System for Cloud Computing. *International Journal of Computer Network and Information Security*, *10*(11), 42.

[18] Lippmann, R. P., & Cunningham, R. K. (2000). Improving intrusion detection performance using keyword selection and neural networks. *Computer networks*, *34*(4), 597-603.

[19] https://becominghuman.ai/natural-vs-artificial-neural-networks-9f3be2d45fdb

[20] Ghosh, P., Karmakar, A., Sharma, J., & Phadikar, S. (2019). CS-PSO based intrusion detection system in cloud environment. In *Emerging Technologies in Data Mining and Information Security* (pp. 261-269). Springer, Singapore.