A Novel Approach of Intrusion Detection System in Cloud Computing Using Ai

Ms. Krupa Bhavsar[1], Ms. Jagruti Patel[2], Dr. Gajendra Purohit[3]

[1,2]Assistant Professor, DCS, Ganpat University
[3]Director, Pacific College of Basic & Applied Sciences, PAHER University

ABSTRACT

IDS (Intrusion Detection System) is primarily used to protect corporate networks. Ideally, IDS can detect all (attempted) intrusions in real time and perform work to prevent the attack (for example, modify firewall rules). Intrusion detection systems are becoming a basic network security system. Currently available commercial tools have limitations in detecting real intrusions. NN (Neural network) with GA (Genetic algorithms) are considered to be an effective way to enhance IDS systems performance based on misuse detection models and anomaly detection models. This research has considered GA and ANN for the detection of intruders with the performance parameters, like Energy consumption, Delay and PDR (Packet delivery ratio) to depict the effectiveness of the research.

Keywords: IDS, GA, ANN, Energy consumption, Delay and PDR

INTRODUCTION

IDS (Intrusion Detection System) plays a major role in the persistence and security of an active defense system for intruder attacks for some IT and business organization. The implementation of cloud computing needs an effective, scalable and virtualization-based mechanism [1]. For cloud, the applications and user data are hosted on the providers of cloud servers and the users have less control on the resources and the data. Therefore, the IDS administrations have become the accountability of cloud providers. Roschke et al. have presented a hybrid solution for essential IDS management which integrates varied renowned IDS sensors outcome report on a lone interface. IDMEF (Intrusion detection message exchange format) standard is utilized for the communiqué with varied IDS sensors [2]. A number of researchers have shown the IDS sensor deployment on different cloud layers such as the application layer, platform layer, and a system layer. The researchers have shown an efficient cloud IDS management framework that can be analyzed and administrated as per cloud user and has given essential IDS management system for varied sensors with IDMEF standard for monitored and communication by cloud users [3].

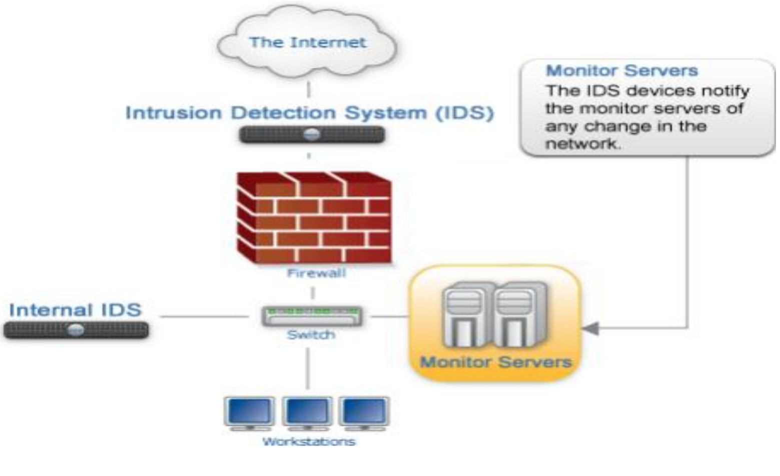
The Internet
Intrusion Detection System (IDS)
Monitor Servers
The IDS devices notify the monitor servers of any change in the network.
Firewall
Internal IDS
Switch
Monitor Servers
Workstations

Figure 1: Traditional IDS

The classification of IDS is into two types, NIDS (Network Intrusion Detection-based) detection system on the basis of data captured network for the examination with the signatures of predicted attacks with the abnormality in the examined network hosts activities. IDS should be situated at a point with more network visibility monitoring. Network-based IDS has been shown below[4].

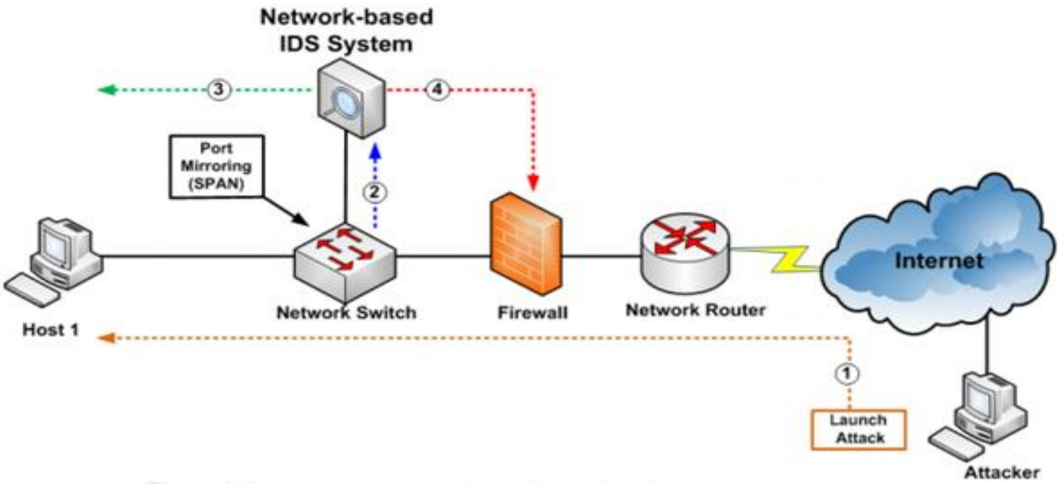

Figure 2: Network-based IDS

HIDS (Host-based Intrusion Detection) examines the local host activity. It could utilize the log files of the OS (Operating system) databases or events for the computation [5]. The aim is the attacks assessment with an attempt of some illegal access towards the machine. In HIDS, IDS is placed on the machine monitor.

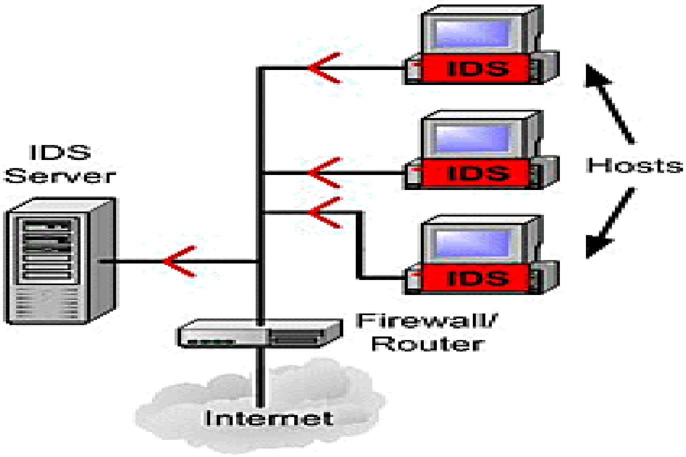

Figure 3: Host-based IDS

In this research, an efficient IDS has been presented with GA (Genetic Algorithm) and ANN (Artificial Neural network). A number of researchers have proposed IDS but the system performance is not satisfactory because of the lack of suitable AI (Artificial intelligence) method for categorizing general communicating nodes with attacker's nodes [6]. For the network, the intrusion is generally considered as an illegal activity for jeopardizing the network resources. The intend of IDS is to examine the activities of users with their behavior in varied communication levels. In the research work, IDS utilizes GA and Ann as a classifier for the detection of intrusions [7]. It has been considered that IDS is basically passive and could only detect the intruders. After the simulation of the network, parameters such as delay, energy consumption and PDR are computed to depict the effectiveness of the proposed work.

Implemented Framework

This research has deals with the idea of proposing a prevention mechanism that identifies intruders on the basis of location with the energy patterns that differs in intruder framework [8]. The process of presented work with routing protocol with GA optimization is provided used for the network. The network has been computed with fixed width and height. Below mathematical notation has been used to set up the network [9]:

$$\mathrm{AreaofNetwork} = \mathrm{HeightXWidth}$$

After the development of the network area, few nodes within in the network area are defined with the source as well as destination nodes for the execution of the proposed work. For obtaining the route in IDS, the coverage area is set up.

After describing the source node with the destination node, the route has been initialized with the routing protocol from the source node headed for the destination node [10]. GA optimization algorithm has been utilized for optimizing the route and for discovering the attacker's nodes. In the end, performance parameters have been computed. Below network specifications have been set up to simulate the work:

Table 1: Network Requirements

Area	1000*1000
Node / Machine Count	50-100
Total number of performance evaluation iterations	5-10
Node Placement	Random Architecture Frame Model
Energy Model	Radio Energy Model

The explanation of the algorithms considered for the execution is given below:

Artificial neural network

ANN is considered as a solution for a number of issues like optimization, control, forecasting with the identification of patterns. A classifier has been designed on for training as well as testing of the system. ANN has been used to enhance the efficiency of the classification process. The ANN algorithm is defined below:

Algorithm 1: Artificial neural network

```
Input: Training data, group, neurons
Output: Obtained best possible route for simulation
Initialize ANN with
        — Training data=Properties of nodes
        — group=possible route
        — Training algorithm=LM
        — Neurons=15
        — Transfer function=T sigmoid
        — Iteration=50
Set performance parameters-MSE
        — Gradient
        — Mutation
        — Validation choice
Generate a structure of ANN
Net=newff (training data, group, neurons)
Net=Train (net, training data, group)
If classify as a secure route
Consider as a intrusion free route
Else
Not consider as a route
End if
Return; optimized returns
End (function)
```

GA (Genetic Algorithm)

GA defines intelligent random search exploitation for solving the optimization problems. GA is randomized for directing the search within the region for enhanced performance in the search space. GA based IDS is used for the development of detection of intrusions for complicated and rare attacks performance.

Algorithm 2: Genetic algorithm

```
I/P: Properties of nodes, fitness function
O/P: Optimized path
Initialize function of genetic algorithm-
        — population size=50
        — Selection function
        — mutation function
        — Crossover function
Defined fitness function (fit_function)
```

```
Fit_function=    true;    if $f_s < f_t$
                 False;   otherwise
For i=1 to all nodes
$f_s$ =Consumption of nodes
$f_t$ = average of nodes consumption
Call fit_function ($f_s$, $f_t$)
Optimized path
End (for)
If route the is optimized
Train ANN
Else
Reject the route
End (if)
Return, list of routes
End (function)
```

RESULT AND ANALYSIS

This section defines the results obtained after the simulation of the proposed work. The parameters considered for the evaluation are Energy consumption, Delay and PDR. The results are shown in tabular and graphical form:

Table 1: Comparison of Energy consumption

Number of iterations	**Energy Consumption with intrusion**	**Energy consumption after prevention**
1	145	130
2	147	125
3	152	140
4	160	139
5	165	145

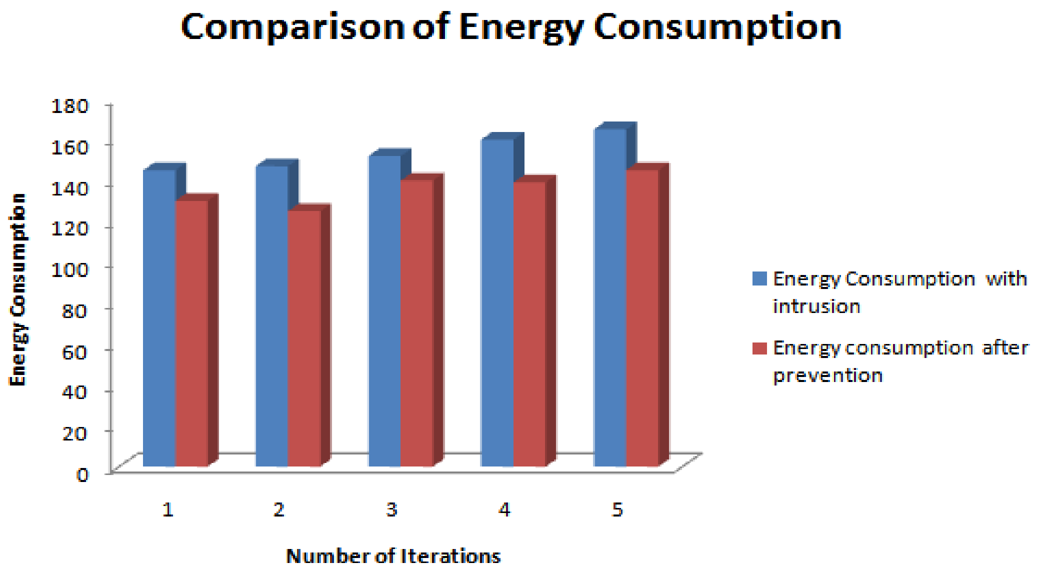

Figure 4: Energy Consumption Computation

Energy consumption explains the total energy being consumed by the network while packet data transmission from source nodes towards the destination node. Energy consumption can be computed as:

$$\text{Energy consumption} = E_{Tx} + E_{Rx} + E_{Amp} + E_{Agg} + E_{Prop}$$

Where, E_{Tx} is the transmission energy, E_{Rx} is the receiving energy, E_{Amp} is the amplification energy, E_{Agg} is the aggregation energy and E_{Prop} is the propagation energy

As shown in figure and table, comparison of energy consumption with intrusion and with prevention has been shown. X-axis describes the number of iterations and Y-axis defines the values obtained after the simulation of energy consumption. Blue bar defines the results of energy consumption with intrusion and red bar defines the energy consumption after prevention. The average value of energy consumption with intrusion is 153.8 and the average value of energy consumption after prevention is 135.8.

Table 2: Comparison of Delay

Number of iterations	Delay with intrusion	Delay after prevention
1	100	90
2	120	115
3	135	122
4	152	146
5	168	154

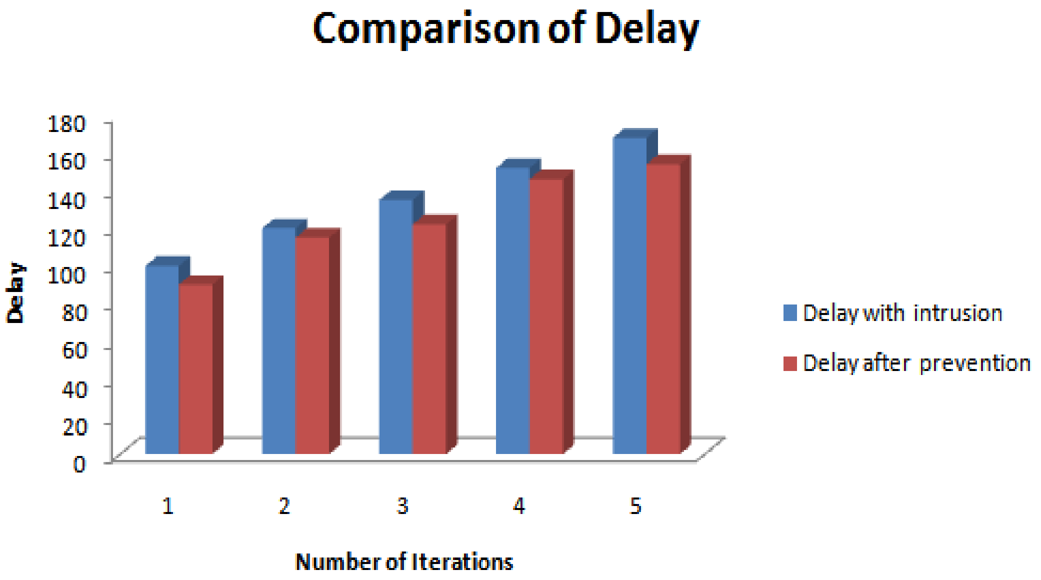

Figure 5: Delay Computation

Delay is the time that a packet takes from source to destination node in a network. Normally, those routes are utilized in the network with less delay probability for the proposed work. Delay can be defined mathematically as:

$D_{end-end}= D_{trans}+D_{prop}+D_{proc}$
As shown, $D_{end-end}$= End-To-End Delay, D_{trans}= Transmission Delay (D_{prop}= Propagation Delay and D_{proc}= Processing Delay

As illustrated in figure and table, comparison of delay with intrusion and with prevention has been shown. X-axis shows the number of iterations and Y-axis defines the values obtained after the simulation of delay. Blue bar depicts the outcome of delay with intrusion and red bar defines the delay after prevention. The average value of delay with intrusion is 135 and the average value of delay after prevention is 125.4.

Table 3: Comparison of PDR

Number of iterations	PDR with intrusion	PDR after prevention
1	0.55	0.85
2	0.67	0.76
3	0.49	0.89
4	0.38	0.72
5	0.53	0.83

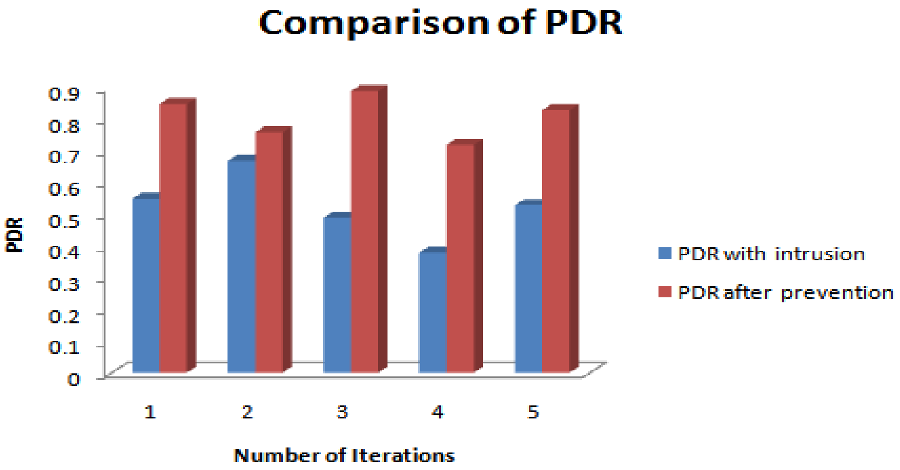

Figure 6: PDR Computation

PDR is illustrated as the proportion of packets that are efficiently set to the destination as contrasted to the packets which are transferred by the sender.

$$PDR = \frac{\text{number of packets delivered}}{\text{number of packets sent}}$$

As represented in figure and table, comparison of PDR with intrusion and with prevention has been shown. X-axis defines the number of iterations and Y-axis defines the values obtained after the simulation of PDR. Blue bar defines the results of PDR with intrusion and red bar defines the delay after prevention. The average value of PDR with intrusion is 0.524 and the average value of PDR after prevention is 0.81.

CONCLUSION

IDS is known as the significant manner to achieve more security in a computer network and is utilized to prevent from a number of attacks. IDS have a dimensional curse that increases the time complexity with the reduction in resource utilization. As a result, it is hoped that intrusion detection systems must analyze important features of the data to decrease the dimensions. In this manuscript, novel mechanism has been presented to identify the intruders by using GA and ANN approach. GA approach has been proposed with enhanced initial population and selection operators for efficiently detecting different network intrusions. The goal of the experiment is to test the use and process of ANN learning for intrusion detection and to test the meaning of the ANN input. This research has used Energy consumption, Delay and PDR parameters to compute the effectiveness of the proposed work. The average value of energy consumption with intrusion is 153.8 and the average value of energy consumption after prevention is 135.8. The average value of delay with intrusion is 135 and the average value of delay after prevention is 125.4. The average value of PDR with intrusion is 0.524 and the average value of PDR after prevention is 0.81.

REFERENCES

[1]. Sebastian Roschke, Feng Cheng, Christoph Meinel,“ Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.

[2]. Joshi, P., Prasad, R., Mewada, P., & Saurabh, P. (2018). A New Neural Network-Based IDS for Cloud Computing. In *Progress in Computing, Analytics and Networking* (pp. 161-170). Springer, Singapore.

[3]. Modi, C., & Patel, D. (2018). A feasible approach to intrusion detection in the virtual network layer of Cloud computing. *Sādhanā*, *43*(7), 11.

[4]. Gai, K., Qiu, M., Tao, L., & Zhu, Y. (2016). Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. *Security and Communication Networks*, *9*(16), 3049-3058.

[5]. Ibrahim, E. F., & Ismail, S. (2018). Detection DDOS Using Ids In Cloud Computing. *Journal of Computing Technologies and Creative Content (JTeC)*, *3*(1), 4-6.

[6]. 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.

[7]. Osanaiye, O., Cai, H., Choo, K. K. R., Dehghantanha, A., Xu, Z., & Dlodlo, M. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking*, *2016*(1), 130.

[8]. Rajendran, P. K., Muthukumar, B., & Nagarajan, G. (2015). Hybrid intrusion detection system for private cloud: a systematic approach. *Procedia Computer Science*, *48*, 325-329.

[9]. Modi, C., & Patel, D. (2018). A feasible approach to intrusion detection in virtual network layer of Cloud computing. *Sādhanā*, *43*(7), 114.

[10]. Al Haddad, Z., Hanoune, M., & Mamouni, A. (2016). A Collaborative Network Intrusion Detection System (C-NIDS) in Cloud Computing. *International Journal of Communication Networks and Information Security*, *8*(3), 130.

[11]. Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2016, September). A survey of intrusion detection systems for cloud computing environment. In *Engineering & MIS (ICEMIS), International Conference on* (pp. 1-13). IEEE.

[12]. Achbarou, O., & El Bouanani, S. (2017). Securing cloud computing from different attacks using intrusion detection systems. *International Journal of Interactive Multimedia and Artificial Intelligence*, *4*(3), 61-64.

[13]. Cabrera, Luis Felipe, Eric Jason Hlutke, Bond Masuda, Jacob Brunetto, Jeff Seifers, and M. Shannon Lietz. "Method and system for extrusion and intrusion detection in a cloud computing environment." U.S. Patent Application 14/171,388, filed August 6, 2015.

[14]. Kim, Jeong Hun, and Sung Hyun Kim. "Method for detecting and preventing a DDoS attack using cloud computing, and server." U.S. Patent 9,386,036, issued July 5, 2016.

[15]. Liang, H., Ge, Y., Wang, W., & Chen, L. (2015, December). Collaborative intrusion detection as a service in cloud computing environment. In *Progress in Informatics and Computing (PIC), 2015 IEEE International Conference on* (pp. 476-480). IEEE.

[16]. Alqahtani, S. M., Al Balushi, M., & John, R. (2014, March). An intelligent intrusion detection system for cloud computing (sidscc). In *Computational Science and Computational Intelligence (CSCI), 2014 International Conference on* (Vol. 2, pp. 135-141). IEEE.