Cloud Security Enhancements by Intrusion Detection Systems with Soft Computing techniques

Sankarsan Sahoo
Asst. Professor, Department of CSE,
Gandhi Institute for Technological Advancement,
Bhubaneswar, Odisha, India

Manoranjan Pradhan
Professor,Department of CSE
Gandhi Institute for Technological Advancement,
Bhubaneswar, Odisha, India

Abstract- We all know that cloud computing has become more widely accepted in the enterprise network. We are starting to see Cloud 2.0 - next generation cloud businesses that provide businesses functionality beyond software rental. Cloud computing is an internet or intranet based computing, where Infrastructure, Platform and Application are provisioned based on demand. The major breach in cloud is its security due to its huge extends of resources available in it. There are various approaches being utilized in intrusion detection, but unfortunately any of the systems so far is not completely flawless. So, the quest of betterment continues. In this paper we surveyed various Intrusion Detection Systems proposed over the years and propose the Soft Computing based techniques are better with the intent of enhancing security requirements in present Cloud Computing environment.

Keywords – Cloud Computing, SaaS, PaaS, IaaS, IDS, HIDS, NIDS, DIDS, VMIDS, DoS, EDoS

I. INTRODUCTION

National Institute of Standards and Technology (NIST) [1] has given the definition of Cloud Computing as: Cloud computing is a model for 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. Cloud computing is cost-efficient where users do not need to buy technical infrastructure, software, and information.

Cloud Computing provides services in three ways: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) over the internet. There are number of users, who use the cloud services over the untrusted network. This model of cloud makes it vulnerable. The applications over the cloud are increasing rapidly and along with these applications vulnerabilities and numbers of attacks are also increasing [2]. In addition, cloud computing is distributed so it is more likely to face security threats and interaction as privacy violations, Denial of service (DoS), and unauthorized access [3]. One of defense lines for such environment is applying Intrusion Detection System to protect cloud resources and services from intrusive activities [4]. In this paper we are highlighting the use of Soft Computing techniques for improving security requirements in Cloud using Intrusion Detection Systems (IDSs).

Remainder of the paper is organized as follows: Sections II and III explains Cloud Computing and its layered architecture with possible attacks on Cloud collected from various research papers. Section IV describes Intrusion Detection Systems and some of the important techniques for Intrusion Detection, highlighting the Soft Computing related works and its significance. Section V dictates the conclusion along with the proposed work of Intrusion Detection Systems with Soft Computing techniques for covering existing unrevealed and dynamic security requirements for scalable Cloud Computing Environment.

II. CLOUD COMPUTING ENVIRONMENT

The Cloud Computing is one of the emerging technologies in the world. It is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. Cloud computing customers do not own the physical infrastructure, thereby avoiding capital expenditure. They rent resources from a third-party provider, consume them as a service and pay only for resources that they use [5]. There are various Cloud service delivery models that are developed, which can be divided into three layers [6] depending on the type of resources provided by the Cloud.

Software as a Service (SaaS) is a model for which the applications are hosted as services to customers who access it via the Internet. When the software is hosted off-site, the customer doesn't have to maintain it or support it. On the other hand, it is out of the customer's hands when the hosting service decides to change it [6]. **Platform as a Service (PaaS)** on the other hand, delivers the cloud services differently. As the name suggests, PaaS supplies all there sources required to build applications and services completely from the Internet, without having to download or install any kind of software. However, PaaS lacks the interoperability and portability among different providers [6]. Google App Engine is an example of PaaS clouds where users can create their own applications with either python or Java and deploy it on Google's cloud .**Infrastructure as a Service (IaaS),** sometimes referred to as Hardware as a Service or HaaS, it is considered the next form of services available in Cloud Computing. Where SaaS and PaaS are providing applications to customers, IaaS provides the organizations with hardware resources that can be used for anything. By renting resources we mean any resources that a person can think of, including Server Space, Network Equipment, Memory, CPU Cycles, Storage Space, etc. Additionally, the infrastructure resources can be scaled up or down based on the application resource needs [6].

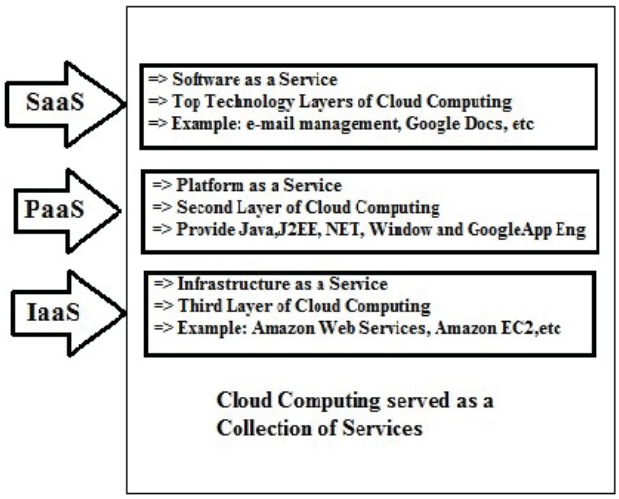

Fig.1. Three Layers in Cloud Computing [6]

Fig - 1 shows a basic Cloud Computing Model as three layers in Cloud Computing. It shows Cloud provides various types of services. It provide storage, infrastructure, and platform as a service. Cloud works in pay-as-you-go basis that means we have to pay according to services which we want to use. Cloud covers broad category of services.

III. ATTACKS ON CLOUD SYSTEMS

In the cloud system the attacks are performed mainly on the availability of services, confidentiality and integrity of stored data. Attacks can be performed by the insiders or by the outsiders. An insider is an authorized user of cloud system, if that user tries to access some services for which he/she is not permitted then this type of attack is called insider attack. Otherwise it is outsider attack. Some of these attacks are:

- *Flooding Attack***:** In this attack, attacker tries to flood any user (victim) by sending huge amount of packets through any innocent host machine. The packets can be of type TCP, UDP, ICMP. Due to this, user's machine will always tries to handle these requests and will not be able to provide services to legitimate user requests. Flooding attack causes DoS and DDoS attacks [7].

- *Economic Denial of Sustainability (EDoS) Attack:* Attacker tries to exhaust the resources allotted to the legitimate user by flooding attack thereby raising the usage bills for the legitimate user.
- *User to Root Attack:* In this attack, attacker gets access to the legitimate user's account by guessing password or sniffing. Any normal system user illegally gains access to the root privileges.
- *Port Scanning Attack:* In the Port Scanning attack, attacker tries to find the list of open ports, closed ports and filtered ports. Then attacker can attack to the services running on the ports of his interest. Through the port scanning information such as IP address, MAC address, router filtering, firewall rules can be found.
- *Backdoor Channel Attack:* A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing illegal remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program or may subvert the system through a Rootkit‖ [8]. Using such backdoor channels attacker can control victim's resources and make it a zombie machine to launch flooding attack.

IV. INTRUSION DETECTION SYSTEMS AND RELATED WORKS

Teodoro et al.[9] has defined **Intrusion Detection Systems (IDS)** is a security tool that, like other measures such as antivirus software, firewall and are intended to strengthen the security of information and communication systems. Therefore, Intrusion detection aims to control the events occurring on a network in an intelligent way.

Cloud Computing is prone to attacks due to its distributed nature. So a solution to the security problems like various attacks in the cloud, is IDS. It monitors the activities of the user and track the network traffic and determines whether the activity is malicious or not. If the activity is malicious IDS generates alarm, as shown in the Fig.2. IDSs uses various techniques like anomalies or signatures of attack to detect the attack and success of IDS also depends upon these techniques. According to the placement of IDS in the network, IDS are two types: **Host Based IDS (HIDS)** and **Network Based IDS (NIDS)**.

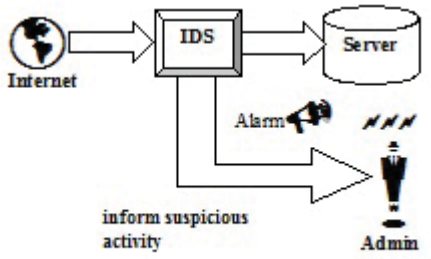

Fig.2. Intrusion Detection System (IDS)

Host based IDS (HIDS): These are placed at the specific host machine and they monitors dynamic behavior and internal state of a system. HIDS looks host's stored information in the file system, log files and check that the contents of these appears as expected! The disadvantage of HIDS is that it can't detect the networked attacks; it only looks into the particular system. For effective usage of Cloud resources, Jun-Ho Lee et al.[10] has proposed a multilevel IDS and log management method. It applies security strength (high, medium, low) to different levels of user behaviour.

Network based Intrusion Detection Systems (NIDS): These are placed at the key network points like routers and switches. It monitors the network traffic and inspects the packets whether it contains any malicious data. Usually the communication between the hosts is encrypted and NIDS can't detect it that is the drawback of the NIDS. But NIDS is better than HIDS because HIDS protects only one system and using NIDS all the hosts connected to the network can be protected. Bakshi, Yogesh et al. [11] proposed an NIDS which uses signature based method for intrusion detection. The IDS is installed on the virtual switch and logs all the incoming and outgoing network traffic into the database for auditing. Alharkan, Martin et al. [12] proposed the Intrusion Detection System as a Service (IDSaaS) framework, which is a network and signature based IDS for the cloud model. In particular, IDSaaS is an on-demand, portable, controllable by the cloud consumer and available through the pay-per-use cost model.

Distributed Intrusion Detection System (DIDS): It consists of multiple Intrusion Detection Systems (IDS) over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring, incident analysis, and instant attack data. DIDS contains both type of sensors (HIDS and NIDS). Lo ,Huang et al. [13] proposed a DIDS to encounter DDoS attacks. In this approach IDS systems are deployed in each cloud region. An IDS sends alert messages to other IDSs. By judging the accuracy of these alerts if agent finds an intrusion, it adds a new rule into the block table.

Virtual Machine based IDS (VMIDS): ***In*** cloud computing every physical machine runs more than one virtual machine to facilitate provisioning of services to more number of users. IDS component is deployed inside each virtual machine. One approach described by Bharadwaja et al. [14] uses Xen Hypervisor based IDS platform. It is a collaborative IDS called Collabra. Collabra works in a virtualized environment. There are multiple hosts in virtualized environment and Collabra instances are integrated with the VMM (Virtual Machine Monitor) of each host.
Intrusion Detection Systems can be used in cloud to detect various attacks. The success of IDSs depends upon the techniques used for the intrusion detection like Signature based Intrusion Detection or Anomaly based Intrusion Detection or Soft Computing based Intrusion Detection or Hybrid Techniques for Intrusion Detection.

Signature based Intrusion Detection: A Signature based IDS uses a database of rules (signatures) of different attacks known previously as shown in Fig.3. These signatures are used to compare the incoming network pattern, if the incoming network pattern matches the signature, an intrusion is detected. This type of detection methods has an advantage, that by knowing the network behavior signatures are easy to develop and understand. For example [15], you might use a signature that looks for particular strings within an exploit payload to detect attacks that are attempting to exploit particular buffer-overflow vulnerability. Signature based IDS have very high accuracy in detecting known attacks and minimum number of false positives. The new signatures can be added into the Signature database without modifying existing ones. The main drawback of Signature based IDSs is that these types of IDSs are not able to detect unknown attacks; even a slight variation in the pattern can fool it.

Lo and Huang [13] proposed a signature based Distributed IDS for DDoS attack, Bakshi and Yogesh [11] proposed a signature based Network IDS for virtual machines and Shelke [16] proposed a multithreaded signature based Network IDS.

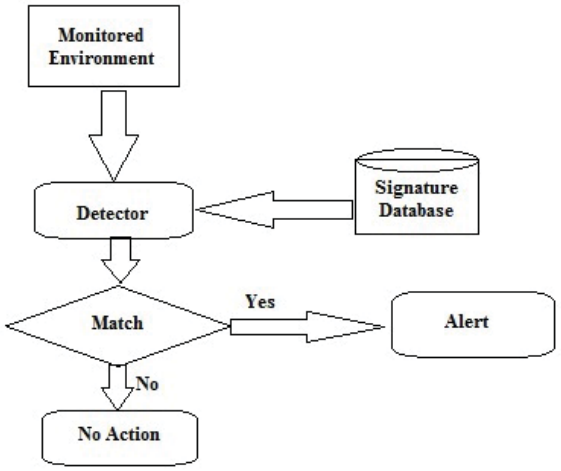

Fig. 3. Signature based IDS architecture

Anomaly based Intrusion Detection: Anomaly based IDS uses behaviour based approach. It identifies the event that seems to be malicious as compared to the normal system behavior. It checks the deviation between the normal behavior and current user's behavior as shown in Fig.4. It collects the information of legitimate user's action or behaviour over a period of time. This information is used to train the system. Then a statistical test is performed to check whether this behaviour belongs to legitimate user's behaviour.

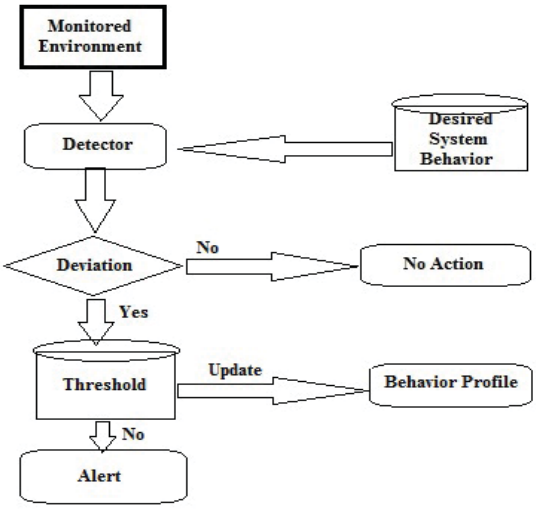

Fig. 4.Anomaly based IDS architecture

Anomaly based IDS can detect unknown or zero-day attacks [17] even though system is not updated [18]. The maintenance of this type of IDS is very difficult because updating the behaviour for which system is trained can't be done without losing the previous one. The detection accuracy of this type of IDSs is also low means false positives are high. P. García-Teodoro et al. [19] proposed anomaly based techniques can be classified in three categories according to the nature of the processing involved in the behavioural model: Statistical based, Knowledge based and Machine learning based techniques.

Soft Computing based Intrusion Detection: Soft computing techniques such as Artificial Neural Network, Fuzzy Logic, Support Vector Machine, Association Rule Mining and Genetic Algorithm can also be used for intrusion detection purpose. Moradi et al.[20] proposed a Soft Computing technique acts as an intelligent agent in the system that is capable of disclosing the secret patterns in abnormal and normal connection audit records, and to generalize the patterns to new (and slightly different) connection records of the same class.

Artificial Neural Network (ANN) consists of an interconnected group of artificial neurons, in this network nodes are artificial neurons. An artificial neuron is a computational model inspired by the natural neurons [21]. The main reason behind the use of ANN for intrusion detection is its ability to generalize data (from incomplete data) and to be able to classify data as being normal or intrusive [22]. Types of Artificial Neural network which can be used in IDSs can be classified into following three categories [22]: Multi-Layer Feed-Forward (MLFF) neural nets, Multi-Layer Perceptron (MLP) and Back Propagation (BP). The ANN based IDS can be used efficiently for unstructured data. The detection accuracy of ANN depends upon the number of hidden layers in the network and the training data. The disadvantage of using ANN is that it requires huge amount of data samples for training.

Support Vector Machines (SVM) are supervised learning models with associated learning algorithms that analyze data recognize patterns, used for classification and regression analysis of both linear and nonlinear data. SVM is useful in detection of intrusions even with the availability of less sample data. SVM has good generalization ability even with the high dimensional data. SVM requires lesser number of training samples as compared to ANN based classifiers. SVM can only be used for binary data. Cheng et al. [23] said that, performance of SVM degrades when it is adapted for multi-class classification.

Fuzzy Logic is a form of many-valued logic or probabilistic logic. It deals with reasoning that is approximate rather than fixed and exact. Fuzzy logic uses truth values between 0.0 and 1.0 to represent the degree of membership that a certain value has in a given category. Dickerson and Dickerson et al. [24] proposed an approach called Fuzzy Intrusion Recognition Engine (FIRE) that uses fuzzy logic to detect the occurrence of any malicious activity. Dickerson et al. [25] modified the FIRE and told that this system is able to detect host and port scanning and Denial of Service attacks.

Association rules are used to find the relationship or similarity between the objects. In the field of intrusion detection, association rules can be used to detect the variants of known attacks, misuse detection and generation of signatures for known attack. Misuse detection is based on the intrusion characteristics. Once detecting any intrusion characteristics, IDS confirms that intrusion happened. Based on those characteristics, new rules can be generated to detect any variant of known attack. To form the rules an Apriori algorithm is used. Hong et al. [26] proposed Signature Apriori algorithm to generate signatures for NIDS. In the Cloud Computing scenario Association rule mining technique can be used to generate new signatures for the variants of known attack.

Genetic Algorithm (GA) is a search heuristic that attempts to incorporate ideas of natural evolution. This heuristic is routinely used to generate useful solutions to optimization and search problems. Wei Li et al. [27] told that GA can be used to generate rules for the network connection that can be used to classify the network behavior as intrusive or normal. In cloud Computing Genetic algorithm can be used for evolving new rules for IDS. Using these rules normal network traffic or audit data can be differentiated from abnormal traffic/data.

Hybrid Techniques for Intrusion Detection: It uses two or more than two techniques for intrusion detection and can detect more intrusions than regular one. Chavan et al. [28] proposed an approach called Evolving Fuzzy Neural Network (EFuNN) that combines Fuzzy Inference System (FIS) and ANN. The training time for the approaches proposed in [28] is quite high. Fuzzy Logic technique for intrusion detection gives better result when it is combined with some other technique, in fact it can be used as a primary step to another technique. Fuzzy Logic can be used to reduce the training time of SVM and ANN. Xia, Qu, Yusuf, et al. [29] proposed a hybrid method to detect network anomalies that is based on information theory and genetic algorithm. Information theory is used to filter traffic data and to reduce complexity of GA. Bashair Al-Shdaifat, et al. [30] has proposed a Hopfield Artificial Neural Network (HANN) that uses Simulating Annealing for Cloud Intrusion Detection with <=93% detection rate. Jabez, J., et al.[31], researchers have designed and implemented a Knowledge-Based Anomaly Intrusion Detection framework, which is based on the Hyperbolic Hopfield Neural Network and trained by using KDD'99 datasets, the Hyperbolic Hopfield Neural Network is more efficient than Genetic Algorithms and Fuzzy Neural Network with a 95 % rate. H. Akramifard, L. Mohammad Khanli et al.[32] has proposed Multi-Level Fuzzy Neural Network (MLF-NN) approach for Intrusion Detection in Cloud Computing environment which has 99.6% detection rate and 0.38% false positive rate.

V. CONCLUSION

We have realized that there are extreme advantages of using the Cloud Computing technology but there are several security issues too. These issues should be considered while adopting the Cloud Computing technology for secure functioning of our systems. There are various types of attacks on cloud services. Various Solutions have been suggested to cope up with these security issues and Intrusion Detection System is one such solution.

In this paper, we have explored various IDSs which are used with Cloud Computing and it is observed that Soft Computing based intrusion detection techniques are better to track various threats efficiently and it also gives better result. They can be used to generalize, classify different threats efficiently than other available security systems. Specifically they acts as an intelligent agents and use association rules to detect attack variations. Our next step is to propose a Hybrid Soft Computing based IDS model or an architecture which can detect and prevent the various threats and other security related issues in Cloud Computing environment with higher detection rate and lower false positive rate and which will continuously deplete the efficiency and the productivity of the cloud.

REFERENCES

[1] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf, "Cloud Computing Reference Architecture", *NIST Special Publication* (2011):500-292

[2] Uttam Kumar, Bhavesh N. Gohil "A Survey on Intrusion Detection Systems for Cloud Computing Environment". *International Journal of Computer Applications* , Volume 109 – No. 1, (2015):0975 – 8887

[3] Raghav Iti., Chhikara Shashi., Hasteer Nitasha,"Intrusion Detection and Prevention in Cloud Environment: a Systematic Review", *International Journal of Computer Applications*, Vol-68, No-24 (2013):7-11

[4] Gyanchandani Manasi., Rana J. L., Yadav R. N.,"Taxonomy of Anomly Based Intrusion Detection System: A Review", *International Journal of Scientific and Research Publications* (2012) Vol-2, Issue-12

[5] Pradip Patil, Gurudatt Kulkarni, Amruta Dongare "Cloud Computing an Overview*", International Journal of Modern Engineering Research*, Vol.2, Issue.2 (2012):380-382

[6] Hassen Mohammed Alsafi ,Wafaa Mustafa Abduallah and Al-Sakib Khan Pathan "IDPS: An Integrated Intrusion Handling Model for Cloud Computing Environment", *International Journal of Computing and Information Technology*, vol no-4, Issue no-1 (2012):1-16

[7] Ashley Chonka, Yang Xiang, Wanlei Zhou, Alessio Bonti,"Cloud security defense to protect cloud computing against HTTP-DoS and XML-DoS attacks", *Journal of Network and Computer Applications*, Vol. 34, Issue 4 (2011): 1097-1107.
[8] Rootkit: http://en.wikipedia.org/wiki/Rootkit (Accessed 30 April 2015)
[9] Teodoro, P., García., Verdejo, J., Díaz., Fernández, G., Maciá., Vázquez, E. "Anomaly-based network intrusion detection: *Techniques, systems and challenges"*, Science Direct., 2009
[10] Jun-Ho Lee; Min-Woo Park; Jung-Ho Eom; Tai-Myoung Chung, "Multi-level Intrusion Detection System and log management in Cloud Computing", *13th International Conference on Advanced Communication Technology (ICACT)*, (2011): 552-555.
[11] Bakshi A.,Yogesh B."Securing cloud from DDOS attacks using intrusion detection system in virtual machine", *Second IEEE International conference on communication software and networks* (2010) :260-264.
[12] Turki Alharkan, Patrick Martin 2012, "IDSaaS: Intrusion Detection System as a Service in Public Clouds", *12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing* (2012): 686-687.
[13] Lo CC, Huang CC, Ku J.,"Cooperative Intrusion detection system framework for cloud computing networks", *39th IEEE International Conference on Parallel Processing Workshops*,(2008) :280-284.
[14] Bharadwaja, S., Weiqing Sun, Niamat, M.,Fangyang Shen,"Collabra: A Xen Hypervisor Based Collaborative Intrusion Detection System", *Eighth International Conference on Information Technology: New Generations,* 2011:695-700.
[15] James C. Foster 2005, "IDS: Signature versus anomaly detection", http://searchsecurity.techtarget.com/tip/IDS-Signature-versus-anomaly-detection (Accessed in April 2016)
[16] Shelke, Ms Parag K., Ms Sneha Sontakke, and A. D. Gawande,"Intrusion Detection System for Cloud Computing", *International Journal of Scientific & Technology Research*, Volume 1, Issue 4 (2012)
[17] Dotan Cohen," What is a Zero-Day Exploit?" http://what-is-what.com/what_is/zero_day_exploit.html (Accessed in April 2016)
[18] Mudzingwa, D.; Agrawal, R., "A study of methodologies used in intrusion detection and prevention systems (IDPS)", *Proceedings of IEEE Southeastcon*, (2012):1-6.
[19] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, E. Vázquez,"Anomaly-based network intrusion detection: Techniques, systems and challenges", Computers & Security, Vol. 28, Issues 1–2, (2009):18-28
[20] Moradi M, Zulkernine M., "A neural network based system for intrusion detection and classification of attacks", *In Proceedings of the 2004 IEEE International conference on advances in intelligent systems—theory and Applications*, 2004
[21] Carlos Gershenson 2003, "Artificial Neural Networks for Beginners". http://arxiv.org/ftp/cs/papers/0308/0308031.pdf (Accessed April 2016)
[22] Ibrahim LM. , "Anomaly network intrusion detection system based on distributed time-delay neural network", *Journal of Engineering Science and Technology*, Vo. 5, Issue: 4,(2010)
[23] Chi Cheng, Wee Peng Tay and Guang-Bin Huang, "Extreme Learning Machines for Intrusion Detection", *The 2012 International Joint Conference on Neural Networks,* (2012):1-8.
[24] Dickerson, J.E., Dickerson, J.A.,"Fuzzy network profiling for intrusion detection", *19th International Conference of the North American Fuzzy Information Processing Society*, (2000):301-306.
[25] Dickerson, J.E., Juslin, J., Koukousoula, O., Dickerson, J.A.,"Fuzzy intrusion detection", *IFSA World Congress and 20th NAFIPS International Conference*, (2001):1506-1510.
[26] Hong Han, Xin-Liang Lu, Li-Yong Ren," Using data mining to discover signatures in network-based intrusion detection", *Proceedings of International Conference on Machine Learning and Cybernetics*, (2004), pp. 13- 17.
[27] Wei Li, "Using Genetic Algorithm for Network Intrusion Detection", *In Proceedings of the United States Department of Energy Cyber Security Group Training Conference*, (2004), pp. 24-27.
[28] Chavan, S., Shah, K., Dave, N., Mukherjee, S., Abraham, A., Sanyal, S.,"Adaptive neuro-fuzzy intrusion detection systems", *Proceedings of International Conference on Information Technology: Coding and Computing*,(2004), pp. 70- 74.
[29] Xia, T.; Qu, G.; Hariri, S.; Yousif, M.,2005 , "An efficient network intrusion detection method based on information theory and genetic algorithm", *24th IEEE International Performance, Computing, and Communications Conference*,(2005), pp. 11-17.
[30] Bashair Al-Shdaifat, Wafa' Slaibi Alsharafat, Mohmmad el-bashir," Applying Hopfield Artificial Network and Simulating Annealing for Cloud Intrusion Detection", *Journal of Information Security Research* Volume 6 Number 2,(2015}: pp:49-54
[31] Jabez, J., Muthukumar, B.," Intrusion Detection System: Time Probability Method And Hyperbolic Hopfield Neural Network" , *Journal of Theoretical and Applied Information Technology*, 2007
[32] H. Akramifard, L. Mohammad Khanli , M.A Balafar, R. Davtalab, "Intrusion Detection in the Cloud Environment Using Multi-Level Fuzzy Neural Networks", *Proceeding of International Conference of Security Management*, 2015 :pp. 75-81