A Survey on Intrusion Detection Systems for Cloud Computing Environment

Uttam Kumar
Department of Computer Engineering
Sardar Vallabhbhai National Institute of Technology,
Surat - 395007, India

Bhavesh N. Gohil
Department of Computer Engineering
Sardar Vallabhbhai National Institute of Technology,
Surat - 395007, India

ABSTRACT

Cloud Computing is a newly emerged technology. It is getting popularity day by day due to its amazing services. The applications and services based on the cloud are emerging day by day. Due to networked nature of the cloud, resources, data and applications are vulnerable to the attack in cloud environment. So Intrusion Detection Systems (IDS) are employed in the cloud to detect malicious behaviour in the network and in the host. IDS monitors network or host system activities by collecting network information, and analyzes this information for malicious activities and generate alarms, if intrusion takes place. In this paper we surveyed various types of Intrusion Detection Systems proposed over the years for Cloud Computing environment.

Keywords

IDS, Cloud Computing, EDoS attack, HIDS, NIDS, and Signature based IDS; Anomaly based IDS, Attacks on Cloud

1. INTRODUCTION

Cloud Computing technology: A new Information Technology delivery paradigm has been enabled to reality because of the rapid development of processing and storage technologies, ubiquitously available Internet, cheaper and more powerful computing resources than ever before. ***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 provides services in three ways: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Cloud Computing provides its services over the internet. There are number of users, who use the cloud services over the untrusted network. This model of cloud makes the cloud vulnerable. The applications over the cloud are increasing rapidly and along with these applications vulnerabilities and numbers of attacks are also increasing.

Cloud Computing suffers from various network attacks such as Denial of Service Attack (DoS), Distributed Denial of Service Attack (DDoS), Flooding Attack, IP Spoofing. Network Attacks typically exploit the vulnerabilities in the network and protocols and can harm to the data and applications on the cloud. It can cause unavailability of data to the legitimate user. So to thwart these attacks and to prevent the cloud from being suffered from these attacks, Intrusion Detection Systems are used in the cloud computing environment. Remainder of the paper is organized as follows: Chapter 2 explains various types of attacks in the cloud environment and some solutions to the EDoS attack. Chapter 3 explains various techniques applicable in the Intrusion Detection Systems. Various types of Intrusion Detection Systems are discussed in the chapter 4. Chapter 5 includes conclusion and references used in the paper.

2. ATTACKS ON CLOUD SYSTEM

In the cloud system the attacks are performed mainly on the availability of services, confidentiality and integrity of stored data. Flooding attacks mainly affects availability. Attacks can be performed by the insiders or by the others. 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.

2.1 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 Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. DoS attacks are of two types: XML based DoS (X-DoS) and HTTP based DoS (H-DoS) [2]. When an XML message is sent to a Web Server or Web Service with malicious content to use up all their resources, X-DoS occurs. In the H-DoS attack, attacker starts up 1500 threads so that it can send randomized HTTP requests to the victim web server to exhaust its communication channels. In DDoS attack a number of host machines are used to send requests to a single machine. The aim of attacker is to make resources unavailable to the legitimate user.

2.2 Economic Denial of Sustainability (EDoS) Attack

This is a cloud specific attack. This attack is transformed from the DDoS attack. In the cloud environment, incoming user’s requests are handled by the virtual machines (VM). More and more VMs are provided if incoming requests are more in number. The cloud services are provided as pay-per-use basis according to service level agreement. Attacker tries to exhaust the resources allotted to the legitimate user by flooding attack thereby raising the usage bills for the legitimate user. The main aim of attacker is to bankrupt the user. Thus a traditional DDoS attack can be transformed into an Economic Denial of Sustainability attack (EDoS) in the cloud Environment.

2.3 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. A system can have a defect or bug and these bugs are exploited by the attacker to execute such a task which can only be executed using root level privileges not by user level privileges. Since attacker is using the legitimate user's account, it can't be diagnosed by just looking the packet. Buffer overflows are the most common type of attack mechanisms in this category. Buffer overflows occur when a program copies data into a buffer smaller than the data without checking the size of the buffer. Authentication process security mechanisms are the frequent target of this attack.

2.4 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. Port scanning attack is used to exploit the Zero-day vulnerability. There are various port scanning techniques such as TCP scanning, UDP scanning, SYN scanning, FIN scanning, ACK scanning, Window scanning etc. In Cloud environment, through port scanning attacker finds the open, close ports and can attack on the offered services at that ports.

2.5 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" [3]. This is a passive attack on the confidentiality of the user. Using such backdoor channels attacker can control victim's resources and make it a zombie machine to launch flooding attack. In Cloud environment, using backdoor channels, attacker can get access and control Cloud user's virtual machines and can use as a Zombie to initiate DoS/DDoS attack.

2.6 Attacks on Virtual Machines or Hypervisors

A hypervisor or virtual machine manager (VMM) is a piece of computer software, firmware or hardware used to create and runs virtual machines. A computer on which a hypervisor is running one or more virtual machines is a host machine. Each of those virtual machines is called a guest machine. Attacker can control the virtual machines by attacking on the hypervisor and consequently can gain access to the host machines. BLUEPILL [4], SubVirt [5] and DKSM [6] are some well-known attacks on virtual layer. Through these attacks, hackers can compromise the installed-hypervisor to gain control over the host machine. Virtual Machines (VMs) have Zero-day vulnerability that attracts an attacker to gain access to hypervisor. Attackers look into the target software for the Zero-day vulnerabilities before the developer of the target software and try to exploit that vulnerability.

Firewalls can be used to prevent some of the attacks such as EDoS attack, attacks on Virtual Machine etc. Sqalli et al. [7] has given an approach EDoS-Shield for mitigating an EDoS attack in cloud computing. The main components of the architecture as shown in the figure 1 are virtual firewalls (VF) and verifier cloud nodes (V-Nodes).

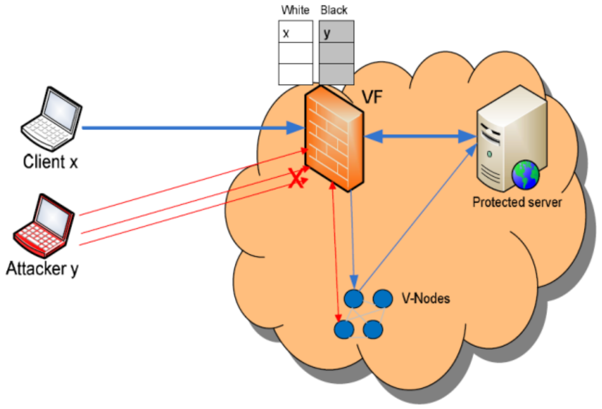

Figure 1: EDoS-Shield Architecture for mitigating EDoS [7]

The VF maintains two lists, a whitelist to track the authenticated source IP addresses and a blacklist to hold those unauthenticated source IP addresses. VF intercepts the incoming packets from outside the cloud and destined to some services hosted in the cloud and uses these two lists to verify the IP addresses of the incoming packets. Firewall will drop the incoming packets if the IP address of incoming packet will match with the IP addresses contained in the blacklist otherwise this incoming IP address will be added into the whitelist. Another component a V-Node has the capability to verify legitimate requests at the application level using graphic Turing tests [8], such as CAPTCHA.

In this approach the incoming request is captured by the VF and is directed to the V-Node. V-Node presents the requester a graphic Turing Test. Requester solves the test and sends response back to V-Node. If the answer to the test is correct, V-Node forwards the request to the destined server and adds the source IP address of the request into the whitelist. Upon receiving the wrong answer, V-Node adds this IP into the blacklist and drops the request packets. The main purpose is to verify the incoming request whether it is originated from a human user or it is an automated one. The IP spoofing is the drawback in this approach.

Another approach given by Sander and Shenai [9] uses a firewall and a puzzle server to prevent the EDoS attack. This approach is quite similar to the previous one. In this approach certificates will be provided to all the layers of cloud architecture such as hardware, virtual, user and network layers by the trusted third party for authentication. The user request to access cloud service is first intercepted by the firewall and then redirected to an on demand cloud service called puzzle server. Puzzle server sends the client a puzzle to solve and verifies the results sent by client. If result is correct, puzzle server sends positive acknowledgement to the firewall and firewall adds the client's IP to its white list and firewall redirects the user to access the cloud services otherwise firewall adds the IP into blacklist and blocks the request packets.

The drawback of both the approaches is that there is a puzzle server and verifier node, which will take some time to verify the user request. This will cause delay to the legitimate user request and these verifier nodes can also be used to launch DoS attack by sending huge number of request packets. Nodes will be busy all the time in processing these request packets.

3. INTRUSION DETECTION TECHNIQUES

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, Anomaly based Intrusion Detection and Artificial Intelligence based Intrusion Detection: ANN.

3.1 Signature based Intrusion Detection

A Signature based IDS uses a database of rules (signatures) of different attacks known previously. A signature is a pre-determined attack pattern. 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 [10], 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 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. Figure 2 presents a general architecture of Signature based IDS.

Roschke et al. [11] proposed a Signature based IDS which is virtual machine based IDS. This approach uses mainly two components: IDS Management unit and IDS sensor VMs. IDS management unit consists of four components: event gatherer, event data-base, analysis component and IDS remote controller. IDS sensor is responsible for identifying the malicious behaviour and Event gatherer stores triggered events in the event database. Event database stores information regarding captured events. Analysis component (configured by users) is responsible for representing the gathered events as well as analysing the events by accessing event database. IDS remote controller manages the IDS-VMs and is responsible for remote configuration and control of all connected IDS sensors. IDS sensors (NIDS) on the VM detect and report malicious behaviour and transmits triggered event to event gatherer [12]. Intrusion Detection Message Exchange Format (IDMEF) [13] has been used for communication between various IDS sensors.

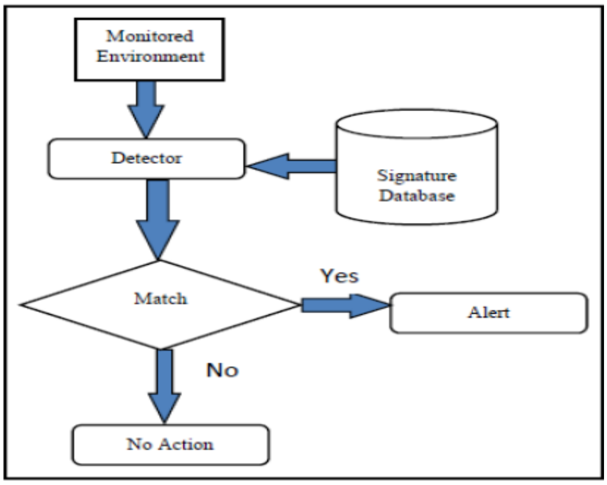

Figure 2: Signature based IDS Architecture [18]

Lo et al. [14] proposed a signature based Distributed IDS for DDoS attack, Bakshi and Yogesh [15] proposed a signature based Network IDS for virtual machines and Shelke et al. [16] proposed a multithreaded signature based Network IDS which we discussed letter.

3.2 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. 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.

Anomaly based IDS can detect unknown or zero-day attacks [17] even though system is not updated [18]. For example [19], suppose that a computer becomes infected with a new type of malware. The malware could perform such type of behaviour like sending large numbers of e-mails and consumption of the computer's processing resources that would be significantly different from the normal system user's behaviour. Figure 3 presents general architecture of Anomaly based IDS.

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. The anomaly based techniques [20] 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.

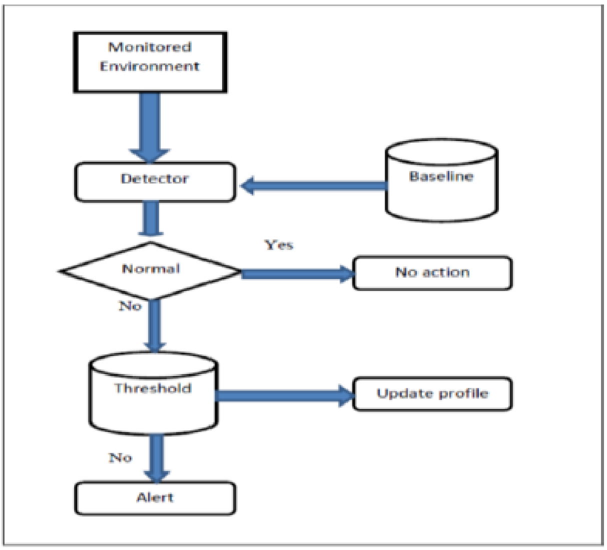

Figure 3: Anomaly based IDS Architecture [18]

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. In IDSs, soft computing techniques [24] 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.

3.3 Artificial Neural Network based Intrusion Detection

"Artificial Neural Network (ANN) is a mathematical model inspired by biological neural networks. A neural network 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 [25]". 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 [26]. Types of Artificial Neural network which can be used in IDSs can be classified into following three categories [26]: Multi-Layer Feed-Forward (MLFF) neural nets, Multi-Layer Perceptron (MLP) and Back Propagation (BP).

Ibrahim [26] has given a Distributed Time Delay Neural Network (DTDNN) and its detection accuracy for most of the network attacks is higher. 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. Bashah et al. [27] presented a neural network based IDS which uses Fuzzy Logic to reduce false alarm rate.

3.4 Support Vector Machine (SVM) based Intrusion Detection

"Support Vector Machines are supervised learning models with associated learning algorithms that analyse data recognize patterns, used for classification and regression analysis of both linear and nonlinear data. The basic SVM takes a set of input data and predicts, for each given input, which of two possible classes forms the output, making it a non-probabilistic binary linear classifier." 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. [28] said that, performance of SVM degrades when it is adapted for multi-class classification. Chitrakar and Chuanhe [29] have given an approach which combines k-Medoids clustering with SVM. In the first step, k-Medoids clustering technique is used to group the instances of similar behaviour. In the second step, SVM classifier classifies the resulting clusters into normal and attack classes. This approach shows good performance for small dataset but detection rate falls in case of larger dataset. Kausar et al. [30] has given an SVM based IDS mechanism with Principal Component Analysis (PCA) feature subsets. The dataset that is used for evaluation is transformed into another space and feature vectors using PCA. Then, these feature vectors are arranged in descending order of the Eigen values and divided into feature subsets. After that, these subsets are used as an input to the SVM classifier for classification purpose. The processing overhead of the classifier is reduced by using few features from the dataset. SVM can be used efficiently for intrusion detection in Cloud, if given sample data is limited in size since the dimensions of data are not affecting accuracy of SVM based IDS.

3.5 Fuzzy Logic based Intrusion Detection

"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 [31] proposed an approach called Fuzzy Intrusion Recognition Engine (FIRE) that uses fuzzy logic to detect the occurrence of any malicious activity. It can be seen by the experimental results given in [31], that the FIRE could detect a wide range of common attacks. After that Dickerson et al. [32] modified the FIRE and told that this system is able to detect host and port scanning and Denial of Service attacks. Tillapart al. [33] proposed a framework for IDS over TCP/IP network. Fuzzy IDS (FIDS) addresses to detect several kinds of attacks: syn-flood attack, udp-flood attack, ping-of-death attack, e-mail bomb, FTP and telnet password guessing, and port scanning. Chavan et al. [34] 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 [33] and [34] 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. Botha et al. [35] presented an approach for intrusion detection which uses Fuzzy Logic and Artificial Neural Network. Naqshbandi and Samawi [36] have given a system called One-Rule Genetic-Fuzzy classifier. In this system the Fuzzy rules has been defined. In this system the Fuzzy Logic is used for feature selection. Fuzzy Logic can be used to reduce the training time of SVM and ANN.

3.6 Association rule based Intrusion Detection

"Association Rule mining is a method for discovering interesting relations between variables in the large databases. It is intended to identify strong rules discovered in databases using different measures of interestingness." 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. [37] proposed Signature Apriori algorithm to generate signatures for NIDS. But Apriori algorithm has its own drawback: multiple database scan, high processing time etc. Ding et al. [38] and Zhengbing et al. [39] solved the problem of Apriori algorithm and proposed some improvement in the association rule mining. Li and Pan [40] have given IDS which uses new association rule mining model: φ-association rule mining and uses FP-tree mining algorithm. Lei et al. [41] proposed an improved Apriori algorithm: a Length-Decreasing Support to detect intrusion based on data mining.

In the cloud computing scenario Association rule mining technique can be used to generate new signatures for the variants of known attack.

3.7 Genetic Algorithm (GA) based Intrusion Detection

"A genetic algorithm 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.” A fitness function will be there for each rule which is a measure of each rules implementation.

Wei Li [42] told that GA can be used to generate rules for the network connection that can be used to classify the network behaviour as intrusive or normal. Both quantitative and categorical features of network data are included for rule generation. Xia et al. [43] 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. Mutual information between network features and the network intrusion (normal or abnormal), is used to extract useful features from network traffic data. Then, a linear structure rule is derived using the selected features and GA. This linear structure rule is used to classify the data as intrusive or normal. For real-time intrusion detection use of few network features is necessary and use of mutual information does this. However, this approach only considers discrete features. Lu and Traore [44] developed a method to derive a set of classification rules by using Genetic Programming (GP) with help of past data of network. Support Confidence based fitness function is used to generate rules. In this method using GP the practical implementation is more difficult due to requirement of more data or time for system. Goyal and Chetan [45] have used GA to form the rules and detected the DoS and probe attack. Abdullah et al. [46] proposed a Genetic Algorithm Intrusion Detection System (GAIDS) which uses first 18 features listed in KDD dataset. Uppalaiah et al. [47] has given a genetic algorithm based approach for IDS which uses different features of network connections such as a protocol type, duration, service, dst_host_srv_count to produce a classification on the rule set. This approach is capable of detecting DoS attack, probe attack, U2R and R2L attacks.

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.

3.8 Hybrid Techniques for Intrusion Detection

Hybrid Intrusion Detection Systems (HIDS) use two or more than two techniques for intrusion detection. It takes the advantages of the other techniques. Hybrid IDSs can detect more intrusions than regular one. Botha et al. [35] presented a hybrid approach for intrusion detection which uses Fuzzy Logic and Artificial Neural Network. Figure 4 depicts the general representation of NeGPAIM (Next Generation Proactive Identification Model).

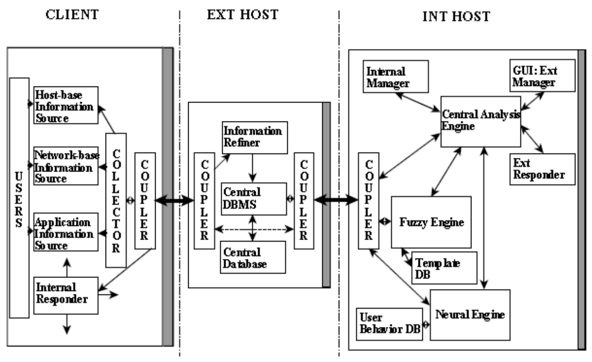

Figure 4: General Representation of NeGPAIM [35]

It has three components: one fuzzy engine for misuse detection, one neural engine for anomaly detection based on Artificial Neural Network and one central analysis engine which analyses the outcome of two engines; based on statistical measure. Bashah et al. [27] presented another approach which uses host based IDS and uses Neural Network and Fuzzy Logic as detection techniques.

Vieira et al. [48] presented another system for intrusion detection in Grid and Cloud Computing which has an audit system to detect attacks that network-and host-based systems can’t detect. Figure 5 depicts the architecture of Grid and Cloud Computing Intrusion Detection System (GCCIDS).

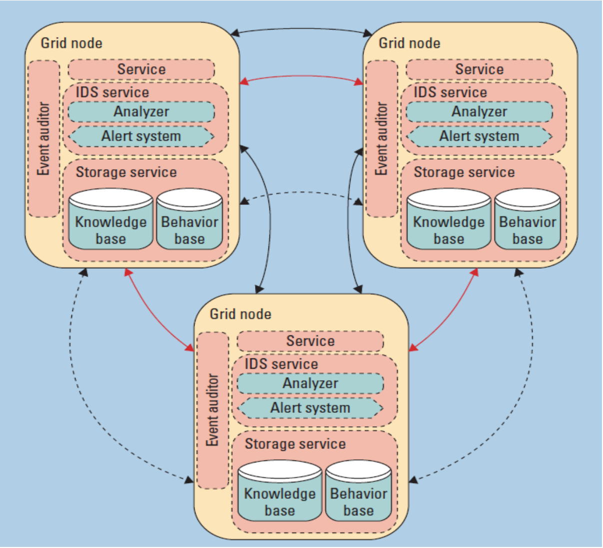

Figure 5: The architecture of grid and cloud computing intrusion detection [48]

In this approach every node has event auditor, service, IDs service and storage service. Event Auditor captures data from various sources, like log system, service, and node messages. After that, IDS service analyzes the captured data and applies the behaviour based detection technique for unknown attacks and knowledge based detection technique for known attacks. The storage service is used to hold the collected data that the IDS service analyses that data. This approach uses artificial neural network (ANN) to detect unknown attacks. When intrusion is detected at any node, then this node sends alerts to other nodes by using alert system.

Behavioural analysis requires a large number of training samples in order to produce very low false positives as well as false negatives and Vieira et al. [48] demonstrated it by his experiments. This approach cannot detect any insider attacks running on virtual machines.

Narwane and Vaikol [49] presented an approaches of HIDS (Host based IDS) which uses Signature based IDS as well as Anomaly based IDS for reducing false positives. Collected information is first filtered with the help of various signatures. Signatures are the evidences of the various attacks. If information will match with any of the evidence, system will detect intrusion and it is verified with the behavioural pattern. If it goes in line with the normal pattern the behaviour is updated. If there is mismatch the system will detects intrusion.

Table 1 shows the summary of all the intrusion detection techniques discussed before.

Table 1 Summary of Intrusion Detection Techniques

Techniques	Characteristics	Limitations
Signature Based Intrusion Detection	• Detection rate is very high for previously known attacks. • Detects attacks by matching the patterns of captured packets with previously acquired patterns.	• For unknown attacks false alarm rate is very high. • Unable to detect new attacks or variants of known attack.
Anomaly Based Intrusion Detection	• Unknown attacks can also be detected. • Low false alarm rate for unknown attacks. • For intrusion detection, behavior of the network is collected and a statistical test is performed.	• This is a Time consuming technique. • A lot of features are required to correctly attack detection.
ANN Based Intrusion Detection	• ANN has ability to generalize data from incomplete data. • More number of hidden layers increases the detection accuracy.	• Learning time is very high. • Requires more number of training samples.
SVM Based Intrusion Detection	• Less training samples are required as compared to ANN based classifier. • Good Generalization ability even for high dimensionality data.	• High training time. • Classification of only discrete features is possible.
Fuzzy Logic Based Intrusion Detection	• Removes the problem of sharp boundary conditions. • Can be used for quantitative features.	• Low detection accuracy. • It can be used in combination of other techniques.
Association Rule Based Intrusion Detection	• Only known attacks can be detected.	• Used only for misuse detection. • Totally unknown attacks can’t be detected.
GA Based Intrusion Detection	• Mainly used to select features for intrusion detection.	• Very complex method. • Generalization is not possible.
Hybrid Techniques for Intrusion Detection	• It is a combination of two or more techniques. • Detection accuracy is very high.	• Computational cost is very high.

4. TYPES OF INTRUSION DETECTION SYSTEM

Cloud Computing is prone to attacks due to its distributed environment. So a solution to the security problems like various attacks in the cloud is Intrusion Detection System (IDS). IDS monitor the activities of the user and track the network traffic then it determines whether the activity is malicious or not. If the activity is malicious IDS generates alarm. IDSs use 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).

4.1 Host based IDS

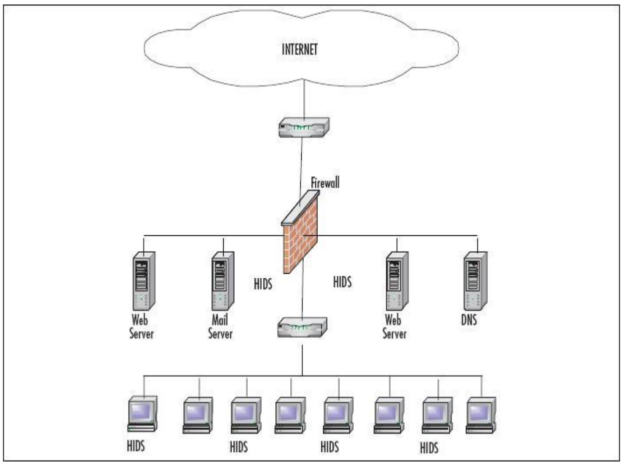

Figure 6: Host Based IDS [50]

Host based Intrusion detection Systems (HIDS) are placed at the specific host machine and monitors the inbound and outbound traffic from the host machine. HIDS monitors dynamic behaviour and internal state of a system. It inspects host specific network packets. HIDS might detect which program accesses which resource in the host and discovers that. 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. Placement of HIDS can be seen in figure 6.

For effective usage of Cloud resources, Lee et al. [51] has proposed a multilevel IDS and log management method. It applies security strength (high, medium, low) to different levels of user behaviour. AAA (Authentication, Authorization and Accounting) is used to manage authentication, authorization and accounting, as shown in figure 7. AAA inspects authenticated user's recently generated information in database and calculates user's anomaly level. After that, that anomaly level is used by AAA to select IDS which has the security level correspondent to that anomaly level. Then, host OS (where selected IDS is installed) is requested by AAA to assign guest OS image to user. Database stores user information, system log, transaction messages between user and system. Storage centre stores user's private data which is kept logically isolated from another user's data so that nobody can access the data except users who have access write. Fast detection mechanism is provided by this approach. Bharadwaja et al. [52] has given an approach which uses host based IDS.

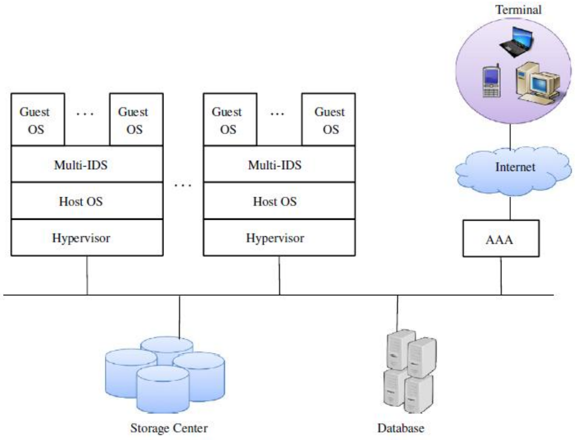

Figure 7: Multi-Level IDS Architecture [51]

4.2 Network based IDS

Network based Intrusion Detection Systems (NIDS) are placed at the key network points like routers and switches. All the traffic passes through the NIDS. 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. Figure 8 shows the placement of the NIDS.

Bakshi and Yogesh [15] 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. An IDS checks the logged packets against predefined rules. An IDS determines nature of attacks and notifies the virtual server about security risk. The virtual server identifies the IP address involved in the attack and drops all the packets received from that IP address. If the identified attack is DDoS, the entire zombie machines will be blocked. Then, virtual server transfers the targeted applications to virtual machine hosted by another data-centre and routing tables are updated immediately. This type of IDS can detect DDoS attack in virtualized environment.

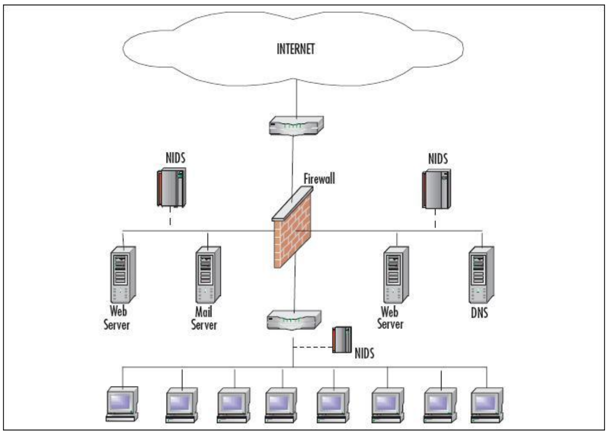

Figure 8: Network Based IDS [50]

Shelke et al. [16] proposed a multithreaded NIDS to handle large amount of data flow through network devices (switch, router) so that packet loss can be reduced. The architecture of this approach contains three modules: capture and queuing module, analysis/processing module and reporting module. The capture module captures the data packets and adds it to the shared queue for analysis. After taking the data packets from shared queue, analysis and process module employees multiple threads to improve the system performance and analyzes it against a predefined signature database. Reporting module prepares the alert reports. A third party monitoring and advisory service informs the user about the attacks. The main advantage of this approach is that, it can process large amount of traffic concurrently without packet loss.

Alharkan and Martin [53] 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.

As seen in the figure 9, the five main components of IDSaaS are; *the Intrusion Engine*: pre-processes the incoming packets and examines their payload section looking for any matching pattern of a threat defined in the loaded attacking rules, *the Output Processor*: increases the performance of the intrusion detection engine by formatting the output log files and inserting them into the Events Database, *the Events Database*: stores the formatted events generated from the Output Processer component, *the Alerts Management*: used as a GUI tool to view the generated alerts and correlate them, allows the security administrator to extract events and relate them to predefined attacking situations and provides the ability to generate reports based on time, source of the attack, or types of threat, and *the Rule-set Manager*: automatically downloads the most up-to-date set of rules from multiple locations.

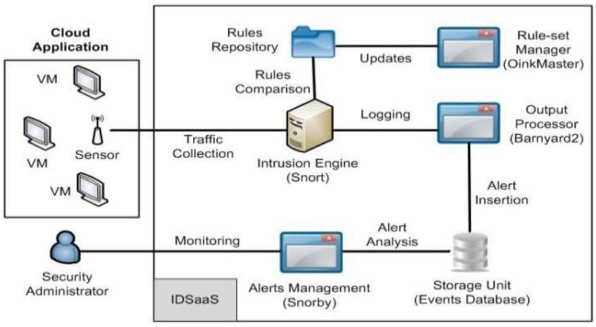

Figure 9: IDSaaS Components [53]

4.3 Distributed IDS

A Distributed Intrusion Detection System (DIDS) 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).

As shown in figure 10 [54], DIDS contains mainly two parts: The Central Analysis Server and The Co-Operative Agent. The Central Analysis Server consists of a database for logging the attack information and a web server. It provides a useful Web Interface to analyze attack information and to perform pre-programmed queries, such as attack aggregation. The agents provide the attack information to the central analysis server. An agent will be placed on different network segments across many physical and geographical locations. Agent machines can use any IDS. The advantages of DIDS are that, the use of multiple agents across a network provides a broader view of network that can't be achieved with single IDS system and it can detect attack patterns across an entire corporate network.

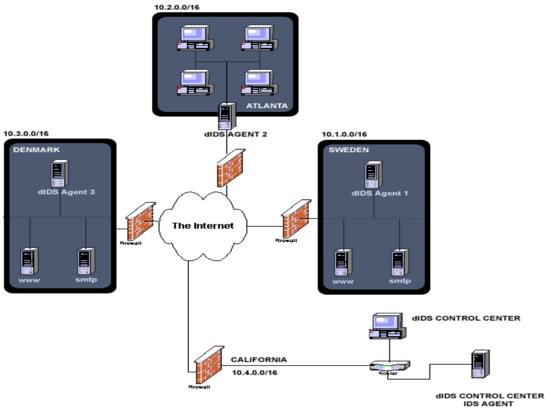

Figure 10: Distributed Intrusion Detection System [54]

Lo et al. [55] proposed a DIDS shown in figure 11 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. This system implements four components; intrusion detection, alert clustering and threshold checking, intrusion response and blocking, cooperative operation. If intrusion is detected by an agent in a region, it drops that packet and sends alert message about that attack to other regions. Alert clustering module is used to collect alerts coming from other regions. The severity of collected alerts is calculated and decision is made whether it is true or false.

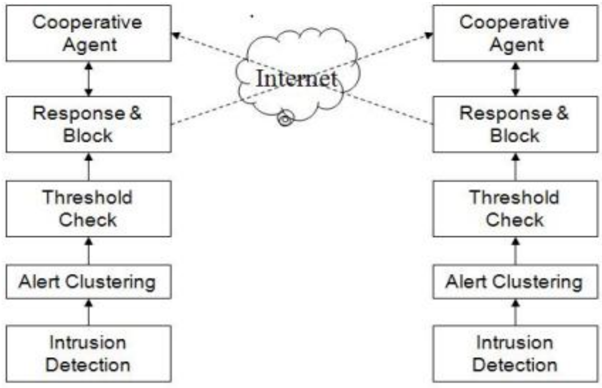

Figure 11: Cooperative IDSs system architecture [55]

4.4 Virtual Machine based IDS

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. [52] 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. In Xen hypervisor, guest operating systems of Virtual Machines (VM) make a resource request to the kernel via hyper-calls which transfers control in the VMM to perform privileged operations. A compromised VM can take control of its VMM so Collabra scans each hyper-call. If it detects any attack, it immediately informs all other VMMs through logical domain channels and notifies the VMM to sanitize that VM so that other VMs on this VMM remain safe. In this type of IDS, the individual VMM based IDS module face the difficulty in identifying the correlation between multiple operations of a correlated attack. This system is useful to detect anomaly based intrusions.

Garfinkel and Rosenblum [21] has given a Virtual Machine introspection based IDS (see figure 12) which is a hypervisor based Intrusion detection system. VMI-IDS isolates the IDS from monitored host, but can look into the host's state. This function (looking into host's state, but remain separate from the host) of VMI-IDS makes it more robust than HIDS as HIDS can't remain separate from the monitored host. VMM (Virtual Machine Monitor) performs the interactions between host software and underlying hardware and performs the hardware virtualization. The architecture of VMI-IDS is divided into two parts; the OS interface library and the policy engine. For easy policy development and implementation, the OS interface library provides an OS-level view of virtual machine's state. With the help of OS interface library and VMM interface, the policy engine executes IDS policies. Policy Engine investigates system state and events from the VMM interface and OS interface library. The communication between VMI-IDS and VMM is facilitated by the VMM interface. It is composed of: UNIX domain socket used by VMI-IDS to send commands and receive response from the VMM, a file to access the physical memory of monitored host. The policy engine is responsible for deciding whether or not the system has been compromised and acts appropriately even if system has been compromised. This VMI-IDS is used for lie detection, signature detection, program integrity detection and row socket detection.

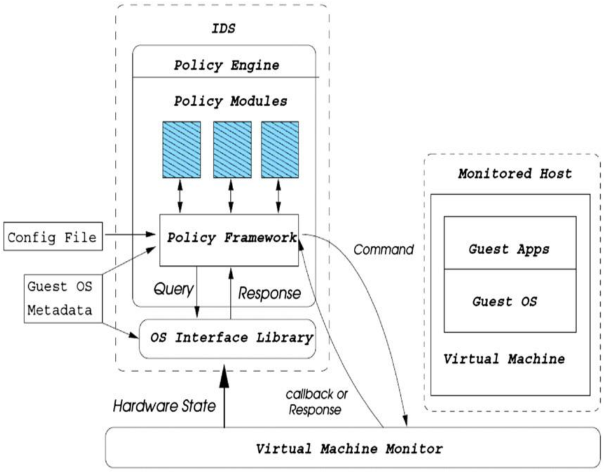

Figure 12: VMI-based IDS architecture [21]

5. CONCLUSION

At the end of above discussion 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. So IDS could be one solution to thwart those attacks. In this paper, we have explored the various IDS techniques and types of IDSs which can be used with cloud computing for security purpose.

6. REFERENCES

[1] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf 2011. NIST SP 500-292, "NIST Cloud Computing Reference Architecture".

[2] Ashley Chonka, Yang Xiang, Wanlei Zhou, Alessio Bonti 2011. "Cloud security defense to protect cloud computing against HTTP-DoS and XML-DoS attacks", Journal of Network and Computer Applications, Vol. 34, Issue 4, pp. 1097-1107.

[3] Rootkit: http://en.wikipedia.org/wiki/Rootkit (Accessed 30 April 2013)

[4] Joanna Rutkowska 2006. "Subverting Vista: Kernel for Fun and Profit", Black Hat Conference. http://blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf (Accessed 30 April 2013)

[5] King, S.T.; Chen, P.M. 2006, "SubVirt: implementing malware with virtual machines", IEEE Symposium on Security and Privacy, pp. 14-327.

http://www.sciencedirect.com/science/article/pii/S1084804510001025

[6] Bahram, S.; Xuxian Jiang; Zhi Wang; Grace, M.; Jinku Li; Srinivasan, D.; Junghwan Rhee; Dongyan Xu 2010. "DKSM: Subverting Virtual Machine Introspection for Fun and Profit", 29th IEEE Symposium on Reliable Distributed Systems, pp. 82-91.

[7] Mohammed H. Sqalli, Fahd Al-Haidari, Khaled Salah 2011. "EDoS-Shield - A Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing", Fourth IEEE International Conference on Utility and Cloud Computing (UCC), pp. 49-56.

[8] W. G. Morein, A. Stavrou, D. L. Cook, A. D. Keromytis, V. Misra, and D. Rubenstein 2003, "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.

[9] S Vivin Sandar, Sudhir Shenai 2012, "Economic Denial of Sustainability (EDoS) in Cloud Services using HTTP and XML based DDoS Attacks", International Journal of Computer Applications (0975 – 8887), Vol. 41, No.20, pp. 11-16.

[10] James C. Foster 2005, "IDS: Signature versus anomaly detection". http://searchsecurity.techtarget.com/tip/IDS-Signature-versus-anomaly-detection

[11] Roschke S., Feng C.,Meinel C. 2009, "Intrusion Detection in the Cloud", Eight IEEE international conference on Dependable, Autonomic and Secure Computing, pp. 729-734.

[12] Modi C, et al. 2012, "A survey of intrusion detection techniques in Cloud", Journal of Network and Computer Applications, http://dx.doi.org/10.1016/j.jnca.2012.05.003

[13] Debar, H., Curry, D., Feinstein, B.: The Intrusion Detection Message Exchange Format, Internet Draft Technical Report, IETF Intrusion Detection Exchange Format Working Group (July 2004).

[14] Lo CC, Huang CC, Ku J. 2008, "Cooperative Intrusion detection system framework for cloud computing networks", 39th IEEE International Conference on Parallel Processing Workshops, pp. 280-284.

[15] Bakshi A.,Yogesh B. 2010, "Securing cloud from DDOS attacks using intrusion detection system in virtual machine", Second IEEE International conference on communication software and networks, pp. 260-264.

[16] Shelke, Ms Parag K., Ms Sneha Sontakke, and A. D. Gawande 2012, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research Volume 1, Issue 4.

[17] Dotan Cohen 2007, "What is a Zero-Day Exploit?" http://what-is-what.com/what_is/zero_day_exploit.html (Accessed 29 April 2013)

[18] Mudzingwa, D.; Agrawal, R. 2012, "A study of methodologies used in intrusion detection and prevention systems (IDPS)", Proceedings of IEEE Southeastcon, pp. 1-6.

[19] Karen Scarfone and Peter Mell 2007, "Guide to Intrusion Detection and Prevention Systems (IDPS)", Computer Security Division, Information Technology Laboratory NIST Gaithersburg.

http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, (Accessed 29 April 2013)

[20] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, E. Vázquez 2009, "Anomaly-based network intrusion detection: Techniques, systems and challenges", Computers & Security, Vol. 28, Issues 1–2, Pages 18-28, ISSN 0167-4048, (http://www.sciencedirect.com/science/article/pii/S0167404808000692)

[21] Garfinkel T, Rosenblum M. 2003, "A Virtual Machine Introspection Based Architecture for Intrusion Detection", In Proc. Network and Distributed Systems Security Symposium 2003, pp. 191–206.

[22] Dastjerdi AV, Bakar KA, Tabatabaei SGH. 2009, "Distributed intrusion detection in clouds using mobile agents", Third international conference on advanced engineering computing and applications in sciences, pp.175-180.

[23] Guan Y, Bao J. 2009, "A CP Intrusion detection strategy on cloud computing", Proceedings of the International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, pp. 084-087.

[24] Moradi M, Zulkernine M. 2004, "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.

[25] Carlos Gershenson 2003, "Artificial Neural Networks for Beginners". http://arxiv.org/ftp/cs/papers/0308/0308031.pdf (Accessed 30 April 2013)

[26] Ibrahim LM. 2010, "Anomaly network intrusion detection system based on distributed time-delay neural network", Journal of Engineering Science and Technology, Vo. 5, Issue: 4, Start page: 457.

[27] Bashah, Idris Bharanidharan Shanmugam, Abdul Manan Ahmed 2005, "Hybrid Intelligent Intrusion Detection System", PROCEEDINGS OF WORLD ACADEMY Of Title SCIENCE, ENGINEERING AND TECHNOLOGY, Vol. 6.

http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.119.8994

[28] Chi Cheng, Wee Peng Tay and Guang-Bin Huang 2012, "Extreme Learning Machines for Intrusion Detection", The 2012 International Joint Conference on Neural Networks (IJCNN), pp. 1-8.

[29] Roshan Chitrakar and Huang Chuanhe 2012, "Anomaly Detection using Support Vector Machine Classification

with k-Medoids Clustering", Third Asian Himalayas International Conference on Internet (AH-ICI), pp. 1-5

[30] Noreen Kausar, BrahimBelhaouari Samir, SuziahBtSulaiman, Iftikhar Ahmad, Muhammad Hussain 2012, "An Approach towards Intrusion Detection using PCA Feature Subsets and SVM", International Conference on Computer & Information Science (ICCIS), PP. 569-574.

[31] Dickerson, J.E., Dickerson, J.A. 2000, "Fuzzy network profiling for intrusion detection", 19th International Conference of the North American Fuzzy Information Processing Society, pp. 301-306.

[32] Dickerson, J.E., Juslin, J., Koukousoula, O., Dickerson, J.A. 2001, "Fuzzy intrusion detection", IFSA World Congress and 20th NAFIPS International Conference, 2001. Joint 9th, pp.1506-1510.

[33] Piyakul Tillapart, Thanachai Thumthawatworn and Pratit Santiprabhob 2002, "Fuzzy Intrusion Detection System", Proc. of 6th World Multiconference on Systemics, Cybernetics and Informatics, pp. 272-276.

[34] Chavan, S., Shah, K., Dave, N., Mukherjee, S., Abraham, A., Sanyal, S. 2004, "Adaptive neuro-fuzzy intrusion detection systems", Proceedings of International Conference on Information Technology: Coding and Computing, pp. 70- 74.

[35] Botha M, Solms R, Perry K, Loubser E,Yamoyany G. 2002, " The utilization of artificial intelligence in a hybrid intrusion detection system", In Proceedings of the 2002 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology, pp. 149-155.

[36] Naqshbandi, Susan M. Al; Samawi, Venus W. 2012, "One-rule Genetic-Fuzzy classifier", IEEE International Conference on Computer Science and Automation Engineering (CSAE), pp. 204-208.

[37] Hong Han; Xin-Liang Lu; Li-Yong Ren; 2004, "Using data mining to discover signatures in network-based intrusion detection", Proceedings of International Conference on Machine Learning and Cybernetics, pp. 13- 17.

[38] Yu-Xin Ding; Hai-Sen Wang; Qing-Wei Liu; 2008, "Intrusion scenarios detection based on data mining", International Conference on Machine Learning and Cybernetics, pp.1293-1297.

[39] Hu Zhengbing; Li ZhiTang; Wu Junqi; 2008, "A Novel Network Intrusion Detection System (NIDS) Based on Signatures Search of Data Mining", First International Workshop on Knowledge Discovery and Data Mining, pp.10-16.

[40] Tian-rui Li; Wu-ming Pan; 2005, "Intrusion detection system based on new association rule mining model", IEEE International Conference on Granular Computing, pp. 512- 515.

[41] Lei Li; De-Zhang Yang; Fang-Cheng Shen; 2010, "A novel rule-based Intrusion Detection System using data mining", 3rd IEEE International Conference on Computer Science and Information Technology, pp.169-172.

[42] Wei Li 2004, "Using Genetic Algorithm for Network Intrusion Detection", In Proceedings of the United States Department of Energy Cyber Security Group Training Conference, pp. 24-27.

[43] 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, pp. 11-17.

[44] WEI LU AND ISSA TRAORE 2004, "DETECTING NEW FORMS OF NETWORK INTRUSION USING GENETIC PROGRAMMING", International Journal on Computational Intelligence, Vol. 20, No. 3, pp. 475-494.

[45] Goyal Anup and Chetan Kumar. 2007, "GA-NIDS: A Genetic Algorithm based Network Intrusion Detection System", not published, Electrical Engineering and Computer Science, Northwestern University, Evanston, IL. http://www.cs.northwestern.edu/~ago210/ganids/GANIDS.pdf (Accessed 30 April 2013)

[46] B. Abdullah, I. Abd-alghafar, Gouda I. Salama, A. Abd-alhafez 2009, "Performance Evaluation of a Genetic Algorithm Based Approach to Network Intrusion Detection System", 13th International Conference on AEROSPACE SCIENCES & AVIATION TECHNOLOGY. http://www.mtc.edu.eg/asat13/pdf/CE14.pdf (Accessed 30 April 2013)

[47] B. Uppalaiah, K. Anand, B. Narsimha, S. Swaraj, T. Bharat 2012, "Genetic Algorithm Approach to Intrusion Detection System", International Journal of Computer Science and Technology, Vol. 3, Issue 1, pp. 156-160.

[48] Vieira, K.; Schulter, A.; Westphall, C.B.; Westphall, C.M. 2010, "Intrusion Detection for Grid and Cloud Computing", IT Professional, vol.12, no.4, pp.38-43.

[49] S.V. Narwane, S. L. Vaikol 2012, "Intrusion Detection System in Cloud Computing Environment", IJCA Proceedings on International Conference on Advances in Communication and Computing Technologies, ICACACT (2):9-17.

[50] http://maltainfosec.org/archives/26-The-concept-of-Intrusion-Detection-Systems.html, 2011

[51] Jun-Ho Lee; Min-Woo Park; Jung-Ho Eom; Tai-Myoung Chung 2011, "Multi-level Intrusion Detection System and log management in Cloud Computing", 13th International Conference on Advanced Communication Technology (ICACT), pp. 552-555.

[52] Bharadwaja, S.; Weiqing Sun; Niamat, M.; Fangyang Shen 2011, "Collabra: A Xen Hypervisor Based Collaborative Intrusion Detection System", Eighth International Conference on Information Technology: New Generations (ITNG), pp. 695-700.

[53] 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, pp. 686 687.

[54] Nathan Einwechter, (updated 2010), "An Introduction to Distributed Intrusion Detection Systems" http://www.symantec.com/connect/articles/introduction-distributed-intrusion-detection-systems (Accessed 30 April 2013)

[55] Lo CC, Huang CC, Ku J. 2008, "Cooperative Intrusion detection system framework for cloud computing networks", 39th IEEE International Conference on Parallel Processing Workshops, pp. 280-284.