Journal of Network and Computer Applications 36 (2013) 42–57

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

A survey of intrusion detection techniques in Cloud

Chirag Modi [a,*], Dhiren Patel [a], Bhavesh Borisaniya [a], Hiren Patel [b], Avi Patel [c], Muttukrishnan Rajarajan [c]

[a] NIT Surat, Gujarat, India
[b] S.P. College of Engineering, Gujarat, India
[c] City University London, UK

ARTICLE INFO

Article history:
Received 3 January 2012
Received in revised form
15 May 2012
Accepted 16 May 2012
Available online 2 June 2012

Keywords:
Cloud computing
Firewalls
Intrusion detection system
Intrusion prevention system

ABSTRACT

In this paper, we survey different intrusions affecting availability, confidentiality and integrity of Cloud resources and services. Proposals incorporating Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in Cloud are examined. We recommend IDS/IPS positioning in Cloud environment to achieve desired security in the next generation networks.

Contents

* Corresponding author. Tel.: +91 9408883560.
E-mail address: cnmodi.956@gmail.com (C. Modi).

1084-8045/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2012.05.003

1. Introduction

Cloud computing aims to provide convenient, on-demand, network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services), which can be rapidly provisioned and released with minimal management effort or service provider interactions (Mell and Grance, 2011). Cloud provides services in various forms: Software as a Service-SaaS (e.g. Google apps, 2011), Platform as a Service-PaaS (e.g. Google app engine (2011)), Microsoft's Azure (Azure services platform, 2011)) and Infrastructure as Service-IaaS (e.g. Amazon web services, 2011(AWS); Eucalyptus, 2011; Open Nebula (Opennebula, 2011)).

As Cloud services are provisioned through the Internet; security and privacy of Cloud services are key issues to be looked upon. International Data Corporation (IDC) survey (Gens, 2009) showed that security is the greatest challenge of Cloud computing. The recent Cloud computing security white paper by Lockheed Martin Cyber Security division (Martin, 2010) shows that the major security concern after data security is intrusion detection and prevention in Cloud infrastructures. Cloud infrastructure makes use of virtualization techniques, integrated technologies and runs through standard Internet protocols. These may attract intruders due to many vulnerabilities involved in it.

Cloud computing also suffers from various traditional attacks such as IP spoofing, Address Resolution Protocol spoofing, Routing Information Protocol attack, DNS poisoning, Flooding, Denial of Service (DoS), Distributed Denial of Service (DDoS), etc. For e.g. DoS attack on the underlying Amazon Cloud infrastructure caused BitBucket.org, a site hosted on AWS to remain unavailable for few hours (Brooks, 2009). Computing-cost using current cryptographic techniques cannot be overlooked for Cloud (Chen and Sion, 2010). Firewall can be a good option to prevent outside attacks but does not work for insider attacks. Efficient intrusion detection systems (IDS) and intrusion prevention systems (IPS) should be incorporated in Cloud infrastructure to mitigate these attacks.

Rest of the paper is organized as follows: Section 2 discusses various attacks applicable to Cloud environment. Traditional firewalls as a security solution are discussed briefly in Section 3. Section 4 presents various techniques for IDS/IPS. Section 5 surveys existing IDS/IPS types and examines Cloud specific work on IDS with conclusion and references at the end.

2. Intrusions to Cloud systems

There are several common intrusions affecting availability, confidentiality and integrity of Cloud resources and services.

2.1. Insider attack

Authorized Cloud users may attempt to gain (and misuse) unauthorized privileges. Insiders may commit frauds and disclose information to others (or modify information intentionally). This poses a serious trust issue. For example, an internal DoS attack demonstrated against the Amazon Elastic Compute Cloud (EC2) (Slaviero, 2009).

2.2. Flooding attack

In this attack, attacker tries to flood victim by sending huge number of packets from innocent host (*zombie*) in network. Packets can be of type TCP, UDP, ICMP or a mix of them. This kind of attack may be possible due to illegitimate network connections.

In case of Cloud, the requests for VMs are accessible by anyone through Internet, which may cause DoS (or DDoS) attack via *zombies*. Flooding attack affects the service's availability to authorized user. By attacking a single server providing a certain service, attacker can cause a loss of availability of the intended service. Such an attack is called direct DoS attack. If the server's hardware resources are completely exhausted by processing the flood requests, the other service instances on the same hardware machine are no longer able to perform their intended tasks. Such type of attack is called indirect DoS attack.

Flooding attack may raise the usage bills drastically as the Cloud would not be able to distinguish between the normal usage and fake usage.

2.3. User to root attacks

Here, an attacker gets an access to legitimate user's account by sniffing password. This makes him/her able to exploit vulnerabilities for gaining root level access to system. For example, Buffer overflows are used to generate root shells from a process running as root. It occurs when application program code overfills static buffer. The mechanisms used to secure the authentication process are a frequent target. There are no universal standard security mechanisms that can be used to prevent security risks like weak password recovery workflows, phishing attacks, keyloggers, etc.

In case of Cloud, attacker acquires access to valid user's instances which enables him/her for gaining root level access to VMs or host.

2.4. Port scanning

Port scanning provides list of open ports, closed ports and filtered ports. Through port scanning, attackers can find open ports and attack on services running on these ports. Network related details such as IP address, MAC address, router, gateway filtering, firewall rules, etc. can be known through this attack. Various port scanning techniques are TCP scanning, UDP scanning, SYN scanning, FIN scanning, ACK scanning, Window scanning etc. In Cloud scenario, attacker can attack offered services through port scanning (by discovering open ports upon which these services are provided).

2.5. Attacks on virtual machine (VM) or hypervisor

By compromising the lower layer hypervisor, attacker can gain control over installed VMs. For e.g. BLUEPILL (Rutkowska, 2006), SubVir (King et al., 2006) and DKSM (Bahram et al., 2010) are some well-known attacks on virtual layer. Through these attacks, hackers can be able to compromise installed-hypervisor to gain control over the host.

New vulnerabilities, such as zero-day vulnerability, are found in Virtual Machines (VMs) (NIST: National vulnerability database, 2011) that attract an attacker to gain access to hypervisor or other installed VMs. Zero-day exploits are used by attackers before the

developer of the target software knows about the vulnerability. A zero-day vulnerability was exploited in the HyperVM virtualization application which resulted in destruction of many virtual server based websites (Goodin, 2009).

2.6. Backdoor channel attacks

It is a passive attack which allows hacker to gain remote access to the infected node in order to compromise user confidentiality. Using backdoor channels, hacker can control victim's resources and can make it as *zombie* to attempt DDoS attack. It can also be used to disclose the confidential data of victim. Due to this, compromised system faces difficulty in performing its regular tasks. In Cloud environment, attacker can get access and control Cloud user's resources through backdoor channel and make VM as *Zombie* to initiate DoS/DDoS attack.

Firewall (in Cloud) could be the common solution to prevent some of the attacks listed above. To prevent attacks on VM/Hypervisor, anomaly based intrusion detection techniques can be used. For flooding attack and backdoor channel attack, either signature based intrusion detection or anomaly based intrusion detection techniques can be used.

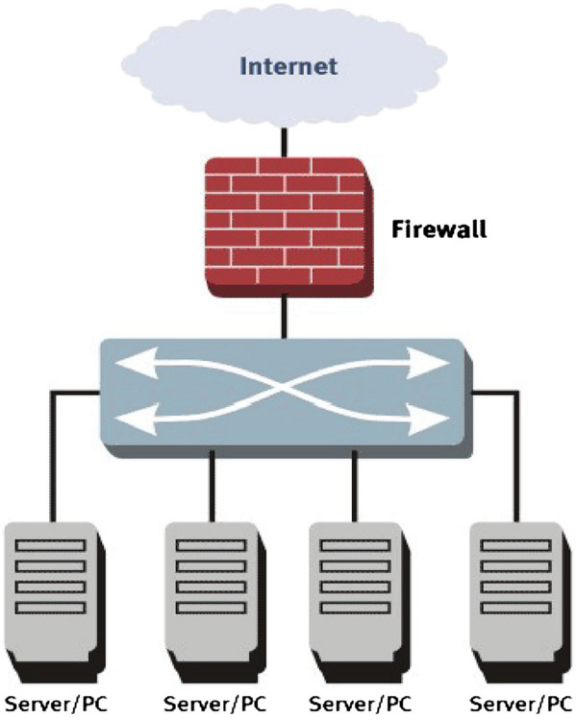

Fig. 1. Basic firewall installation (2011, http://teleco-network.blogspot.com/).

3. Firewalls: common solution to intrusions

Firewall protects the front access points of system and is treated as the first line of defense. Firewalls are used to deny or allow protocols, ports or IP addresses. It diverts incoming traffic according to predefined policy. Basic firewall installation is shown in Fig. 1 (2011, http://teleco-network.blogspot.com/), where it is installed at entry point of servers. Several types of firewalls are discussed in Sequeira (2002).

In Table 1, we summarize different firewalls used in network for security purpose. As firewalls sniff the network packets at the boundary of a network, insider attacks cannot be detected by traditional firewalls. Few DoS or DDoS attacks are also too complex to detect using traditional firewalls. For instance, if there is an attack on port 80 (web service), firewalls cannot distinguish good traffic from DoS attack traffic (2011, http://en.wikipedia.org/wiki/Denial-of-service_attack).

4. IDS and IPS techniques: evolution

Another solution is to incorporate IDS or IPS in Cloud. However the efficiency of IDS/IPS depends on parameters like technique used in IDS, its positioning within network, its configuration, etc. Traditional IDS/IPS techniques such as signature based detection, anomaly detection, artificial intelligence (AI) based detection etc. can be used for Cloud.

4.1. Signature based detection

Signature based intrusion detection attempts to define a set of rules (or signatures) that can be used to decide that a given pattern is that of an intruder. As a result, signature based systems are capable of attaining high levels of accuracy and minimal number of false positives in identifying intrusions. Little variation in known attacks may also affect the analysis if a detection system is not properly configured (Brown et al., 2002). Therefore, signature based detection fails to detect unknown attacks or variation of known attacks. One of the motivating reasons to use signature based detection is ease in maintaining and updating preconfigured rules. These signatures are composed by several elements that identify the traffic. For example, in SNORT (2011, https://www.snort.org/) the parts of a signature are the header

Table 1
Summary of firewalls.

Firewall type	Summary
Static packet filtering firewalls	• Allow/deny packet by inspecting only header information such as source or destination address, port numbers etc. • Do not detect malicious code in packets and cannot prevent against spoofing and fragment attack.
Stateful packet filtering firewalls	• Used in client server environment where client initiates request and server responses which are allowed in bypassing the firewall rules. • Requires additional resources like memory for state tables maintained in hardware or software.
Stateful inspection firewalls	• Enhanced form of stateful packet filtering firewalls. • Used for applications like FTP where multiple ports are used and examine the payload and open or close the ports as per the protocol.
Proxy firewalls	• Can isolate internal network within Internet. Analyze the protocol syntax by breaking up client/server connection. • Require lots of network resources.

(e.g. source address, destination address, ports) and its options (e.g. payload, metadata), which are used to determine whether or not the network traffic corresponds to a known signature. Stiawan et al. (2010) presented some issues regarding signature based intrusion prevention system and showed different possible frameworks.

In Cloud, signature based intrusion detection technique can be used to detect known attack. It can be used either at front-end of Cloud to detect external intrusions or at back end of Cloud to detect external/internal intrusions. Like traditional network, it cannot be used to detect unknown attacks in Cloud. Approaches presented by Roschke et al. (2009), bakshi and Yogesh (2010), Lo et al. (2008), and Mazzariello et al. (2010) use signature based intrusion detection system for detecting intrusions on VMs (or front end of Cloud environment). These approaches are discussed in the later section.

4.2. Anomaly detection

Anomaly (or behavioral) detection is concerned with identifying events that appear to be anomalous with respect to normal system behavior. A wide variety of techniques including data mining, statistical modeling and hidden markov models have been explored as different ways to approach the anomaly detection problem. Anomaly based approach involves the collection of data relating to the behavior of legitimate users over a period of time, and then apply statistical tests to the observed behavior, which determines whether that behavior is legitimate or not. It has the advantage of detecting attacks which have not been found previously. The key element for using this approach efficiently is to generate rules in such a way that it can lower the false alarm rate for unknown as well as known attacks.

Dutkevyach et al. (2007) provided anomaly based solution to prevent intrusion in real time system, which analyzes protocol based attack and multidimensional traffic. However, there is a scope of optimization to reduce number of IPS. Zhengbing et al. (2007) presented lightweight intrusion detection system to detect the intrusion in real-time, efficiently and effectively. In this work, behavior profile and data mining techniques are automatically maintained to detect the cooperative attack.

Anomaly detection techniques can be used for Cloud to detect unknown attacks at different levels. In Cloud, large numbers of events (network level or system level) occur, which makes difficult to monitor or control intrusions using anomaly detection technique. Garfinkel and Rosenblum (2003), Vieira et al. (2010), Dastjerdi et al. (2009) and Guan and Bao (2009) proposed anomaly detection techniques are proposed to detect intrusions at different layers of Cloud.

The ability of soft computing techniques to deal with uncertain and partially true data makes them attractive to be applied in intrusion detection (Moradi and Zulkernine, 2004). There are many soft computing techniques such as Artificial Neural Network (ANN), Fuzzy logic, Association rule mining, Support Vector Machine (SVM), Genetic Algorithm (GA), etc. that can be used to improve detection accuracy and efficiency of signature based IDS or anomaly detection based IDS.

4.3. Artificial neural network (ANN) based IDS

The goal of using ANNs (Han and Kamber, 2006) for intrusion detection is to be able to generalize data (from incomplete data) and to be able to classify data as being normal or intrusive (Ibrahim, 2010). Types of ANN used in IDS are as (Ibrahim, 2010): Multi-Layer Feed-Forward (MLFF) neural nets, Multi-Layer Perceptron (MLP) and Back Propagation (BP).

Cannady (1998) proposed a three layer neural network for misuse detection in network. The feature vector used in Cannady (1998) was composed of nine network features (Protocol ID, Source Port, Destination Port, Source IP Address, Destination IP Address, ICMP Type, ICMP Code, Raw Data Length, Raw Data). However, intrusion detection accuracy is very low. Moradi and Zulkernine (2004) presented MLP based IDS. They showed that inclusion of more hidden layers increase detection accuracy of IDS. This approach improves detection accuracy of the approach proposed in Cannady (1998). Grediaga et al. (2006) compared the rate of successively finding intrusion with MLP and self organization map (SOM) and showed that SOM has high detection accuracy than ANN. It is claimed that, Distributed Time Delay Neural Network (DTDNN) (Ibrahim, 2010) has higher detection accuracy for most of the network attacks. DTDNN is a simple and efficient solution for classifying data with high speed and fast conversion rates. Accuracy of this approach can be improved by combining it with other soft computing techniques mentioned above.

ANN based IDS is an efficient solution for unstructured network data. The intrusion detection accuracy of this approach is based on number of hidden layers and training phase of ANN.

An approach proposed by Vieira et al. (2010), uses ANN based anomaly detection technique for Cloud environment, which requires more training samples as well as more time for detecting intrusions effectively.

4.4. Fuzzy logic based IDS

Fuzzy logic (Han and Kamber, 2006) can be used to deal with inexact description of intrusions.

Tillapart et al. (2002) proposed Fuzzy IDS (FIDS) for network intrusions like SYN and UDP floods, Ping of Death, E-mail Bomb, FTP/Telnet password guessing and port scanning. Evolving fuzzy neural network (EFuNN) is introduced in Chavan et al. (2004) for reducing training time of ANN. It uses mixture of supervised and unsupervised learning. The experimental results shown indicate that using reduced number of inputs EFuNN has better classification accuracy for IDS than only using ANN. The approaches proposed by Tillapart et al. (2002) and Chavan et al. (2004) cannot be used in real time for detecting network intrusions as the training time is significant by more. Fuzzy association rules presented by Su et al. (2009 are used to detect network intrusion in real time. Two rule sets are generated and mined online from training data. Features for comparison are taken from network packet header. This approach is used for large scale DoS/DDoS attacks.

To reduce training time of ANN (Vieira et al., 2010), fuzzy logic with ANN can be used for fast detection of unknown attacks in Cloud.

4.5. Association rule based IDS

Some intrusion attacks are formed based on known attacks or variant of known attacks. To detect such attacks, signature apriori algorithm (Han et al., 2002) can be used, which finds frequent subset (containing some features of original attack) of given attack set.

Han et al. (2002) proposed network based intrusion detection using data mining technique. In this approach, signature based algorithm generates signatures for misuse detection. However, drawback of the proposed algorithm is its time consumption for generating signatures. Zhengbing et al. (2008) solved the database scanning time problem examined in Han et al. (2002). They proposed scanning reduction algorithm to reduce number of database scans for effectively generating signatures from previously known attacks. However, it has very high false positive alarm rate since unwanted patterns are produced. Lei et al. (2010)

proposed length decreasing support based apriori algorithm to detect intrusions to reduce production of short pattern as derived by Han et al. (2002) and Zhengbing et al. (2008) and allows some interesting patterns. It is faster than other apriori based approaches.

In Cloud, association rules can be used to generate new signatures. Using newly generated signatures, variations of known attacks can be detected in real time.

4.6. Support vector machine (SVM) based IDS

SVM (Han and Kamber, 2006) is used to detect intrusions based on limited sample data, where dimensions of data will not affect the accuracy.

In Chen et al. (2005), it is shown that the results (regarding false positive rate) are better in case of SVM compared with that of ANN, since ANN requires large amount of training samples for effective classification, whereas SVM has to set fewer parameters. However, SVM is used only for binary data. Nevertheless, detection accuracy can be improved by combining SVM with other techniques (Li and Lu, 2010). Li and Lu, 2010 designed an intelligent module for network intrusion prevention system with a combination of SNORT and configurable firewall. The SVM classifier is also used with SNORT to reduce false alarm rate and improve accuracy of IPS.

In Cloud, if limited sample data are given for detecting intrusions, then use of SVM is an efficient solution; since dimensions of data are not affecting accuracy of SVM based IDS.

4.7. Genetic algorithm (GA) based IDS

Genetic algorithms (GAs) (Dhanalakshmi and Ramesh Babu, 2008; Li, 2004) are used to select network features (to determine optimal parameters) which can be used in other techniques for achieving result optimization and improving accuracy of IDS.

Gong et al. (2005) used seven features (Duration, Protocol, Source_port, Destination_port, Source_IP, Destination_IP, Attack_name) of captured packet. They used support confidence based framework for fitness function, which is simple and flexible. Generated rules are used to detect network intrusions. The paper uses quantitative as well as categorical features of network for generating classification rules. This increases the detection rate and improves accuracy. However, limitation of this approach is the best fit problem. Lu and Traore (2004) presented GP based approach to generate rules from network features. They used support confidence based fitness function for deriving rules, which classifies network intrusions effectively. However, training period for the fitness function takes more time. Xiao et al. (2005) proposed information theory and GA based approach that is used to detect abnormal behavior. It identifies small number of network features closely with network attacks based on mutual information between network features and type of intrusion. However, this approach only considers discrete features. Dhanalakshmi and Ramesh Babu (2008) proposed a method which is used to detect misuse and anomaly by combining fuzzy and genetic algorithms. Fuzzy is used to include quantitative parameters in intrusion detection, whereas genetic algorithm is used to find best fit parameters of introduced numerical fuzzy function. This approach solves best fit problem as reported by Lu and Traore (2004).

In Cloud environment, selection of optimal parameters (network features) for intrusion detection will increase the accuracy of underlying IDS. For that, Genetic algorithm (GA) based IDS can be used in Cloud.

4.8. Hybrid techniques

Hybrid techniques use the combination of two or more of above techniques.

As shown in Fig. 2 (Botha et al., 2002), NeGPAIM is based on hybrid technique combining two low level components including fuzzy logic for misuse detection and neural networks for anomaly detection, and one high level component which is a central engine analyzing outcome of two low level components. It is an effective model, which does not require dynamic updates of rules.

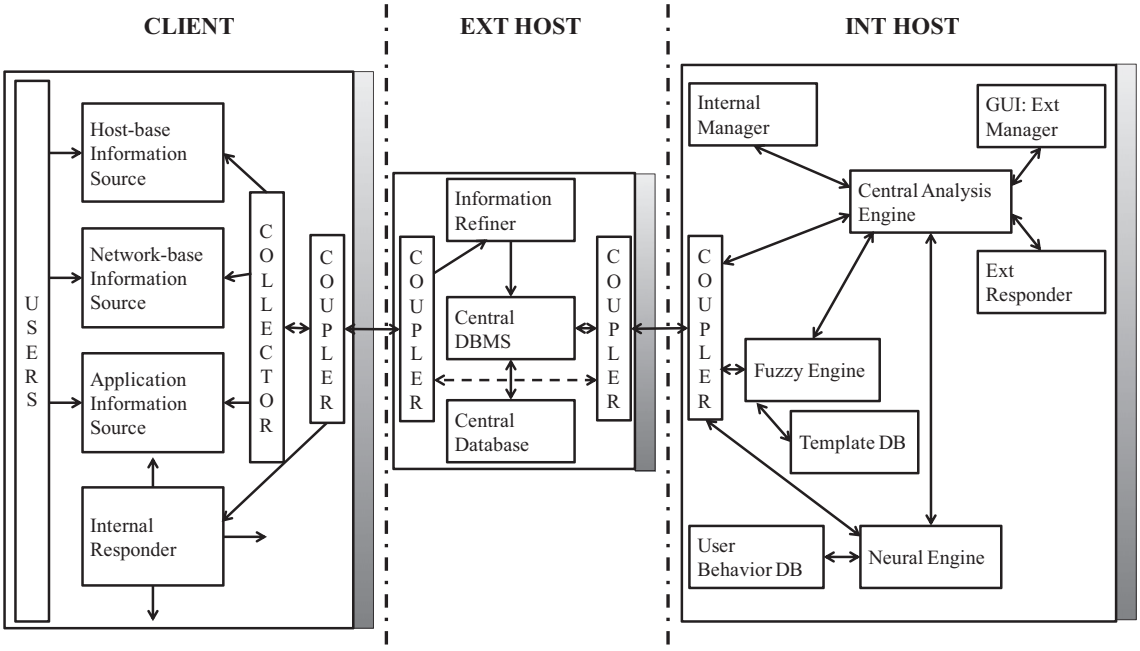

Fig. 2. Architecture of NeGPAIM (Botha et al., 2002).

To improve performance of IDS, Katar (2006) presented an approach which uses combination of Naïve Bayes, ANN and Decision Tree (DT) classifiers on three separate sets of data input. Independent output of each classifier is generated and combined using the multiple fusion techniques. This approach uses the advantages of each classifier and improves overall performance of IDS.

It is advantageous to use soft computing techniques on traditional IDS for Cloud environment. However, each technique has some advantages and limitations, which affect the performance of IDS. For e.g. Higher time consumption to learn ANN network and lesser flexibility are the major drawbacks of ANN. Combining fuzzy logic to data mining techniques improves flexibility. GA with fuzzy logic enhances performance of IDS, since GA selects best fit rules for IDS. GA has better efficiency for matching patterns but in specific manner rather than general (Beg et al., 2010). For handling large number of network features, SVM is preferable. Association rule based IDS is efficient for only correlated attacks. However, an efficiency of association rule based IDS depends on the used knowledge base.

In Table 2, a summary of existing IDS/IPS techniques is presented with their strengths and limitations.

5. Various types of IDS/IPS used in Cloud computing

There are mainly four types of IDS used in Cloud: Host based intrusion detection system (HIDS), Network based intrusion detection system (NIDS), Hypervisor based intrusion detection system and Distributed intrusion detection system (DIDS).

5.1. Host based intrusion detection systems (HIDS)

HIDS monitors and analyzes the information collected from a specific host machine. HIDS detects intrusion for the machine by collecting information such as file system used, network events, system calls, etc. HIDS observes modification in host kernel, host file system and behavior of the program. Upon detection of deviation from expected behavior, it reports the existence of attack. The efficiency of HIDS depends on chosen system characteristics to monitor. Each HIDS detects intrusion for the machines in which it is placed as shown in Fig. 3.

With respect to Cloud computing, HIDS can be placed on a host machine, VM or hypervisor to detect intrusive behavior through monitoring and analyzing log file, security access control policies, and user login information. If installed on VM, HIDS should be monitored by Cloud user whereas in case of installing it on Hypervisor, Cloud provider should monitor it (cox, 2011).

HIDS based architecture for Cloud environment is proposed by (Vieira et al., 2010). In this architecture, each node of Grid/Cloud contains IDS which provides interaction among service offered (e.g. IaaS), IDS service and storage service. As shown in Fig. 4 (Vieira et al., 2010), IDS service is composed of two components: Analyzer and Alert System.

The event auditor captures data from various resources like system logs. Based on the data received from event auditor, the IDS service is used for detecting intrusion by using behavior based technique or knowledge based technique. Knowledge based technique is used to detect known attacks, whereas the behavior based technique is used to detect unknown attacks. For detecting unknown attacks, artificial neural network (ANN) is used in this approach. When any attack or intrusion is detected, alert system informs other nodes. So, this approach is efficient even for detecting unknown attacks by applying feed forward ANN.

The experiments demonstrated by Vieira et al. (2010) show that the false positive and false negative alarm rate is very low when large numbers of training samples are applied for behavior analysis method. The limitation of this approach is that it cannot detect any insider intrusions which are running on VMs.

For effective usage of Cloud resources, multilevel IDS and log management (Lee et al., 2011) is applied at different level of

Table 2
Summary of IDS/IPS techniques.

IDS/IPS technique	Characteristics/advantages	Limitations/challenges
Signature based detection	• Identifies intrusion by matching captured patterns with preconfigured knowledge base. • High detection accuracy for previously known attacks. • Low computational cost.	• Cannot detect new or variant of known attacks. • High false alarm rate for unknown attacks.
Anomaly detection	• Uses statistical test on collected behavior to identify intrusion. • Can lower the false alarm rate for unknown attacks.	• More time is required to identify attacks. • Detection accuracy is based on amount of collected behavior or features.
ANN based IDS	• Classifies unstructured network packet efficiently. • Multiple hidden layers in ANN increase efficiency of classification.	• Requires more time and more samples training phase. • Has lesser flexibility.
Fuzzy Logic based IDS	• Used for quantitative features. • Provides better flexibility to some uncertain problems.	• Detection accuracy is lower than ANN.
Association rules based IDS	• Used to detect known attack signature or relevant attacks in misuse detection.	• It cannot detect totally unknown attacks. • It requires more number of database scans to generate rules. • Used only for misuse detection.
SVM based IDS	• It can correctly classify intrusions, if limited sample data are given. • Can handle massive number of features.	• It can classify only discrete features. So, preprocessing of those features is required.
GA based IDS	• It is used to select best features for detection. • Has better efficiency.	• It is complex method. • Used in specific manner rather than general.
Hybrid techniques	• It is an efficient approach to classify rules accurately.	• Computational cost is high.

security strength (e.g. high, medium, and low) to user based on the degree of anomaly. As shown in Fig. 5, AAA is used for authentication, authorization and accounting. Authenticated user's information (stored in database) is used to calculate anomaly level. AAA uses anomaly level to select proper IDS that has corresponding security level. Then host OS (where selected IDS is installed) is requested to assign guest OS image to user. Database stores user information, system log, transaction of user and system, whereas storage center stores user's private data which are isolated from one user to another. This approach provides fast detection mechanism. However, it requires more guest OSs (having IDS) for high level users.

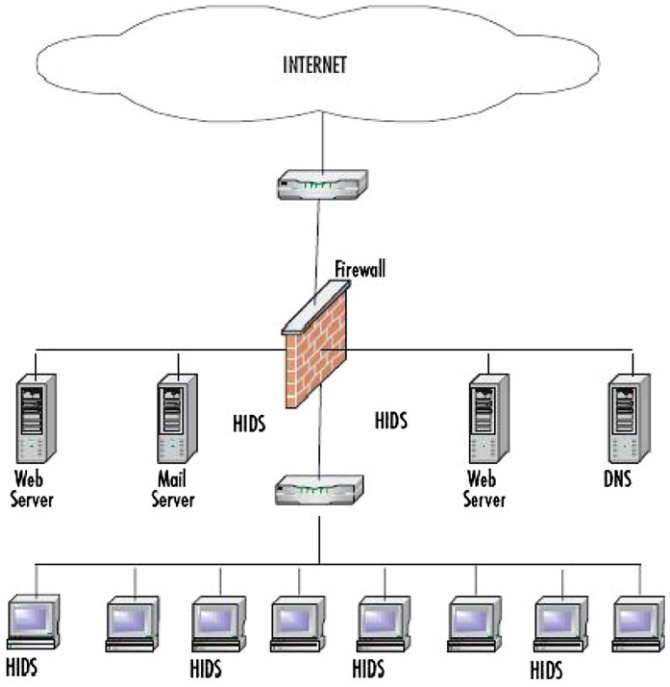

Fig. 3. Host based intrusion detection system (HIDS) (2011, http://maltainfosec.org/archives/26-The-concept-of-Intrusion-Detection-Systems.html).

Guan and Bao (2009) have proposed change point based idea to detect all types of attacks in attack space. In this approach, all attacks are taken as a sample space. Then the set is decomposed using statistics based on mutually exclusive sets. The generated subsets which belong to sample space are used to construct intrusion detection algorithm. However, no experimental results or deployment mechanisms are reported yet.

In self-similarity based lightweight intrusion detection method for Cloud Computing (Kwon et al., 2011), the number of events from the Windows' security event log is extracted. Feature selection procedure makes groups by combining security ID (SID) and EventID in Windows system. Then each VM measures self-similarity. Self-similarity is calculated using two techniques viz; cosine and hybrid (Kwon et al., 2011). If calculated similarity deviated from normal behavior, IDS generates alerts. Outlier source procedure identifies intruder and associated IP address. Then IDS reports the information to a system administrator. This approach is cost effective and efficient for detecting anomaly in Cloud environment. However, it works only for Windows system.

Arshad et al. (2011) proposed an abstract model for intrusion detection and severity analysis to provide the overall security of the Cloud. It consists of six components viz; system call handler, detection module, security analysis module, profile engines, global components and intrusion response system. System call handler collects system calls executed by guest VM. Detection module applies anomaly or signature based techniques to collected system calls for detecting intrusions in VM. Severity analysis module calculates severity of detected intrusion for victim VM. Profile engine generates and manages profiles specific

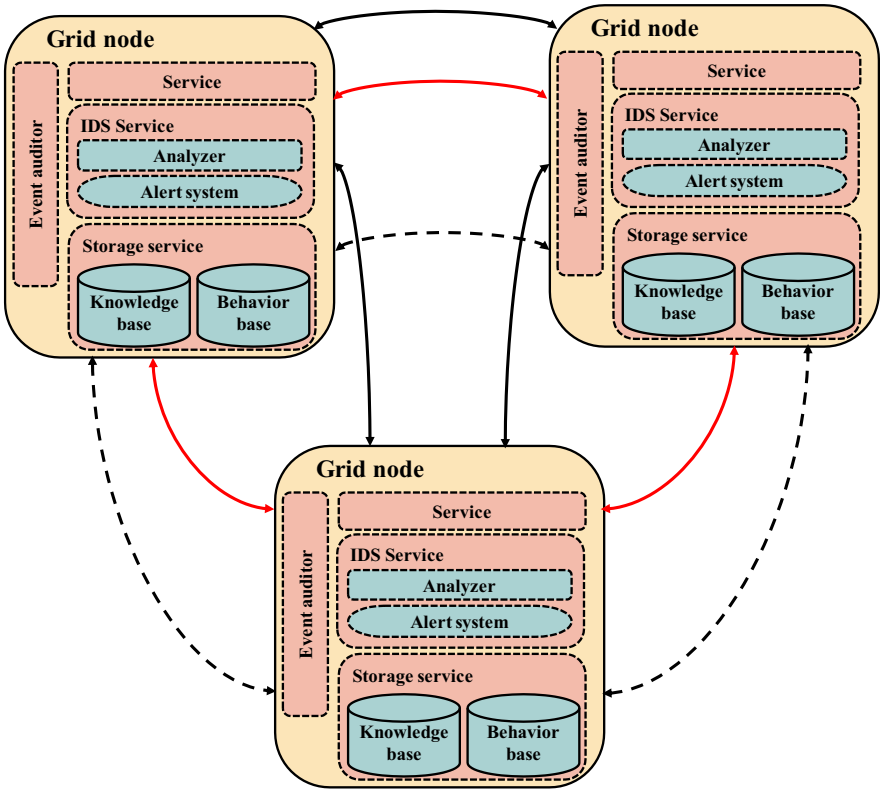

Fig. 4. IDS architecture for Grid/Cloud environment (Vieira et al., 2010).

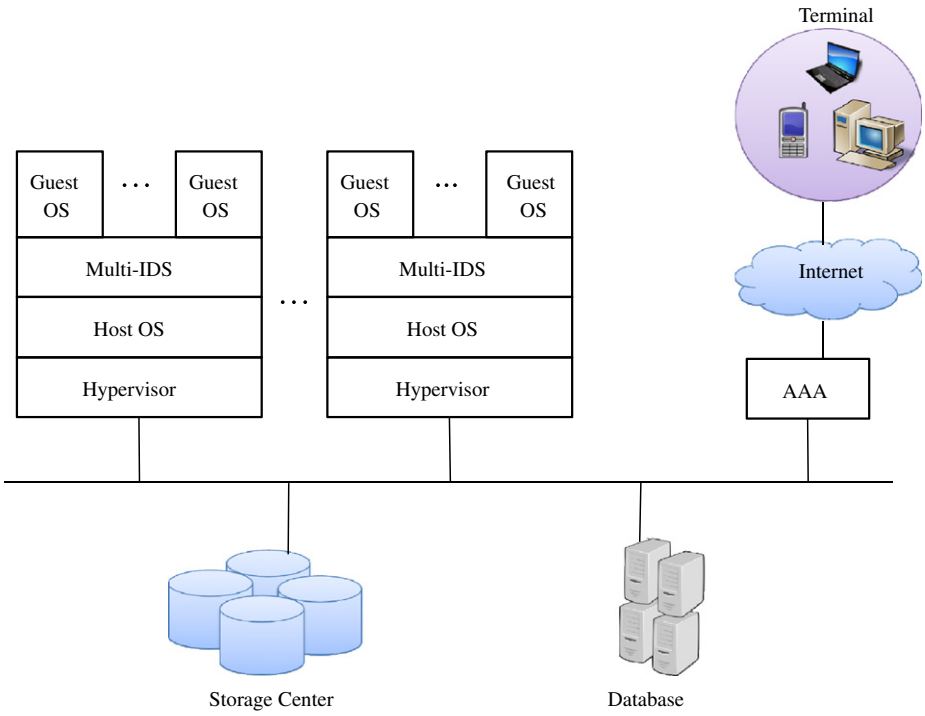

Fig. 5. Multilevel IDS architecture (Lee et al., 2011).

to VM. These profiles are used for differentiating malicious behavior and normal behavior of user. Global components are used for overall infrastructure including resource manager, scheduler, profile and other security components. Intrusion response system is used to select appropriate response mechanism for a particular intrusion. This approach has minimal response time and human intervention. However, experimental results are not evaluated.

5.2. Network based intrusion detection system (NIDS)

NIDS monitors network traffic to detect malicious activity such as DoS attacks, port scans or even attempts to crack into computers. The information collected from network is compared with known attacks for intrusion detection. NIDS has stronger detection mechanism to detect network intruders by comparing current behavior with already observed behavior in real time. NIDS mostly monitors IP and transport layer headers of individual packet and detects intrusion activity. NIDS uses signature based and anomaly based intrusion detection techniques. NIDS has very limited visibility inside the host machines. If the network traffic is encrypted, there is no effective way for the NIDS to decrypt the traffic for analysis.

Hemairy et al. (2009) surveyed about the security solutions that can be applicable to detect ARP spoofing attacks through experiments and implementation. They concluded that XArp 2 tool (2011, http://www.filecluster.com/Network-Tools/Network-Monitoring/Download-XArp.html) is an efficient available security solution that can accurately detect ARP spoofing attacks among other tools. By combining it to ARP request storm and ARP scanning detection mechanism, its performance can be improved.

Fig. 6 represents positioning of NIDS in a typical network with aim to direct the traffic through the NIDS. NIDS placed between firewall and various hosts of the network.

NIDS can be deployed on Cloud server interacting with external network, for detecting network attacks on the VMs and hypervisor. However, it has several limitations. It cannot help when attack is within a virtual network that runs entirely inside the hypervisor. In Cloud environment, installing NIDS is the responsibility of Cloud provider.

VM compatible IDS architecture proposed by Roschke et al. (2009) is shown in Fig. 7. There are mainly two components used in this approach: IDS management unit and IDS sensor.

IDS management unit consists of event gatherer, event database, analysis component and remote controller. Event gatherer collects malicious behavior identified by IDS sensor and stores in event database. Event database stores information regarding captured events. Analysis component (configured by users) accesses event database and analyze events. IDS-VMs are managed by the IDS Remote Controller which can communicate with IDS-VMs and IDS sensors. IDS sensors on the VM detects and reports malicious behavior and transmits triggered event to event gatherer. Sensors can be NIDS configured by IDS remote controller. In this approach, new sensors can be easily integrated, which require only sender/receiver pair to connect event gatherer. IDS-VM management controls, monitors and configures VM. The VM management can also recover VMs. This approach is used in virtualized environment to prevent VMs from being compromised. However, this approach requires multiple instances of IDS.

In the approach proposed (bakshi and Yogesh, 2010), for detecting DDoS attack in VM, IDS is installed in virtual switch to log incoming or outgoing traffic into database. To detect known attacks, the logged packets are analyzed and compared by the IDS in real time with known signature. The IDS determines nature of attacks and notifies virtual server. Then virtual server drops packets coming from the specified IP address. If attack type is DDoS, all the zombie machines are blocked. The virtual server then transfers targeted applications to other machines hosted by separate data center and routing tables are immediately updated. Firewall (placed at new server) blocks all the packets coming from identified IP address. This approach can block the DDoS attack in virtualized environment and can secure services running on virtual machines.

Mazzariello and Bifulco (2010) presented SNORT based misuse detection in open source Eucalyptus Cloud. In this approach, SNORT is deployed at Cloud controller (CC) as well as on physical machines (hosting virtual machines) to detect intrusions coming from external network. This approach solves the problem of deploying multiple instances of IDS as in bakshi and Yogesh (2010). It is a fast and cost effective solution. However, it can detect only known attacks since only SNORT (2011, https://www.snort.org/) is involved.

Hamad and Hoby (2012) proposed a method for providing intrusion Detection as a Service in Cloud, which delivers Snort for Cloud clients in a service-based manner. Fig. 8 shows subscription and IDS operation request of Cloud intrusion detection service (CIDS). User request related to his subscription details is forwarded to the database layer, whereas the IDS operation requests are forwarded to the system layer. The system layer and the database layer can communicate with each other to translate preferences (that exist in the database layer) into runtime-configurations that are used at the system layer. The limitation of this service is that it can detect only known attacks at network level.

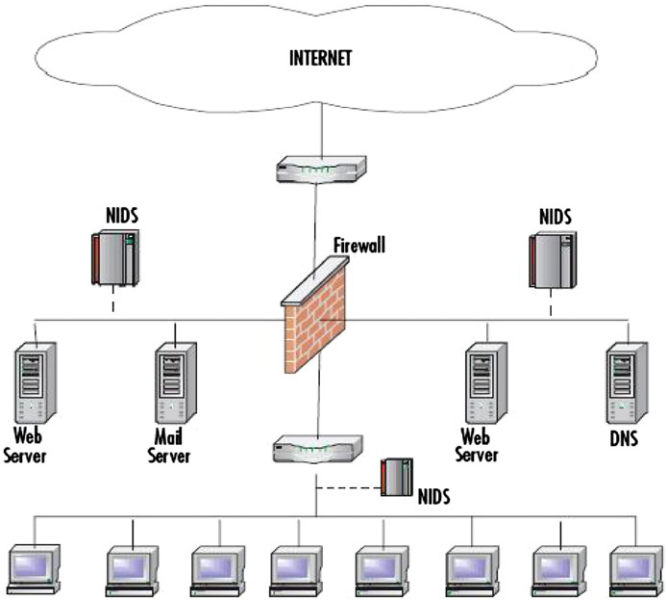

Fig. 6. Network based intrusion detection system (2011, http://maltainfosec.org/archives/26-The-concept-of-Intrusion-Detection-Systems.html).

Sandar and Shenai (2012) introduced new type of DDoS attack, called Economic Denial of Sustainability (EDoS) in Cloud services and proposed solution framework for EDoS protection. EDoS attack can be called as HTTP and XML based DDoS attack. EDoS protection framework uses firewall and puzzle server to detect EDoS attack. Firewall is used to detect EDoS at entry point of Cloud, where as puzzle server is used to authenticate user. In this work, authors demonstrated EDoS attack in the Amazon EC2 Cloud. However, proposed solution is not efficient since it uses only traditional firewall. Research is still needed to detect EDoS attack in Cloud.

Houmansadr et al. (2011) proposed Cloud based intrusion detection and response system for mobile phones. In this approach, intrusion detection and response services are delivered to registered smartphones. It copies smartphone to VM in Cloud using proxy that copies incoming traffic to device. This traffic is used for intrusion detection. If any intrusion is detected, intrusion response mechanism selects an action for detected intrusion and sends a non-intrusive software agent in the device.

5.3. Distributed intrusion detection system (DIDS)

A Distributed IDS (DIDS) consists of several IDS (e.g. HIDS, NIDS, etc.) over a large network, all of which communicate with each other, or with a central server that enables network monitoring. The intrusion detection components collect the system information and convert it into a standardized form to be passed to central analyzer. Central analyzer is machine that aggregates information from multiple IDS and analyzes the same. Combination of anomaly and signature based detection approaches are used for the analysis purpose. DIDS can be used for detecting known and unknown attacks since it takes advantages of both the NIDS and HIDS (Jones and Sielken, 2000). Fig. 9, demonstrates the working of DIDS.

In Cloud environment, DIDS can be placed at host machine or at the processing server (in backend).

In cooperative agent based approach (Lo et al., 2008), individual NIDS module is deployed in each Cloud region as shown in Fig. 10 (Lo et al., 2008). If any Cloud region detects intrusions, it alerts other region. Each ID sends alert to each other, to judge severity of this alert. If new attack is detected, the new blocking rule is added to block list. So, this type of detection and prevention helps to resist attacks in Cloud.

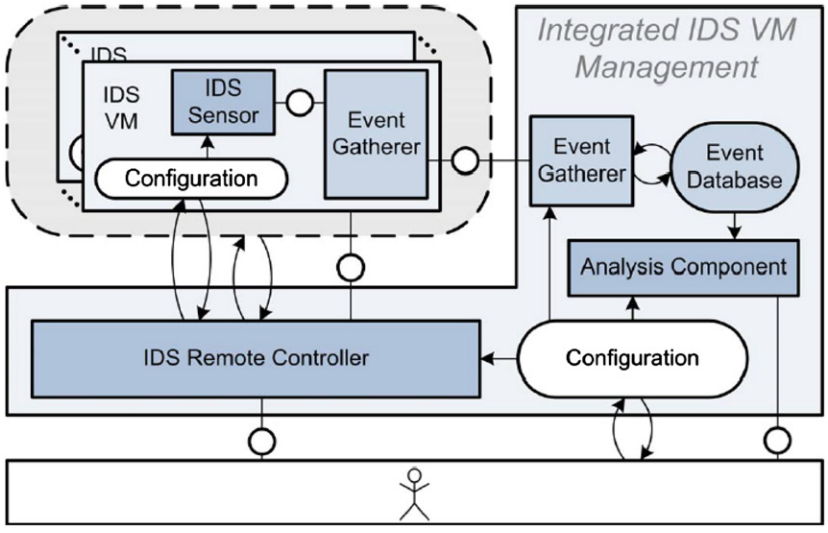

Fig. 7. Architecture of VM integrated IDS management (Roschkeet al., 2009).

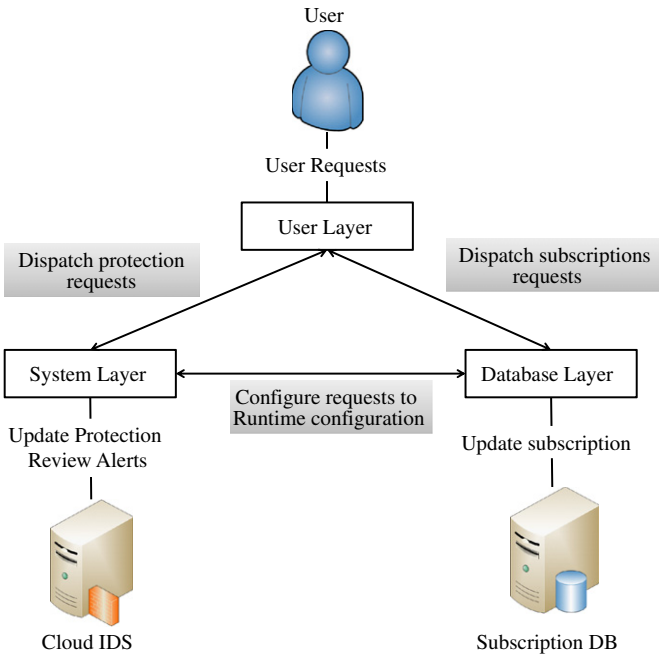

Fig. 8. Intrusion detection as a service in Cloud (Hamad and Hoby, 2012).

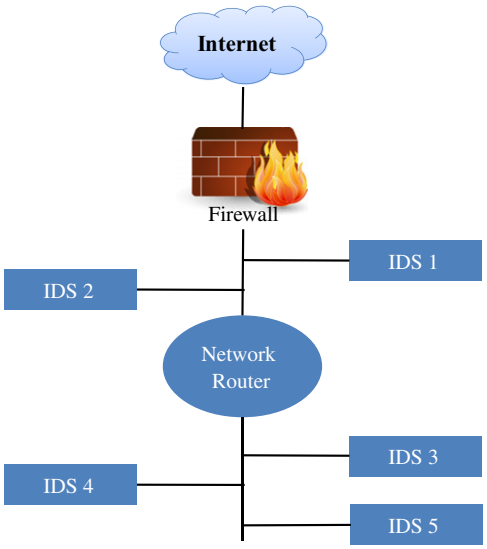

Fig. 9. Distributed intrusion detection system (DIDS).

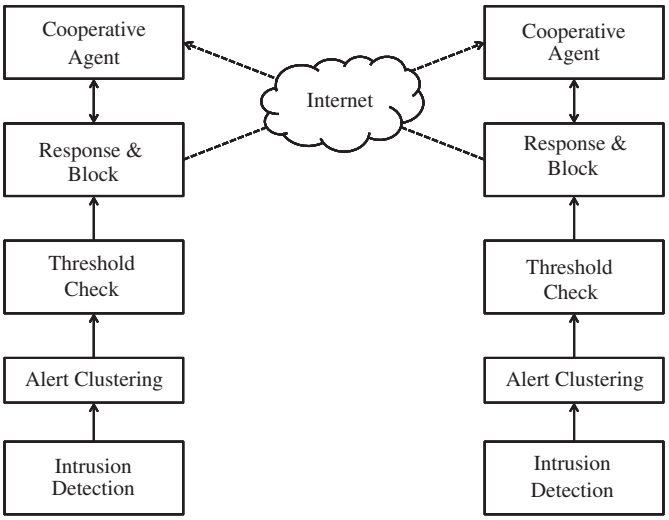

Fig. 10. Block diagram of cooperative agent based approach (Lo et al., 2008).

The system architecture consists of intrusion detection, alert clustering, threshold check, intrusion response and blocking and cooperative agent. In case of intrusion detection, it drops attacker packet, then sends alert message about the attack detected by itself to other region. Alert clustering module collects alert produced by other regions. The decision about alert (whether it is true or false) is identified after calculating severity of collected alerts. This approach is suitable for preventing Cloud system from single point of failure caused by DDoS attack.

Dastjerdi and Bakar (2009) proposed scalable, flexible and cost effective method to detect intrusion for Cloud applications regardless of their locations using mobile agent. This method aims for protecting VMs that are outside the organization. Mobile agent collects evidences of an attack from all the attacked VM for further analysis and auditing. This approach is used to detect intrusion in VM migrated outside the organization. However, it produces more network load.

Ram (2012) proposed mutual agent based approach to detect DDoS attack in Cloud computing. In this approach, IDS module is deployed in each Cloud region, as presented by Lo et al. (2008). If any region finds intrusion, mutual agent at that region notifies other regions. Each region calculates severity of alerts generated from other regions. If new attack is found after calculating severity of intrusion, new blocking rule is added into block table at each region. In such a way, DDoS attack is detected in whole Cloud by using mutual cooperation among Cloud regions. For intrusion detection, Snort is used in this approach. Therefore, known attacks in network can be detected. However, it cannot detect unknown attack. Also, it requires high computation cost for exchanging alerts.

5.4. *Hypervisor-based intrusion detection system*

Hypervisor is a platform to run VMs Hypervisor-based intrusion detection system is running at hypervisor layer. It allows user to monitor and analyze communications between VMs, between hypervisor and VM and within the hypervisor based virtual network. Availability of information is one of the benefits of hypervisor-based IDS.

VM introspection based IDS (Garfinkel and Rosenblum, 2003) is one of the examples of hypervisor based intrusion detection system. Hypervisor based IDS is one of the important techniques, specifically in Cloud computing, to detect intrusion in virtual environment.

Virtual machine introspection based IDS (VMI-IDS) architecture is shown in Fig. 11 (Garfinkel and Rosenblum, 2003). VMI-IDS is different from traditional HIDS since it directly observes hardware states, events and software states of host and offers more robust view of the system than HIDS. Virtual machine monitor (VMM) is responsible for hardware virtualization and also offers isolation, monitoring and interposition properties. VMI-IDS has greater access to the VMM than the code running in monitored VM.

VMM interface is used for VMI-IDS to communicate with VMM, which allows VMI-IDS to get VM state information, monitoring certain events and controlling VMs. This VMM interface is composed of Unix socket to send commands or receive responses to/from VMM. It also supports physical memory access of monitored VM. OS interface library is used to provide low level machine states from VMM in terms of higher level OS structure. Policy engine is incorporated for making high-level queries about the OS of monitored host. Policy engine responds in appropriate manner, even if system is compromised. VMI-IDS implements

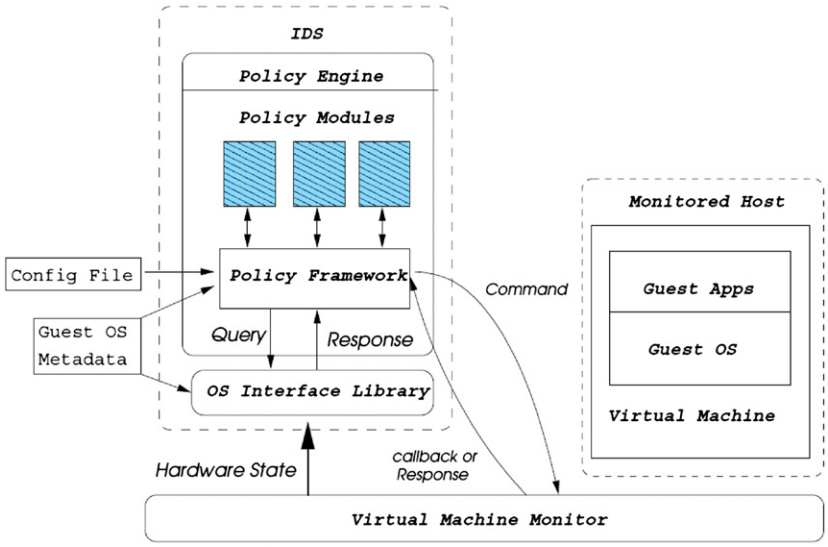

Fig. 11. VMI-based IDS architecture (Garfinkel and Rosenblum, 2003).

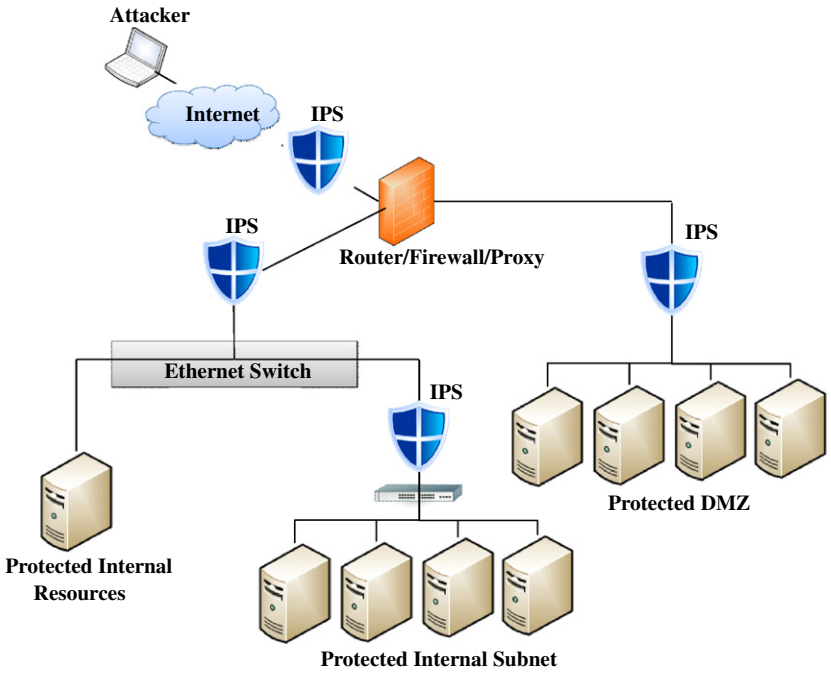

Fig. 12. Network based intrusion prevention system (2011, http://www.javvin.com/networksecurity/IPS.html).

complex anomaly detection. It is used for lie detection, signature detection, program integrity detection and row socket detection. According to results shown by (Garfinkel and Rosenblum, 2003), performance of policy engine is good in terms of workload and time. However, VMM or OS library can be compromised.

Recently IBM Research is pursuing virtual machine introspection approach to create a layered set of security services inside protected VM running on same physical machine as the guest VMs running in the Cloud (2011, http://www.zurich.ibm.com/csc/security/securevirt.html#top).

5.5. Intrusion prevention system (IPS)

IPS monitors network traffic and system activities to detect possible intrusions (With the help of IDS) and dynamically responds to intrusions for blocking the traffic or quarantine it. IPS should be configured accurately for expected results; otherwise it stops flow of packets resulting in network unavailability. For intrusion prevention, mostly firewall with IDS is used which contains signature specifying network traffic rules. Based on the preconfigured rules, IPS decides whether network traffic should be passed or blocked. In response to detected attack, IPS can stop the attack itself, can change the attack contents or change security environment.

Ahmed et al. (2009) proposed efficient network based intrusion detection and prevention approach, which does not require installing IDS on every node. This approach solves trust problem and transferring alert message problem. It has less overhead and no false alarm rate. Leu and Li (2009) proposed Cumulative-Sum-based Intrusion Prevention System (CSIPS) for preventing DoS or DDoS attacks. In this work, authors used packet classification algorithm and three detection algorithms (namely inbound,

outbound, and forwarded) which cooperatively detect DDoS attack and send their logs to remote IPS machine.

IPSs are mainly classified into two categories: Host based IPS (HIPS) and Network based IPS (NIPS). The possible positioning of IPS in a typical network is shown in Fig. 12.

In Cloud computing architecture, HIPS can be used to detect and prevent intrusion on VM, Hypervisor or host system where it is deployed. NIPS can be used to protect the whole network (or part of network) to safeguard multiple systems (such as VMs) at a time.

Fagui et al. (2009) presented Xen based host system firewall and its extensions. In this approach, Netfilter and Iptables are used to build firewall on host Linux system which inspects network data. Netfilter is the framework which Linux kernel implements. Iptables is a firewall management program based on Netfilter framework. As shown in Fig. 13 (Fagui et al., 2009), Iptables extensions consist of two parts: First part is interacting with Iptables application layer which is developed as shared library and second part is Iptable kernel developed as kernel dynamic library. Kernel dynamic library is uploaded at runtime. Moreover, a firewall GUI is used to configure firewall rules. Iptables application extension is used for authentication of rules configured by users and to parse the parameters of the rules. Each rule filled in data structure supplied by Iptables. Iptable kernel extension uploaded dynamically when the firewall is running. It is developed based on Netfilter/Iptables. When network packet goes through HOOK, HOOK function is called.

The HOOK function identifies whether the data packet matches the preconfigured rules or not and returns the result to kernel which will decide to accept or to drop the packet. General data structure then transferred to HOOK function which transforms data structure to another structure defined as Iptable application module. Also pointer to skb buffer storing the packet information is transferred to

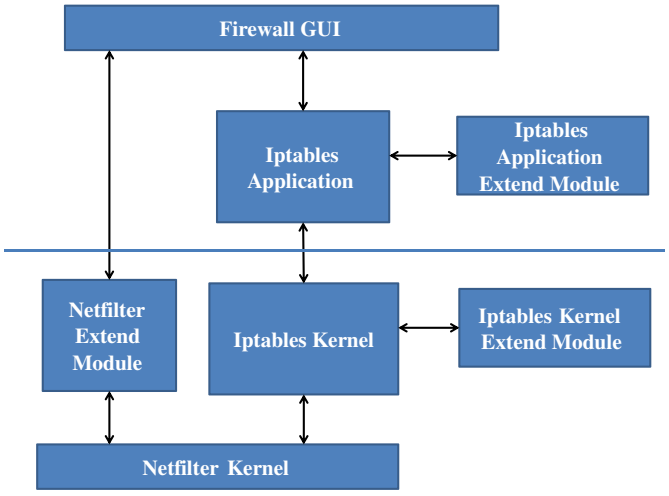

Fig. 13. The architecture of Xen based firewall and its extension (Fagui et al., 2009).

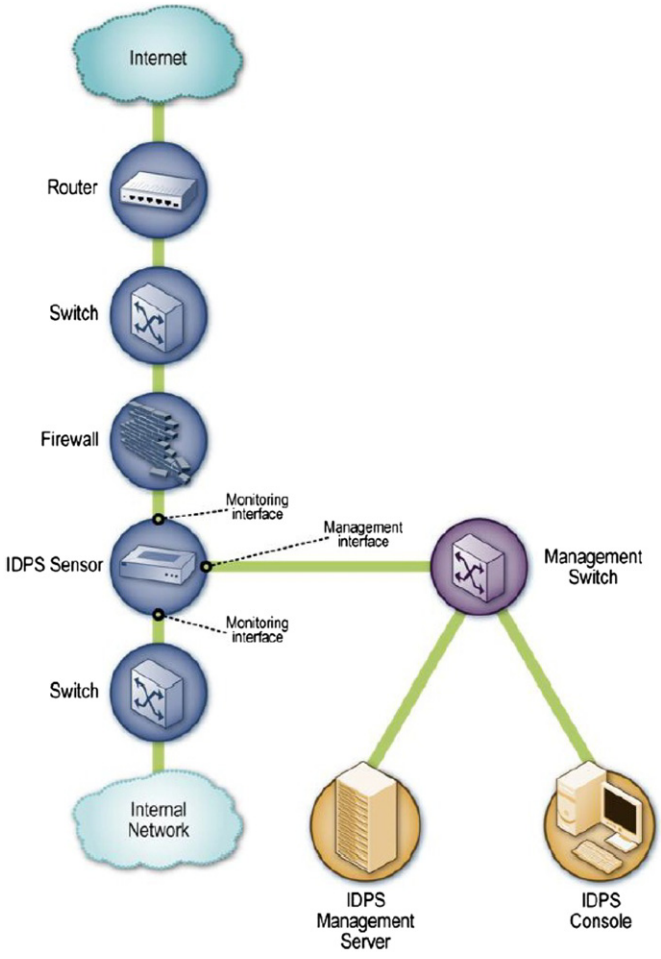

Fig. 15. Positioning IDPS in network (Scarfone and Mell, 2007).

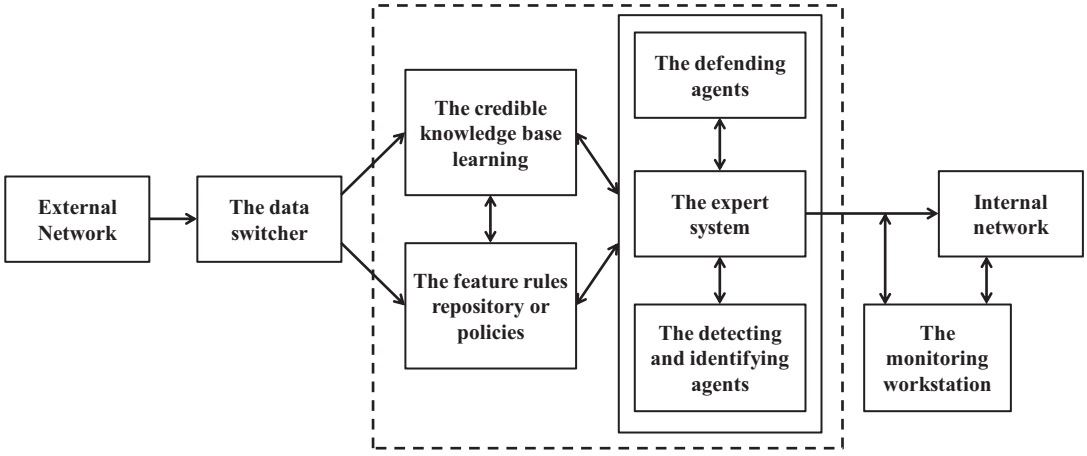

Fig. 14. Architecture of dynamic intelligence Cloud firewall (Jia and Wang, 2011).

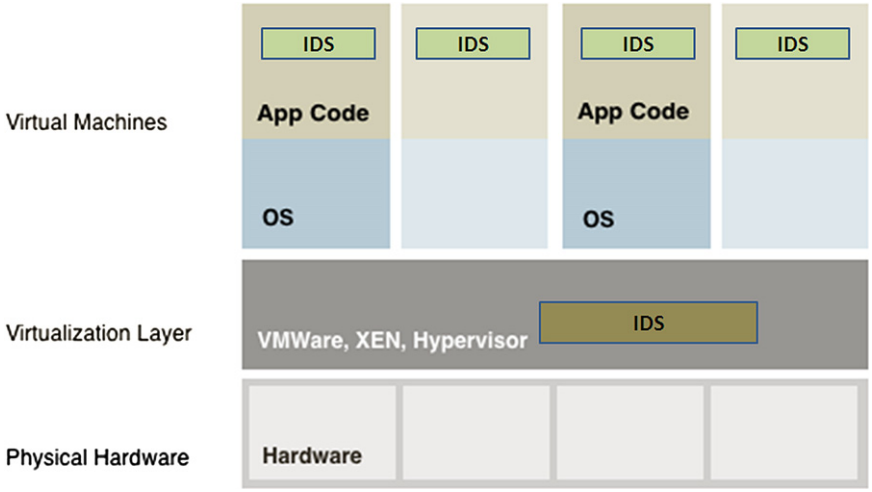

Fig. 16. Placement of IDS on VMs and hypervisor/host system.

Table 3
Summary of IDS/IPS types.

IDS/IPS Type	Characteristics/strengths	Limitations/Challenges	Positioning in Cloud	Deployment and monitoring authority
HIDS	• Identify intrusions by monitoring host's file system, system calls or network events. • No extra hardware required.	• Need to install on each machine (VMs, hypervisor or host machine). • It can monitor attacks only on host where it is deployed.	On each VM, Hypervisor or Host system.	On VMs: Cloud Users. On Hypervisor: Cloud provider.
NIDS	• Identify intrusions by monitoring network traffic. • Need to place only on underlying network. • Can monitor multiple systems at a time.	• Difficult to detect intrusions from encrypted traffic. • It helps only for detecting external intrusions. • Difficult to detect network intrusions in virtual network.	In external network or in virtual network.	Cloud provider.
Hypervisor based IDS	• It allows user to monitor and analyze communications between VMs, between hypervisor and VM and within the hypervisor based virtual network.	New and difficult to understand.	In hypervisor.	Cloud provider.
DIDS	• Uses characteristics of both NIDS and HIDS, and thus inherits benefits from both of them.	• Central server may be overloaded and difficult to manage in centralized DIDS. • High communication and computational cost.	In external network, on Host, on Hypervisor or on VM.	On VMs: Cloud Users. For other cases: Cloud provider.
IPS	• Prevents intrusion attacks. • NIPS prevent network attacks. • HIPS prevent system level attacks.	• Detection accuracy for preventing attacks is lower than IDS.	For NIPS: In external/internal network. For HIPS: On VM or Hypervisor.	NIPS: Cloud provider. HIPS on VM: Cloud user. HIPS on Hypervisor: Cloud provider.
IDPS	• Effectively detect and prevent intrusion attacks.	• Complex architecture.	Network based IDPS: In external/internal network. Host based IDPS: On VM or hypervisor.	NIDPS: Cloud provider. HIDPS (on VM): Cloud user. HIDPS (on Hypervisor): Cloud provider.

HOOK function to identify the rules irrespective of the rules matching the data. The skb buffer saves the data of the packet, such as source IP address, destination port number, which is captured when it goes through the HOOK. However, Unknown attacks cannot be prevented by this approach.

Jia and Wang (2011) designed an IPS model based on dynamically distributed Cloud firewall linkage. Authors introduced the structure and function of Cloud firewall. As shown in Fig. 14, external information is trained using data switcher through credible database. Then this information is learned

Table 4
Summary of existing IDS approaches in Cloud

Title	IDS type	Technique used	Positioning	Pros	Cons
IDS architecture for Cloud environment (Vieira et al., 2010)	HIDS	Signature based and Anomaly detection using ANN.	On each node	False rate for unknown attack is lower since ANN used.	Requires more training time and samples for detection accuracy.
Multi-level IDS (Lee et al., 2011)	HIDS	Anomaly detection	On each Guest OS	Provides fast detection mechanism.	Requires more resources for high level users.
Self-similarity based IDS (Kwon et al., 2011)	HIDS	Anomaly detection	On each VM	Can be used in real time.	Works only for Windows system.
Abstract model of IDS (Arshad et al., 2011)	HIDS	Signature based and anomaly detection	On each VM	It has minimal response time and human intervention.	Experimental results are not evaluated.
VM compatible IDS architecture (Roschke et al., 2009)	NIDS	Signature based detection	On each VM	Secures VM based on user configuration.	Multiple instances of IDS are required which degrades performance.
DDoS attack detection in virtual machine (bakshi and Yogesh, 2010)	NIDS	Signature based detection	On each VM	Secures VM from DDoS attacks.	Can only detects known attacks.
NIDS in open source Cloud (Mazzariello et al., 2010)	NIDS	Signature based detection	On traditional network	Can detect several known attacks.	It cannot detect insider attacks as well as unknown attacks.
IDS as a Service (Hamad and Hoby, 2012)	NIDS	Signature based detection	Snort is provided as a web service	Provides user to detect known attack on his/her running service.	It cannot detect unknown attacks.
EDoS protection (Sandar and Shenai, 2012)	NIDS	Signature based detection	On traditional network	Blocks HTTP and XML based DDoS attack.	It cannot detect unknown attacks.
Cloud based IDS for mobile phones (Houmansadr et al., 2011)	NIDS	Anomaly detection	On VM	Detects malicious behavior on smartphones.	It cannot be used as general purpose.
Cooperative agent based approach (Lo et al., 2008)	DIDS	Signature based detection	On each Cloud region	Prevents system from single point failure.	Cannot be used for all types of attacks.Computational overhead high.
Mobile agent based approach (Dastjerdi et al., 2009)	DIDS	Anomaly detection	On each VM	Provides IDS for Cloud application regardless by their location.	Produce network load with increase of VMs attached to mobile agent.
Mutual agent based approach (Ram, 2012)	DIDS	Signature based detection	On each Cloud region	Detects DDoS attack in whole cloud environment.	Cannot be used to detect unknown attacks.High computational cost.
VMI-IDS based architecture (Garfinkel and Rosenblum, 2003)	Hypervi-sor based	Anomaly detection.	On hypervisor	Detects attacks on VMs	VMI IDS can be attacked. Very complex method
Xen based Host system firewall (Fagui et al., 2009)	-	Prevention	On each Host	Prevention using user configured rules	Not used for preventing unknown attacks
IPS model based on cloud firewall linkage (Jia and Wang, 2011)	HIPS	Anomaly prevention.	In internal network	Can be used for real time interactive defense and better optimization to Cloud firewall	Experimental results are not yet available
CP based approach (Guan and Bao, 2009)	-	Anomaly detection	-	Used to detect all types of attacks. Solves limitation of computing time	Experimental results are not yet available

using knowledge base and compared with predefined rules or policies. Rules or policies are generated by using data mining techniques. The defending agents, expert system, and the detecting and identifying agents are used for real time defense, detection of intrusions and identification. If the intrusions are detected, the monitor station calls defending filter, prevention and generates alerts, then give auditing record. The monitoring work station is used to monitor internal intrusions. An intelligent IPS module based on dynamically distributed Cloud firewall linkage is used for real time interactive defense and better optimization of Cloud firewall. When user of internal network accesses external network resources, IPS uses feature detection and recognition mode of Cloud security for analyzing and deciding safety of resources which are accessed by users. It uses expert system used in Cloud firewall. In this approach user's behaviors, files, web pages etc are used for calculating resources' reputation and detecting intrusions. Experimental results of this approach are not evaluated.

5.6. Intrusion detection and prevention system (IDPS)

Having their own strengths and weaknesses, individual IDS and IPS are not capable of providing full-fledged security. It is very effective to use combination of IDS and IPS, which is called IDPS. Apart from identifying possible intrusions, IDPS stops and reports them to security administrators (Scarfone and Mell, 2007). Proper configuration and management of IDS and IPS combination can improve security. NIST (Scarfone and Mell, 2007) explained how intrusion detection and prevention can be used together to strengthen security, and also discussed different ways to design, configure, and manage IDPS.

IDPS is classified into three broad categories: Signature-based, anomaly-based, and stateful protocol analysis. There are many types of IDPS technologies. IDPS are divided into four groups based on the type of events that they monitor and the ways in which they are deployed (Scarfone and Mell, 2007): (a) Network-Based (b) Wireless (c) Network Behavior Analysis (NBA) (d) Host-Based. Positioning of network based IDPS in typical network is shown in Fig. 15 (Scarfone and Mell, 2007).

Considering the Cloud scenario, network-based IDPS can be used to protect multiple VMs from network end points. Host-based IDPS can be deployed at VMs or hypervisors to protect the machines on which it is placed.

Concluding the whole section, we now graphically represent positioning of various types of IDS/IPS (mentioned above) in the different layers of Cloud architecture. Fig. 16 demonstrates the same followed by its summary.

Incorporating IDS on VM allows monitoring the activity of VM itself. Cloud user should be held responsible to deploy, manage and monitor IDS on VM. Placing IDS on underlying hypervisor provides ability to detect intrusion activity including communication between VMs on that hypervisor. However large amount

of communicating data reduces performance of IDS or causes packet dropping. Deploying, managing and monitoring IDS should be done by Cloud provider. The virtual network (established in host system) allows VMs to communicate directly without using external network. IDS can be located within such network to monitor traffic between the VMs as well as between the VM and host. Cloud provider can be given duties to manage IDS. IDS can be deployed in external network, which is a door to Cloud system for users. It allows monitoring of network traffic over the traditional network. Cloud provider should be the proper entity to serve here. Summary of various IDSs are shown in Table 3.

In Tables 4, we summarize presented approaches with their type, technique, positioning in Cloud, pros and cons. This illustrates several challenges which need to be addressed before a standard security framework for the Cloud can be proposed.

6. Conclusions

We discussed several intrusions which can threat integrity, confidentiality and availability of Cloud services. Firewall only may not be sufficient to solve Cloud security issues. This paper emphasized the usage of alternative options to incorporate intrusion detection and intrusion prevention techniques into Cloud and explored locations in Cloud where IDS/IPS can be positioned for efficient detection and prevention. Recent research findings incorporating IDS/IPS in Cloud have been discussed with their advantages and disadvantages. The adoption of soft computing techniques in IDS/IPS can improve the security. We finally identify several security challenges that need to be addressed by the research community to make Cloud a secure and trusted platform for the delivery of future Internet of Things.

References

Azure services platform, Website, 〈http://www.microsoft.com/azure〉; 2011.

Amazon web services, Website, 〈http://aws.amazon.com〉; 2011.

Arshad J, Townend P, Xu J. An abstract model for integrated intrusion detection and severity analysis for clouds. International Journal of Cloud Applications and Computing 2011;1(1):1–17.

Ahmed M., Pal, R., Hossain, H.M., Bikas, M., Hasan, M.K., NIDS: A Network Based Approach to Intrusion Detection and Prevention, Computer Science and Information Technology—Spring Conference;2009: pp. 141–4.

Brooks C, Amazon EC2 Attack Prompts Customer Support Changes. Tech Target, 〈http://searchcloudcomputing.techtarget.com/news/article/0,289142,sid201_gci1371090,00.html〉; 2009.

Bahram S, Jiang X, Wang Z, Grace M. DKSM: subverting virtual machine introspection for fun and profit.In: Proceedings of the 29th IEEE international symposium on reliable distributed systems; 2010.

Brown DJ, Suckow B, Wang T, A Survey of Intrusion Detection Systems. Department of Computer Science, University of California, San Diego; 2002.

Bakshi A, Yogesh, B. Securing cloud from DDOS attacks using intrusion detection system in virtual machine. In: Second international conference on communication software and networks; 2010: pp. 260–4.

Botha M, Solms R, Perry K, Loubser E, Yamoyany G. The utilization of artificial intelligence in a hybrid intrusion detection system. SAICSIT 2002:149–55.

Beg S, Naru1 U, Ashraf M, Mohsin S. Feasibility of intrusion detection system with high performance computing: a survey. International Journal for Advances in Computer Science 2010;1(1).

Chen Y, Sion R. On securing untrusted clouds with cryptography. In WPES 2010;10: 109–14.

Cannady J. Artificial neural networks for misuse detection, National Information Systems Security Conference, 1998.

Chavan S, Shah K, Dave N, Mukherjee S, Adaptive neuro-fuzzy intrusion detection systems, IEEE international conference on information technology: coding and computing (ITCC'04); 2004: pp 70–4.

Chen W-H, Su S-H, Shen H-P. Application of svm and ann for intrusion detection. Computer Oper Res 2005;32(10):2617–34.

Dutkevyach T, Piskozub A, Tymoshyk, N. Real-time intrusion prevention and anomaly analyze system for corporate networks. In: Fourth IEEE workshop on intelligent data acquisition and advanced computing systems: technology and applications, 2007. IDAACS 2007: 2007: pp. 599–602.

Dastjerdi AV, Bakar KA, Tabatabaei SGH. Distributed intrusion detection in clouds using mobile agents. In: Third international conference on advanced engineering computing and applications in sciences, 2009. ADVCOMP '09; 2009: pp. 175–180.

Dhanalakshmi Y, Ramesh Babu I. Intrusion detection using data mining along fuzzy logic and genetic algorithms. International Journal of Computer Science & Security 2008;8(2):27–32.

Eucalyptus, Website, 〈http://eucalyptus.cs.ucsb.edu/〉; 2011.

Fagui Liu L, Xiang S Wenqianl Su, L. The design and application of xen-based host system firewall and its extension. In: The 2009 international conference on electronic computer technology; 2009: pp. 392–5.

Google apps, Website, 〈http:/www.google.com〉; 2011.

Google app engine, Website, 〈http://code.google.com/appengine/〉; 2011.

Gens F, New IDC IT Cloud Service Survey: Top Benefits and Challenges, IDC Exchange, 〈http://blogs.idc.com/ie/?p=730〉; 2009.

Goodin, D, Webhost Hack Wipes Out Data for 100,000 Sites, 〈http://www.theregister.co.uk/2009/06/08/webhost_attack/〉; 2009.

Garfinkel T, Rosenblum M. A Virtual Machine Introspection Based Architecture for Intrusion Detection. Proc. Network and Distributed Systems Security Symposium 2003:191–206.

Guan Y, Bao J. A CP Intrusion detection strategy on cloud computing, in international symposium on web information systems and applications (WISA); 2009: pp 84–7.

Grediaga A, Ibarra F, García F, Ledesma B, Brotons F. Application of neural networks in network control and information security. LNCS 2006:208–13.

Gong RH, Zulkernine M, Abolmaesumi P. A software implementation of a genetic algorithm based approach to network intrusion detection. In: Proceedings of the sixth international conference on software engineering, artificial intelligence, networking and parallel/distributed computing and first ACIS international workshop on self-assembling wireless networks (SNPD/SAWN'05); 2005.

Han J, Kamber M. Data mining concepts and techniques. 2nd edition Morgan Kaufmann Publishers; 2006.

Han H, Lu XL, Ren LY.Using data mining to discover signatures in network-based intrusion detection. In: Proceedings of the first international conference on machine learning and cybernetics, Beijing (1) (2002).

Hemairy MA, Amin S, Trabelsi Z. Towards more sophisticated ARP Spoofing detection/prevention systems in LAN networks. In: International conference on the current trends in information technology (CTIT); 2009: pp. 1–6.

Hamad H, Hoby MA. Managing intrusion detection as a service in cloud networks. International Journal of Computer Applications 2012;41(1):35–40.

Houmansadr A, Zonouz SA, Berthier, R, Cloud-based, A. Intrusion detection and response system for mobile phones. In: Proceedings of the 2011 IEEE/IFIP 41st international conference on dependable systems and networks workshops; 2011: pp. 31–2.

Ibrahim LM. Anomaly network intrusion detection system based on distributed time-delay neural network. Journal of Engineering Science and Technology 2010;5(4):457–71.

Jones AK, Sielken RS. Computer system intrusion detection: a survey, 〈http://www.cs.virginia.edu/~jones/IDS-research/Documents/jones-sielken-survey-v11.pdf〉; 2000.

Jia T, Wang X. The research and design of intelligent IPS model based on dynamic cloud firewall linkage. International Journal of Digital Content Technology and its Applications 2011;5(3):304–9.

King S, Chen P, Wang Y-M. SubVirt: Implementing malware with virtual machines. In: 2006 IEEE symposium on security and privacy; 2006: pp 314–27.

Katar C. Combining multiple techniques for intrusion detection. International Journal of Computer Science & Network Security 2006;6(2B):208–18.

Kwon H, Kim,T, Yu, SJ, Kim HK. Self-similarity based lightweight intrusion detection method for cloud computing. In: Proceedings of the third international conference on intelligent information and database systems—Volume Part II; 2011: pp. 353–62.

Lo CC, Huang CC, Ku J. Cooperative Intrusion detection system framework for cloud computing networks. In: First IEEE International Conference on Ubi-Media Computing; 2008: pp. 280–4.

Lei L, Yang D-Z, Shen F-C. A Novel rule based Intrusion Detection system using Data Ming. 3rd IEEE International Conference on Computer Science and Information Technology 2010;6:169–72.

Li H, Liu D. Research on intelligent intrusion prevention system based on snort. International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE), 2010;1:251–3.

Li W. A genetic algorithm approach to network intrusion detection.USA: SANS Institute; 2004.

Lu W, Traore I. Detecting new forms of network intrusion using genetic programming. Computational Intelligence 2004;20(3):475–94.

Lee, J-H, Park M-W, Eorn J-H, Chung T-M. Multi-level Intrusion detection system and log management in cloud computing. In: 13th International conference on advanced communication technology (ICACT); 2011, pp. 552–5.

Leu FY, Li ZY. Detecting DoS and DDoS attack using an intrusion detection and remote prevention system. Fifth International Conference on Information Assurance and Security 2009;2:251–4.

Mell P, Grance T, The NIST definition of cloud computing (draft), NIST, 〈http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf〉 ; 2011.

Martin L, White Paper, 〈http://www.lockheedmartin.com/data/assets/isgs/documents/CloudComputingWhitePaper.pdf〉; 2010.

Mazzariello C, Bifulco R, Canonoco R. Integrating a network IDS into an open source cloud computing. In: Sixth international conference on information assurance and security (IAS); 2010; pp. 265–70.

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.
NIST: National vulnerability database, Website, Available from: 〈http://web.nvd.nist.gov/view/ vuln/detail?vulnId=CVE-〉2009-3733; 2011.
Opennebula, Website, 〈http://www.opennebula.org〉; 2011.
Rutkowska J, Subverting VistaTM Kernel for Fun and Profit, Black Hat Conference; 2006.
Roschke S, Feng C, Meinel C. An extensible and virtualization compatible IDS management architecture. In: Fifth international conference on information assurance and security, 2; 2009: pp. 130–4.
Ram S. Secure cloud computing based on mutual intrusion detection system. International journal of computer application 2012;2(1):57–67.
Slaviero M. BlackHat presentation demo vids: Amazon, 〈http://www.sensepost.com/blog/3797.html〉; 2009.
Sequeira D, Intrusion Prevention Systems- Security's Silver Bullet? SANS Institute InfoSec Reading Room 2002, 〈http://www.sans.org/reading_room/whitepapers/detection/intrusion_prevention_systems_securitys_silver_bullet_366?show=366.php&cat=detection〉; 2002.
Su M-Y, Yu G-J, Lin C-Y. A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach. Computer Security 2009:301–9.
Sandar SV, Shenai S. Economic denial of sustainability (EDoS) in cloud services using HTTP and XML based DDoS attacks. International Journal of Computer Applications 2012;41(20):11–6.
Scarfone K, Mell P, Guide to intrusion detection and prevention systems (IDPS), Recommendations of the National Institute of Standards and Technology, 〈http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf〉; 2007:175–180 457–471.
Tillapart P, Thumthawatworn T, Santiprabhob P. Fuzzy intrusion detection system. Assump University J Technology (A.U. J.T.) 2002;6(2):109–14.
Vieira K, Schulter A, Westphall C, Westphall C. Intrusion detection techniques in grid and cloud computing environment. IEEE IT Professional Magazine 2010.
Xiao T, Qu G, Hariri S, Yousif M. An efficient network intrusion detection method based on information theory and genetic algorithm. In: Proceedings of the 24th IEEE international performance computing and communications conference (IPCCC '05), Phoenix, AZ, USA; 2005.
Zhengbing H, Jun S, Shirochin VP. An intelligent lightweight intrusion detection system with forensic technique. In: 4th IEEE workshop on intelligent data acquisition and advanced computingsystems: technology and applications, 2007. IDAACS; 2007: pp. 647–51.
Zhengbing H, Zhitang L, Jumgi W, Novel A. Intrusion detection system (NIDS) based on signature search of datamining, WKDD First International Workshop on Knowledge discovery and Data Ming; 2008: pp. 10–6.
cox P. Intrusion detection in a cloud computing environment. 〈http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment〉; 2011.
Firewall, Telecom-Network Tech,〈http://teleco-network.blogspot.com/〉; 2011.
Denial-of-service attack, Website, 〈http://en.wikipedia.org/wiki/Denial-of-service_attack〉; 2011.
Snort-Home page, Website, 〈https://www.snort.org/〉; 2011.
The concept of Intrusion Detection System, Website, 〈http://maltainfosec.org/archives/26-The-concept-of-Intrusion-Detection-Systems.html〉 (2011).
XArp 2.2.2, Website, 〈http://www.filecluster.com/Network-Tools/Network-Monitoring/Download-XArp.html〉; 2011.
IBM Research-Zurich, Website, 〈http://www.zurich.ibm.com/csc/security/securevirt.html#top〉; 2011.
IPS: Intrusion Prevention System. Javvin, Website,〈http://www.javvin.com/networksecurity/IPS.html〉; 2011.
stiawanD, Abdullah, AH, Idris, MY.The trends of intrusion prevention system network. In: Second international conference on education technology and computer (ICETC) 4; 2010: 217–21.