A survey of intrusion detection techniques in Cloud

Chirag Modi, Dhiren Patel, Hiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan

Centre for Cyber Security Sciences, City University London EC1V 0HB

Email: *R.Muttukrishnan@city.ac.uk*

***Abstract*—Cloud computing provides scalable, virtualized on-demand services to the end users with greater flexibility and lesser infrastructural investment. These services are provided over the Internet using known networking protocols, standards and formats under the supervision of different managements. Existing bugs and vulnerabilities in underlying technologies and legacy protocols tend to open doors for intrusion. This paper, surveys different intrusions affecting availability, confidentiality and integrity of Cloud resources and services. It examines proposals incorporating Intrusion Detection Systems (IDS) in Cloud and discusses various types and techniques of IDS and Intrusion Prevention Systems (IPS), and recommends IDS/IPS positioning in Cloud architecture to achieve desired security in the next generation networks.**

***Index Terms*— Cloud computing, Firewalls, Intrusion detection system, Intrusion prevention system.**

I. 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 [1]. Cloud provides services in various forms: Software as a Service-SaaS (e.g. Google Apps [2]), Platform as a Service-PaaS (e.g. Google App Engine [3], Microsoft's Azure [4]) and Infrastructure as Service-IaaS (e.g. Amazon Web Service (AWS) [5], Eucalyptus [6], Open Nebula [7]).

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 [8] showed that security is the greatest challenge of Cloud computing. The recent cloud computing security white paper by Lockheed Martin Cyber Security division [9] 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. E.g. DoS attack on the underlying Amazon Cloud infrastructure caused BitBucket.org, a site hosted on AWS to remain unavailable for few hours [10]. As shown in [12], the computing-cost using current cryptographic techniques cannot be overlooked for Cloud. 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 intrusion 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 and section 5 surveys existing IDS/IPS types and examines Cloud specific work on IDS. Section 6 concludes with references at the end.

II. INTRUSIONS TO CLOUD SYSTEMS

This section illustrates several common intrusions, which causes availability, confidentiality and integrity issues to Cloud resources and services.

A. Insider attack

Authorized Cloud users may attempt to gain (and misuse) unauthorized privileges. Insiders may commit frauds and disclose information to others (or destroy information intentionally). This poses a serious trust issue. For example, an internal DoS attack demonstrated against the Amazon Elastic Compute Cloud (EC2) [11].

B. Flooding attack

Here, attacker tries to flood victim by sending huge number of packets from innocent host (*zombies*) 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 on 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 distributed attack is called indirect 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.

C. User to Root attacks

Here, an attacker gets an access to legitimate user's account by sniffing password. This makes him 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 since 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.

D. 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 (same as ACK scan but it checks any modifications in the window field of packet) etc. In Cloud scenario, attacker can attack offered services (by discovering open ports upon which these services are provided) through port scanning.

E. Attacks on Virtual Machine (VM) or hypervisor

By compromising the lower layer hypervisor, attacker can gain control over installed VMs. E.g. BLUEPILL [13], SubVir [14] and DKSM [15] 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) [16] that attract an attacker to gain access to hypervisor or other installed VMs. A zero-day vulnerability is a threat that tries to exploit application vulnerabilities that are unknown to others or the software developer. 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 [17].

F. Backdoor channel attacks

It is a passive attack which allows hackers to gain remote access to the infected node in order to compromise user confidentiality. Using backdoor channels, hackers 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.

For insider attacks, signature based intrusion detection solutions can normally be used. 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. Firewall (in Cloud) could be the common solution to prevent some of the attacks listed above. Several intrusion detection techniques are discussed in section IV.

III. FIREWALLS: COMMON SOLUTION TO INTRUSIONS

Firewall protects the front access points of system and is treated as the first line of defense. Firewalls [18] 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. 2 [18], where it is installed at entry point of servers. Several types of firewalls are discussed in [19].

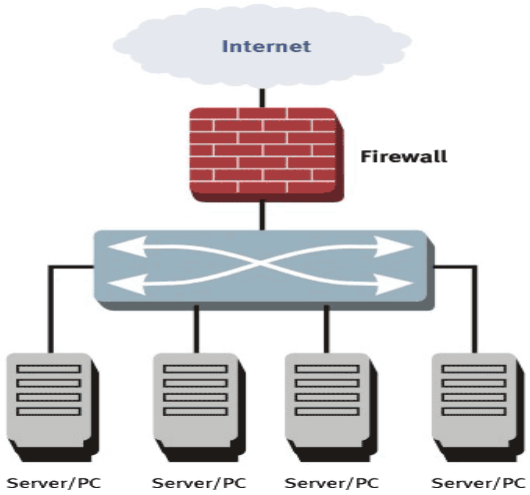

Fig. 2. Basic firewall installation [65].

TABLE I
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. ➢ 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. ➢ 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.

In Table I, 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 [20].

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.

IV. IDS AND IPS TECHNIQUES: EVOLUTION

Traditional IDS/IPS techniques such as signature based detection, anomaly detection, artificial intelligence (AI) based detection etc. can be used for Cloud.

A. Signature based Detection

Signature based intrusion detection attempts to define a set of rules or signatures or predefined knowledge base 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 even very subtle intrusions. Little variation in known attacks may also affect the analysis if a detection system is not properly configured [32]. Therefore, signature based detection is an efficient solution for detecting known attacks but 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 [22] the parts of a signature are the header (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. D. Stiawan et al. [23] 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 in [56][57][59][62] use signature based intrusion detection system for detection of intrusion on VMs (front end of Cloud environment). These approaches are discussed in the next section.

B. Anomaly Detection

Anomaly (or behavioral) detection is concerned with identifying events that appear to be anomalous with respect to normal system behavior [32]. 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 behaviour, which determines whether that behaviour 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.

T. Dutkevych et al. [33] 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. H. Zhengbing, *et al*.,[34] presented lightweight intrusion detection system to detect the intrusion in real-time, efficiently and effectively. In this work, behaviour 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 it difficult to monitor or control them using anomaly detection technique. In [26][55][60][61], 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 [38]. 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. used to improve detection accuracy and efficiency of signature based IDS or anomaly detection based IDS.

C. Artificial Neural Network (ANN) based IDS

The goal of using ANNs [35] 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 [36]. The types of ANN used in IDS are as follows [36]: Multi-Layer Feed-Forward (MLFF) neural nets, Multi-Layer Perceptron (MLP) and Back Propagation (BP).

J. Cannady [37] proposed a three layer neural network for misuse detection in network. The feature vector used in [37] 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. Authors of [38] 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 [37]. Grediaga et al. [39] 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) [36] 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. However, 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. However, it requires more training samples and time for effective learning of ANN.

Use of only ANN based IDS cannot be an efficient solution to detect intrusions for Cloud as it requires quick intrusion detection mechanism. An approach proposed in [55], uses ANN based anomaly detection technique for Cloud environment, which requires more training samples as well as more time for detecting intrusions effectively.

D. Fuzzy Logic based IDS

Fuzzy logic [35] can be used to deal with inexact description of intrusions. It provides some flexibility to the uncertain problem of intrusion detection.

Tillapart et al. [40] 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 [41] 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 [40] [41] cannot be used in real time for detecting network intrusions as the training time is significant. Fuzzy association rules presented in [42] are used to detect network intrusion in real time. There are two rule sets generated which are mined online from training data. Features for comparison are taken from network packet header. This approach is used for large scale attacks such as DoS/DDoS.

To reduce training time of ANN[55], fuzzy logic with ANN can be used for fast detection of unknown attacks in Cloud.

E. Association Rule based IDS

Some intrusion attacks are formed based on known attacks or variant of known attacks. To detect such signatures or attacks, signature apriori algorithm [43] can be used, which finds frequent subset (containing some features of original attack) of given attack set.

H. Han, *et al*.,in [43] proposed network based intrusion detection using data mining technique. In this approach, signature based algorithm generates signature for misuse detection. However, drawback of the proposed algorithm is its time consumption to scan database for generating signatures. Authors in [44] solved the database scanning time problem examined in [43]. They proposed scanning reduction algorithm to reduce number of database scans for effectively generating signatures or attacks from previously known attacks. However, it has very high false positive alarm rate since some interesting patterns are ignored and unwanted patterns are produced. L. Li et. al [45] proposed length decreasing support based apriori algorithm to detect intrusions to reduce production of short pattern as derived in [43][44] 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.

F. Support Vector Machine (SVM) based IDS

SVM [35] is used to detect intrusions based on limited sample data, where dimensions of data will not affect the accuracy.

In [46], it is showed 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 [47]. Li and D. Liu [47] designed an intelligent module for network intrusion prevention system with a combination of SNORT and configurable firewall. The support vector machine (SVM) classifier is also used with SNORT to reduce false alarm rate and improve accuracy of IPS. However, performance results are not evaluated yet.

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

G. Genetic Algorithm (GA) based IDS

Genetic algorithms (GAs) [48] [50] are used to select network features or to determine optimal parameters which can be used in other techniques for achieving result optimization and improving accuracy of IDS.

Authors in [51] used seven features (Duration, Protocol, Source_port, Destination_port, Source_IP, Destination_IP, Attack_name) of captured packet having categorical and

numerical values. 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 et al. [49] 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. In [52] information theory and GA based approach 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. Authors in [48], 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 shown in [49]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.

H. Hybrid Techniques

Hybrid techniques use the combination two or more of above techniques. It is advantageous since each technique has some advantages and drawbacks.

NeGPAIM in [53] 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. To improve performance of IDS, author in [54] 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 an example, 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 [18]. 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 II, a summary of existing IDS/IPS techniques with their strengths and limitations are given

TABLE II
SUMMARY OF IDS/IPS TECHNIQUES

IDS/IPS Technique	Characteristics / Advantages	Limitations / Challenges
Misuse 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. • Knowledge base for matching should be crafted carefully. • High false alarm rate for unknown attacks.
Anomaly detection	• Uses statistical test on collected behaviour to identify intrusion. • Can lower the false alarm rate for unknown attacks.	• Lot of time required to identify attacks. • Detection accuracy is based on amount of collected behaviour or features.
ANN based IDS	• Classifies unstructured network packet efficiently. • Multiple hidden layers in ANN increase efficiency of classification.	• It requires lot of time at training phase. • Large number of samples required for training effectively. • 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 be used for 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 before applying.
GA based IDS	• It is used to select best features for detection. • Has better efficiency.	• It is complex a method. • Used in specific manner rather than general.
Hybrid Techniques	• It is an efficient approach to classify rules accurately.	• Computational cost is high.

V. 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).

A. Host based Intrusion Detection Systems (HIDS)

A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyzes the information collected from a specific host machine. HIDS running on a host machine 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 behaviour of the program. Upon detection of deviation from expected behaviour, it reports the existence of attack. The efficiency of HIDS depends on chosen system characteristics to monitor. In Fig. 3, some host machines are with HIDS installed. Each HIDS detects intrusion for the machines in which it is placed.

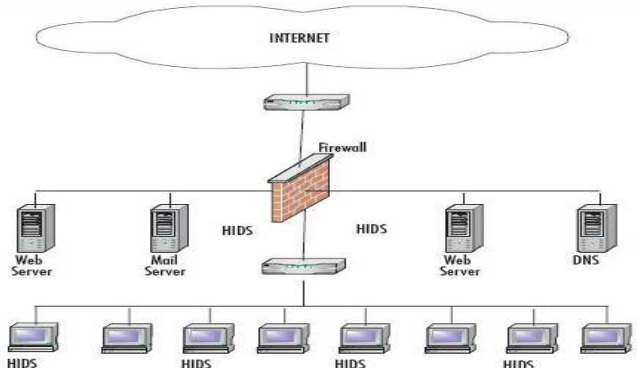

Fig. 3. Host based intrusion detection system (HIDS) [63]

With respect to Cloud computing, HIDS can be placed on a host machine, VM or hypervisor to detect intrusive behaviour 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 [21].

HIDS based architecture for Cloud environment is proposed in [55]. 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 [55], 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 behaviour based technique or knowledge based technique. Knowledge based technique is used to detect known attacks, whereas the behaviour 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 for detecting known attacks by using knowledge base as well as unknown attacks by applying feed forward ANN.

The experiments demonstrated in [55] show that the false positive and false negative alarm rate is very low when large numbers of training samples of intrusion attack are applied for behaviour analysis method. The limitation of this approach is that it cannot detect any insider intrusions which are running on VMs.

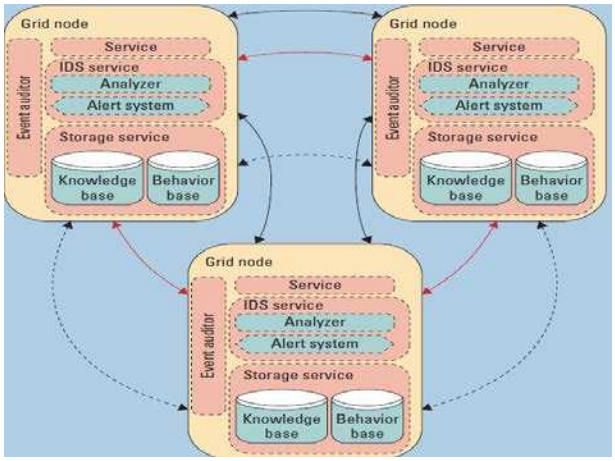

Fig. 4. IDS architecture for Grid/Cloud environment [55].

Authors [61] have proposed change point based idea to detect all types of attacks in attack space. This approach is based on statistics and probability theory. 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 issues are reported yet.

B. Network based Intrusion Detection System (NIDS)

A Network based Intrusion Detection System (NIDS) is an intrusion detection system that tries to detect malicious activity such as DoS attacks, port scans or even attempts to crack into computers by monitoring network traffic. 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 behaviour with already observed behaviour 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 really no effective way for the NIDS to decrypt the traffic for analysis.

M. A. Hemairy at el. [24] surveyed about the security solutions that can be applicable to detect ARP spoofing attacks through experiments and implementation. They concluded that XArp 2 tool [25] is 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 further be improved.

Fig. 5 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.

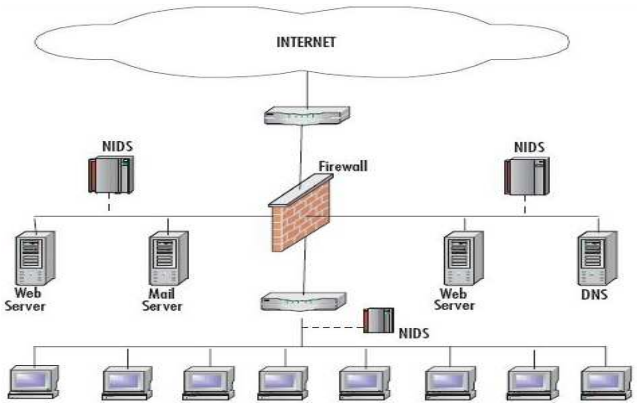

Fig. 5. Network based intrusion detection system [63].

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 it comes to attack 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 in [56] is shown in Fig. 6. 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 behaviour identified by IDS sensor and stores in event database. Event database stores information regarding captured events. Analysis component accesses event database and analyze events, which is configured by users. 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 behaviour 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.

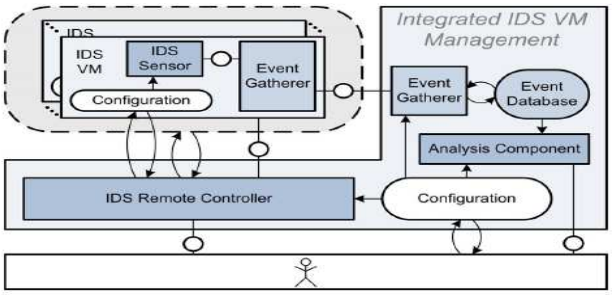

Fig. 6. Architecture of VM integrated IDS management [56].

In the approach proposed [57], for detecting DDoS attack in VM, IDS systems are 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. But it cannot detect all types of attacks as the tool used here (SNORT) identifies only known attacks.

C. Mazzariello et al [62] 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 [57]. It is a fast and cost effective solution. However, it can detect only known attacks since only SNORT [22] is involved.

C. 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, which are complement of each other [28]. Fig. 7, demonstrates the working of DIDS.

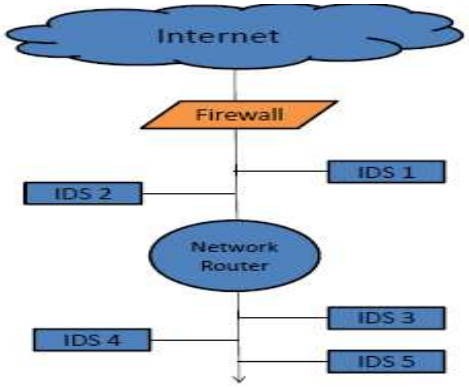

Fig. 7 Distributed intrusion detection system (DIDS).

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

In ccooperative agent based aapproach [59], individual NIDS module is deployed in each Cloud computing region as shown in Fig. 8 [59]. 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 computing region.

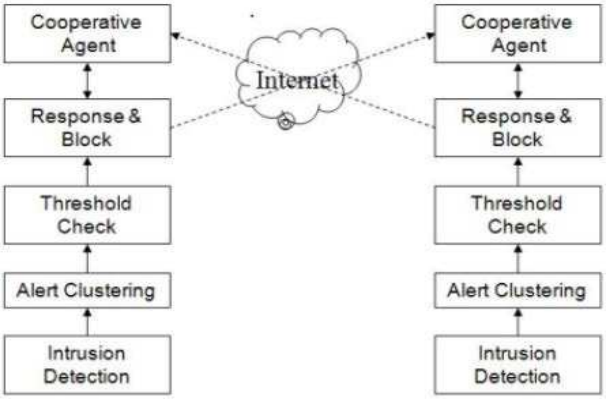

Fig. 8. Block diagram of cooperative agent based approach [59].

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. However, the computational effort is increased.

A. V. Dastjerdi et al. [60] 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, if numbers of VMs are attached to mobile agent increases.

D. Hypervisor-based Intrusion Detection Systems

Hypervisor-based intrusion detection system is an intrusion detection system specifically designed for hypervisors. Hypervisor is a platform to run VMs. Running at hypervisor layer, this type of IDS 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. Novelty in the technology and lack of experience are the few of its challenges [21].

VM introspection based IDS [26] is one of the examples of hypervisor based intrusion detection system. Recently IBM Research is pursuing virtual machine introspection approach used to create a layered set of security services inside protected VM running on same physical machine as the guest VMs running in the Cloud system [27].

As Cloud computing is defined as a pool of virtualized computer resources and to manage various virtual machines,

hypervisor (also known as virtual machine manager) is used. Hypervisor based IDS is one of the important techniques, specifically in Cloud computing, to detect intrusion in virtual environment.

Authors of [26] propose virtual machine introspection based IDS (VMI-IDS) architecture as shown in Fig. 9 [26]. 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 [26]. 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 complex anomaly detection. It is used for lie detection, signature detection, program integrity detection and row socket detection. According to results shown in [26], performance of policy engine is good in terms of workload and time. However, VMM or OS library can be compromised [26].

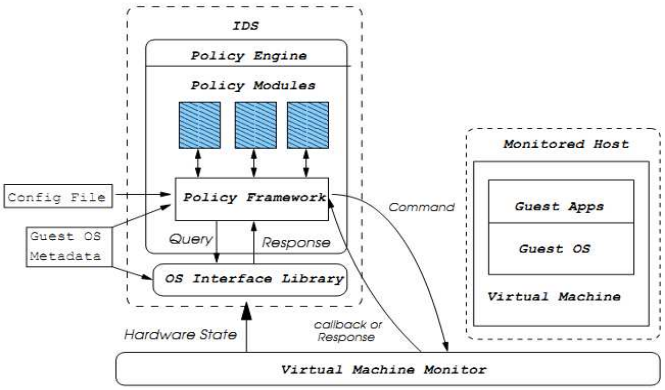

Fig. 9. VMI-basedIDS architecture [26].

E. Intrusion Prevention System (IPS)

With the help of IDS, IPS monitors network traffic and system activities to detect possible intrusions 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 [18].

M. Ahmed et al. [29] 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 [29]. F. Y. Leu and Z. Y. Li [30] 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. 10.

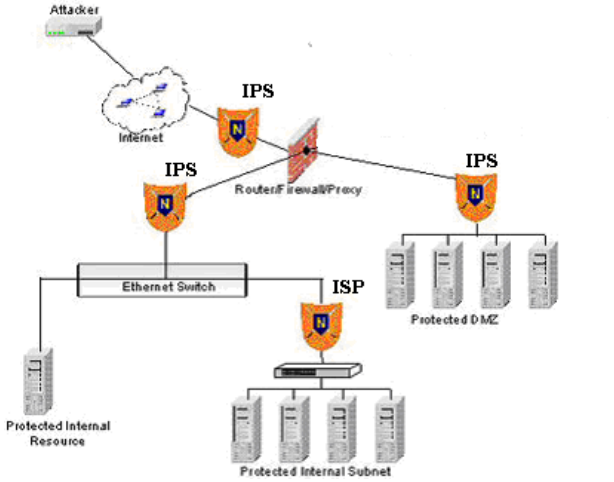

Fig. 10. Network based intrusion prevention system [64].

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.

Authors in [58], 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. 11 [58], 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 structure defined by Iptable application module. Also pointer to skb buffer storing the packet information is transferred to 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.

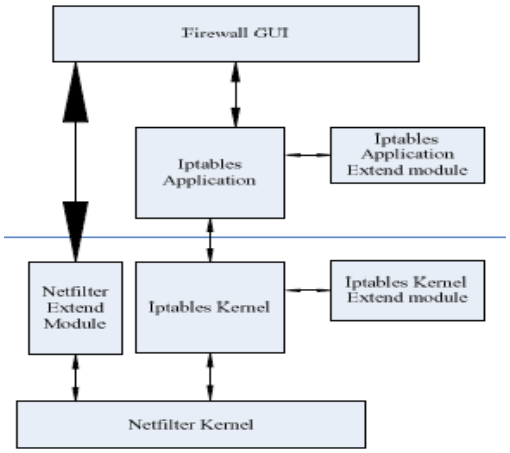

Fig. 11. The Architecture of Firewall and its extension Xen [58].

F. 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 [31]. Proper configuration and management of IDS and IPS combination can improve security. NIST [31] 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 following four groups based on the type of events that they monitor and the ways in which they are deployed [31]: (a) Network-Based (b) Wireless (c) Network Behaviour Analysis (NBA) (d) Host-Based. Positioning of network based IDPS in typical network is shown in Fig. 12 [31].

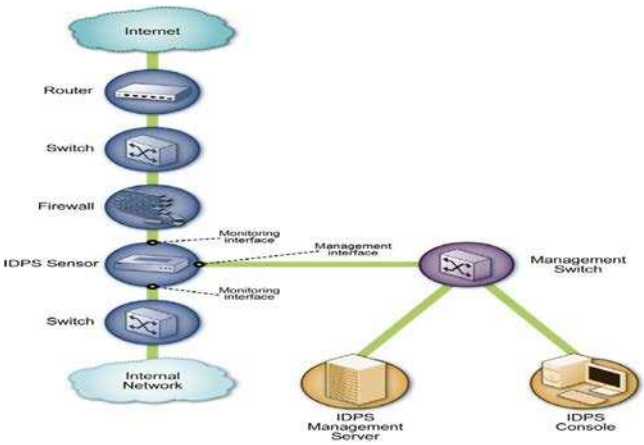

Fig. 12. Positioning IDPS in network [31].

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. 13 demonstrates the same followed by its summary.

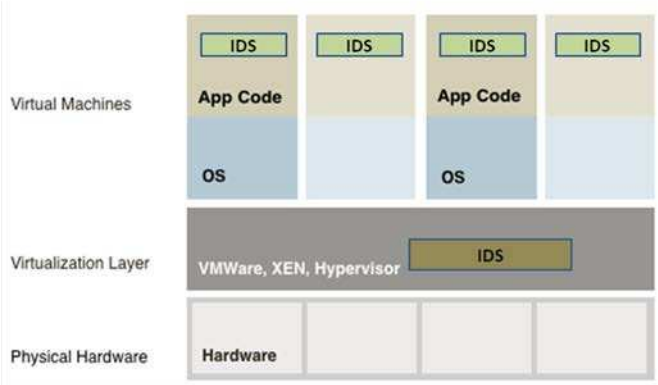

Fig. 13. Placement of IDS on VMs and hypervisor/host system.

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 III.

TABLE III
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 such as 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 intruders. • 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.	Network based IDPS: Cloud provider. Host based IDPS (on VM): Cloud user Host based IDPS (on Hypervisor): Cloud provider.

So far, we have discussed some of the existing approaches which are incorporating IDS into Cloud. However, there is no universal efficient solution found yet. Each has some limitations. In Table IV, we summarize presented approaches with their type, technique, positioning in Cloud, pros and cons. This gives the cloud security research community several challenges to address before a standard security framework for the cloud can be proposed.

TABLE IV
SUMMARY OF EXISTING IDS APPROACHES IN CLOUD

Title	IDS Type	Technique used	Positioning	Pros	Cons
IDS architecture for Cloud environment [55]	HIDS	Signature based detection 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.
VM compatible IDS architecture [56]	NIDS	Signature based detection	On each VM	Secure VM based on user configuration.	Multiple instances of IDS are required which degrades performance.
DDoS attack detection in virtual machine [57]	NIDS	Signature based detection	On each VM	Secures VM from DDoS attacks.	Can only detects known attacks since only snort used.
NIDS in open source Cloud [62]	NIDS	Signature based detection	On traditional Network	Can detect several known attacks.	It cannot detect insider attacks as well as known attacks since only snort used.
Cooperative agent based approach [59]	DIDS	Signature based detection	On each Cloud region	Prevent system from single point failure.	Cannot be used for all types of attacks. Computational overhead high.
Mobile agent based approach [60]	DIDS	Anomaly detection	On each VM	Provides IDS for Cloud application regardless by their location.	Produce network load with increase of VMs attached to MA.
VMI-IDS based architecture [26]	Hypervisor based	Anomaly detection.	On hypervisor	Detect attacks on VMs.	VMI IDS can be attacked. Very complex method.
Xen based Host based firewall [58]		Prevention	On each Host	Prevention using user configured rules.	Not used for preventing unknown attacks.
CP based approach [61]		Anomaly detection	-	Used to detect all types of attacks. Solves limitation of computing time.	No any experimental results are shown.

VI. CONCLUSION

This survey, discussed several intrusions which can threat integrity, confidentiality and availability of Cloud services in the future. One of the existing solutions viz. firewall may not be sufficient to solve Cloud security issues. The paper emphasized the usage of alternative options to incorporate intrusion detection or intrusion prevention techniques into Cloud and explored locations in Cloud where IDS/IPS can be positioned for efficient detection and prevention of intrusion. Recent research findings incorporating IDS/IPS specifically in Cloud have been discussed and their advantages and disadvantages have been highlighted. . The adaptation of soft computing techniques in IDS/IPS can optimistically improve the security. The paper has finally identified several security challenges that need to be addressed by the cloud research community before the cloud can become a secure and trusted platform for the delivery of future Internet of Things.

REFERENCES

[1] P. Mell, and T. Grance. (2011). The NIST Definition of Cloud Computing (Draft). *NIST* [Online]. Available: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[2] Google apps. [Online]. Available: http://www.google.com/apps/business

[3] "Google apps engine." [Online]. Available: URL http://code.google.com/appengine.

[4] Azure services platform. [Online]. Available: http://www.microsoft.com/azure

[5] Amazon web services. [Online]. Available: http://aws.amazon.com

[6] Eucalyptus. [Online]. Available: http://eucalyptus.cs.ucsb.edu/.

[7] Opennebula. [Online]. Available: http://www.opennebula.org

[8] International Data Corporation. 2009. [Online]. Available: http://blogs.idc.com/ie/wpcontent/uploads/2009/12/idc_cloud_challenges_2009.jpg, 2009.

[9] Lockheed Martin White Paper: Available: http://www.lockheedmartin.com/data/assets/isgs/documents/CloudComputingWhitePaper.pdf

[10] C. Brooks. Amazon EC2 Attack Prompts Customer Support Changes. *Tech Target*. [Online]. Available: http://searchcloudcomputing.techtarget.com/news/article/0,289142,sid201_gci1371090,00.html

[11] M. Slaviero, "BlackHat presentation demo vids: Amazon." [Online]. Available: http://www.sensepost.com/blog/3797.html

[12] Y. Chen, and R. Sion, "On securing untrusted clouds with cryptography," *In WPES '10*, pp. 109–114, 2010.

[13] J. Rutkowska, "Subverting VistaTM Kernel for Fun and Profit," *Black Hat Conference*, 2006.

[14] S. King, P. Chen, and Y-M. Wang, "SubVirt: Implementing malware with virtual machines," *2006 IEEE Symposium on Security and Privacy*, 2006, pp.314-327.

[15] S. Bahram, X. Jiang, Z. Wang, and M. Grace, "DKSM: Subverting Virtual Machine Introspection for Fun and Profit," *Proceedings of the 29th IEEE International Symposium on Reliable Distributed Systems*, 2010.

[16] NIST: National vulnerability database. [Online]. Available: http://web.nvd.nist.gov/view/ vuln/detail?vulnId=CVE-2009-3733

[17] D. Goodin, "Webhost Hack Wipes Out Data for 100,000 Sites." [Online]. Available: http://www.theregister.co.uk/2009/06/08/webhost_attack/

[18] S. Beg, U. Naru1, M. Ashraf, and S. Mohsin, "Feasibility of Intrusion Detection System with High Performance Computing: A Survey," *International Journal for Advances in Computer Science*, vol. 1, no. 1, 2010.

[19] Dinesh Sequeira, "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

[20] Denial-of-service attack. [Online]. Available: http://en.wikipedia.org/wiki/Denial-of-service_attack

[21] Phil cox, "Intrusion detection in a cloud computing environment." [Online]. Available: http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment

[22] "Snort-Home page." [Online]. Available: https://www.snort.org/

[23] D. stiawan, A. H. Abdullah, and M. Y. Idris, "The Trends of Intrusion Prevention System Network," 2nd International Conference on Education Technology and Computer (ICETC), vol. 4, 2010, pp. 217-221.

[24] M. A. Hemairy, S. Amin, and Z. Trabelsi, "Towards more sophisticated ARP Spoofing detection/prevention systems in LAN networks," *International Conference on the Current Trends in Information Technology (CTIT)*, 2009, pp. 1-6.

[25] XArp 2.2.2. [Online]. Available: http://www.filecluster.com/Network-Tools/Network-Monitoring/Download-XArp.html

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

[27] IBM Research-Zurich. [Online]. Available: http://www.zurich.ibm.com/csc/security/securevirt.html#top

[28] A. K. Jones, and R. S. Sielken. Computer System Intrusion Detection: A Survey. [Online]. Available: http://www.cs.virginia.edu/~jones/IDSresearch/ Documents/jones-sielken-survey-v11.pdf

[29] M. Ahmed, R. Pal, H. M. Hossain, M. Bikas, and M. K. Hasan, "NIDS: A Network Based Approach to Intrusion Detection and Prevention," *Computer Science and Information Technology - Spring Conference*, 2009, pp. 141-144.

[30] F. Y. Leu, and Z. Y. Li, "Detecting DoS and DDoS Attack Using an Intrusion Detection and Remote Prevention System," *Fifth International Conference on Information Assurance and Security*, Vol. 2, 2009, pp. 251-254.

[31] K. Scarfone, and P. Mell. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[32] D. J. Brown, B. Suckow, and T. Wang. *A Survey of Intrusion Detection Systems*. Department of Computer Science, University of California, San Diego.

[33] T. Dutkevyach, A. Piskozub, and N. Tymoshyk, "Real-Time Intrusion Prevention and Anomaly Analyze System for Corporate Networks," *4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2007. IDAACS 2007*, 2007, pp. 599-602.

[34] H. Zhengbing, S. Jun, and V. P. Shirochin, "An Intelligent Lightweight Intrusion Detection System with Forensic Technique," *4th IEEE Workshop on Intelligent Data Acquisition and Advanced ComputingSystems: Technology and Applications, 2007. IDAACS*, 2007, pp. 647-651.

[35] J. Han and M. Kamber. *Data Mining Concepts and Techniques 2nd edition*. Morgan Kaufmann Publishers, 2006

[36] L. M. Ibrahim, "Anomaly Network Intrusion Detection System Based On Distributed Time-Delay Neural Network," *Journal of Engineering Science and Technology*, vol. 5, no. 4, pp. 457 – 471, 2010.

[37] J. Cannady, "Artificial Neural Networks for Misuse Detection," *National Information Systems Security Conference*. 1998.

[38] M. Moradi, and M. Zulkernine, "A Neural Network Based System for Intrusion Detection and Classification of Attacks," *Proceedings of the 2004 IEEE International Conference on Advances in Intelligent Systems - Theory and Applications*, 2004.

[39] Grediaga, F. Ibarra, F. García, B. Ledesma, and F. Brotons, "Application of neural networks in network control and information security," *LNCS*, pp. 208–213, 2006.

[40] P. Tillapart, T. Thumthawatworn, and P. Santiprabhob, "Fuzzy intrusion detection system," *Assump University J Technology (A.U. J.T.)*, vol. 6, no. 2, pp.109–114, 2002.

[41] S. Chavan, K. Shah, N. Dave, and S. Mukherjee, "Adaptive neuro-fuzzy intrusion detection systems," *IEEE international conference on information technology: coding and computing (ITCC'04)*, 2004, pp 70–74.

[42] M-Y. Su, G-J. Yu, and C-Y. Lin, "A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach," *Computer Security*, pp.301–309, 2009.
[43] H. Han, X. L. Lu, and L. Y. Ren, "Using Data Mining To Discover Signatures In Network-Based Intrusion Detection", *Proceedings of the First International Conference on Machine Learning and Cybernetics*, Beijing, vol. 1, 2002.
[44] H. Zhengbing, L. Zhitang, and W. Jumgi, "A Novel Intrusion Detection System (NIDS) Based on Signature Search of DataMining," *WKDD First International Workshop on Knowledge discovery and Data Ming*, 2008, pp. 10-16.
[45] L. Lei, D-Z Yang, and F-C Shen, "A Novel rule based Intrusion Detection system using Data Ming," *3rd IEEE International Conference on Computer Science and Information Technology*, vol. 6, pp. 169-172, 2010.
[46] W-H. Chen, S-H. Su, and H-P. Shen, "Application of svm and ann for intrusion detection," *Computer Oper Res*, vol. 32, no.10, pp. 2617–2634, 2005.
[47] H. Li, and D. Liu, "Research on Intelligent Intrusion Prevention System Based on Snort," *International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE)*, vol. 1, pp. 251-253, 2010.
[48] Y. Dhanalakshmi, and I. Ramesh Babu, "Intrusion detection using data mining along fuzzy logic and genetic algorithms," *International Journal of Computer Science & Security*, vol. 8, no.2, pp. 27–32, 2008.
[49] W. Lu, and I. Traore, "Detecting new forms of network intrusion using genetic programming," *Computational Intelligence*, vol. 20, no. 3, pp. 475-494, 2004.
[50] W. Li, "A Genetic Algorithm Approach to Network Intrusion Detection", SANS Institute, USA, 2004.
[51] R H. Gong, M. Zulkernine, and P. Abolmaesumi, "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.
[52] T. Xiao, G. Qu, S. Hariri, and M. Yousif, "An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm," *Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC '05)*, Phoenix, AZ, USA. 2005.
[53] M. Botha, R. Solms, K. Perry, E. Loubser, and G. Yamoyany, "The utilization of Artificial Intelligence in a Hybrid Intrusion Detection System", *SAICSIT*, 2002, pp. 149-155.
[54] C. Katar, "Combining multiple techniques for intrusion detection," *International Journal of Computer Science & Network Security*," vol. 6, no.2B, pp. 208–218, 2006.
[55] C. B. W. C. M. W. K. M. VIEIRA, A. SCHULTER, "Intrusion detection techniques in grid and cloud computing environment," *IEEE IT Professional Magazine*, 2010.
[56] S. Roschke, C. Feng, and C. Meinel, "An Extensible and Virtualization Compatible IDS Management Architecture," *Fifth International Conference on Information Assurance and Security*, vol. 2, 2009, pp. 130-134.
[57] A.bakshi, and B. Yogesh, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine," *Second International Conference on Communication Software and Networks*, 2010, pp. 260-264
[58] L. Fagui Liu, S. Xiang Su, and L. Wenqianl, "The Design and Application of Xen-based Host System Firewall and its Extension," *in The 2009 International Conference on Electronic Computer Technology*, 2009, pp. 392-395.
[59] C. C. Lo, C. C. Huang, and J. Ku, "Cooperative Intrusion Detection System Framework for Cloud Computing Networks," *First IEEE International Conference on Ubi-Media Computing*, 2008, pp. 280-284.
[60] K. A. B. A. V. Dastjerdi, and S. G. H. Tabatabaei, "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.
[61] Y. Guan, and J. Bao, "A CP Intrusion Detection Strategy on Cloud Computing," *In International Symposium on Web Information Systems and Applications (WISA)*, pp. 84–87, 2009.
[62] C. Mazzariello, R. Bifulco, and R. Canonoco, "Integrating a network IDS into an Open source Cloud computing," *Sixth International conference on Information Assurance and Security (IAS)*, 2010, pp. 265-270.
[63] The concept of Intrusion Detection System. [Online]. Available: http://maltainfosec.org/archives/26-The-concept-of-Intrusion-Detection-Systems.html
[64] IPS:Intrusion Prevention System. *Javvin*. [Online]. Available: http://www.javvin.com/networksecurity/IPS.html
[65] Firewall. *Telecom-Network Tech.* [Online]. Available: http://teleco-network.blogspot.com/