Intrusion Detection System in Cloud Computing: Challenges and opportunities

Conference Paper · December 2013

DOI: 10.1109/NCIA.2013.6725325

4 authors, including:

Awais Shibli
National University of Sciences and Technology
57 PUBLICATIONS **351** CITATIONS

SEE PROFILE

Umme Habiba
National University of Sciences and Technology
6 PUBLICATIONS **37** CITATIONS

SEE PROFILE

Rahat Masood
UNSW Sydney
27 PUBLICATIONS **191** CITATIONS

SEE PROFILE

Intrusion Detection System in Cloud Computing: Challenges and Opportunities

Yasir Mehmood
SEECS, National University of Science and Technology
Islamabad, Pakistan
E-mail: 11msccsymehmood@seecs.edu.pk

Umme Habiba
SEECS, National University of Science and Technology
Islamabad, Pakistan
E-mail: 11msccsuhabiba@seecs.edu.pk

Muhammad Awais Shibli
SEECS, National University of Science and Technology
Islamabad, Pakistan
E-mail: awais.shibli@seecs.edu.pk

Rahat Masood
SEECS, National University of Science and Technology
Islamabad, Pakistan
E-mail: rahat.masood@seecs.edu.pk

***Abstract*— Today, Cloud Computing is the preferred choice of every IT organization since it provides flexible and pay-per-use based services to its users. However, the security and privacy is a major hurdle in its success because of its open and distributed architecture that is vulnerable to intruders. Intrusion Detection System (IDS) is the most commonly used mechanism to detect attacks on cloud. This paper provides an overview of different intrusions in cloud. Then, we analyze some existing cloud based intrusion detection systems (IDS) with respect to their type, positioning, detection time, detection technique, data source and attacks they can detect. The analysis also provides limitations of each technique to evaluate whether they fulfill the security requirements of cloud computing environment or not. We emphasize the deployment of IDS that uses multiple detection methods to cope with security challenges in cloud.**

Keywords*— *Cloud Computing; Cloud Security; Intrusion Detection System; Signature; Anomaly

I. INTRODUCTION

Cloud Computing offers omnipresent, convenient, demand-based access to a shared group of configurable computing resources (like storage, network, services applications and servers) that can be quickly provisioned and released with least management effort or service provider interactions [1]. It provides services to its users in different ways: Infrastructure as a Service (IaaS), where the user has control over complete virtual machines [2] such as Eucalyptus, Open Nebula [3]. Platform as a Service (PaaS), where the user can deploy user-created applications in cloud if the provider supports the languages, APIs, and tools used for creating application, [1] like Google App Engine, Microsoft's Azure [3]. Software as a Service (SaaS) which enables users to execute provider's applications [1] such as Google apps [3]. These services are provided via the Internet. There are four deployment models for cloud: *Public cloud*, its infrastructure is intended to be used by general public and managed by a governmental academic or business organization. *Private cloud*, it is deployed for a particular organization having multiple users. Its management is the responsibility of organization using its services or a third party. *Community cloud* which is deployed for use by a particular group of users from organizations having common goals. It can be managed by any of the organizations within that group or a third party. *Hybrid cloud*, its infrastructure consists of two or more different cloud infrastructures (public, private, or community) that ensures the portability of applications and data using a standard technology. The unique features of clouds forming hybrid cloud are retained [1].

The architecture of cloud is open and fully distributed, making it a susceptible target for intruders. So the security of cloud environment is at risk where traditional network attacks as well as cloud-specific attacks threaten the cloud users (may be individuals or organizations). According to IDG Enterprise's 2013 Cloud Computing survey, security is the second major problem after lack of control which hinders the enterprises from adopting cloud computing paradigm [4]. Most common network-based attacks affecting cloud security at the network layer include: Address Resolution Protocol (ARP) spoofing, IP spoofing, DNS poisoning, port scanning, man-in-the-middle attack, Routing Information Protocol (RIP) attack, Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks [5]. Traditional network security measures like firewall are better to stop many outsider attacks but attacks from within the network [3] as well as some complicated outsider attacks (e.g. DoS and DDoS) [5]can't be tackled effectively by using such mechanisms. This is the scenario where intrusion detection systems (IDS) come into play. The role of IDS in the security of cloud is very important since it acts as additional preventive layer of security [5] and apart from detecting only known attacks, it can detect variants of many known attacks and unknown attacks.

An intrusion is defined as an attempt to compromise the Confidentiality, Integrity, and Availability (CIA) or to bypass the security mechanisms of a computer or network [6]. Intrusions may be triggered by attackers trying to access the cloud resources through the Internet, legitimate users trying to

obtain privileges not given to them formally, and privileged users who misuse their rights to access resources[6]. Intrusion detection is the process of monitoring the events in a computer system or network and analyzing them for signs of intrusions. Intrusion detection system could be a software, hardware or a combination of both for automating the process of intrusion detection. It captures data from the system or network under observation and notifies network manager by mailing or logging the intrusion event [7]. However, the alerts generated by IDS are not always relevant to actual intrusion due to false negatives and false positives which affect the performance of IDS.

A. *Limitations of existing IDS*

The existing IDS deployed in traditional Internet or Intranet environments lack the features of *scalability* and *autonomic self-adaptation*. Moreover they are not *deterministic* which make them unsuitable for cloud based environments [14]. This urges the need of a new cloud based IDS which can fulfill its security requirements.

Rest of the paper is organized as follows: In section II, we briefly describe different possible intrusions in cloud. Section III describes intrusion detection systems (IDS), including their significance in cloud, and some desired characteristics of cloud-based IDS. Section IV presents various types of IDS in cloud. In section V, we describe detection techniques used by IDS whereas section VI presents detailed analysis of various existing IDS techniques for cloud. Section VII concludes our work with references at the end.

II. INTRUSIONS IN CLOUD

An intrusion is any attempt that can compromise the CIA of a system or network. The most common intrusions that affect the CIA of cloud are the following: [3]

A. *Attacks on hypervisor or virtual machines*

An attacker may successfully control the virtual machines by compromising the hypervisor. The most common attacks on virtual layer are SubVir [8], BLUEPILL [9], and DKSM [10] which enable hackers to supervise host through hypervisor. Attackers target the hypervisor or VMs to access them by exploiting the zero-day vulnerabilities in virtual machines [11], prior to the developers' awareness about such exploits [3]. The exploitation of a zero-day vulnerability in the HyperVM application caused damage to several websites based on virtual server [12].

B. *User to root (U2R) attacks*

The attacker uses password sniffing to access a genuine user's account which enables him to obtain root privileges to a system by exploiting vulnerabilities, e.g. Root shells can be created by using Buffer overflows from a root-level process. In the cloud scenario, attacker achieves root privileges of host or VMs by first getting access to legal user instances. This attack violates the integrity of cloud based systems [3].

C. *Insider attack*

The attackers are the authorized users who try to obtain and misuse the privileges that are either assigned or not assigned to them officially [3]. This attack is closely related to trust since insiders may reveal secrets to opponents, e.g. Amazon Elastic Compute Cloud (EC2) suffered from an internal DoS attack [13]. This attack breaches the confidentiality of cloud users.

D. *Port Scanning*

Attackers can use port scanning to obtain list of closed ports, open ports, and filtered ports and then launch attacks against the services running on open ports. Different techniques of port scanning are SYN scanning, ACK scanning, TCP scanning, FIN scanning, UDP scanning etc. In cloud environment, attacker can discover the open ports using port scanning and attack the services running on these ports [3]. This attack may cause loss of confidentiality and integrity on cloud.

E. *Backdoor channel attacks*

Hackers can remotely access the infected machines by exploiting this passive attack to compromise the confidentiality of user information. Hacker can use backdoor channels to get control of victim's resources and utilize it as zombie to launch DDoS attack [3]. This attack targets the confidentiality and availability of cloud users.

F. *Denial of Service (DoS) attack*

The attacker exploits zombies for sending a large number of network packets to overwhelm the available resources. Consequently, legitimate users are unable to access the services offered over the Internet. In cloud environment, the attacker may send huge number of requests through zombies to access VMs thus disabling their availability to legitimate users which is called DoS attack [3]. This attack targets the availability of cloud resources.

III. INTRUSION DETECTION SYSTEM IN CLOUD

In the Cloud computing environment, the deployment of already available Intrusion Detection and Prevention Systems (ID/PS) can't achieve the desired level of security and performance since architecture of cloud computing paradigm is different from existing computing methods like Grid computing. The rapidly growing demand of cloud resources by its users urges the need of some efficient mechanism for secure provisioning of its resources since intruders may compromise the cloud resources and can cause damages to users' data stored there. A. Patel et al. [14] has emphasized the need to develop an IDPS that is specifically designed according to the characteristics of cloud rather than deployment of a traditional IDPS. For this, authors recommended the use of four novel concepts namely; *autonomic computing, fuzzy theory, ontology, and risk management*. Autonomic computing is the on demand, self-management capability of cloud resources. Fuzzy logic works on the basis of degrees between false and truth, or 0 and 1. It is a probabilistic approach to reach a conclusion instead of using exact values. Risk manager works in assistance with

Fuzzy logic to analyze system vulnerabilities, manage false positive rate, and help in calculation of risk severity level for taking appropriate action. Ontology refers to the representation of knowledge in the form of a set of concepts.

The effectiveness of IDS depends on aspects like the detection method, location of IDS in network, and its configuration [7]. In cloud, the IDS can be installed at different locations like: at the boundary of a network, at a host, at a VM/hypervisor, or distributed across all regions of cloud. The detection method used by IDS may be signature based, anomaly based, or hybrid. The incorporation of soft computing techniques like *Fuzzy Logic, Artificial Neural Networks (ANN), Support Vector Machines (SVM), association rules and Genetic Algorithms (GA)* or a *hybrid* combination of any of these to increase the performance of signature based or anomaly based IDS [3]. A brief description of each of these soft computing techniques will be provided in section V.

IV. TYPES OF CLOUD-BASED IDS

Cloud-based IDS can be divided into four types. These types are shown in Fig. 1 (in green). We will describe each of them in the following subsections.

A. Network based IDS

Networks based IDSs (NIDS) capture the traffic of entire network and analyze it to detect possible intrusions like port scanning, DoS attacks etc. NIDS usually performs intrusion detection by processing the IP and transport layer headers of captured network packets. It utilizes the anomaly based and signature based detection methods to identify intrusions. NIDS collects the network packets and looks for their correlation with signatures of known attacks or compares the users' current behavior with their already known profiles in real-time. Multiple hosts in the network can be secured from attackers by utilizing a few properly deployed NIDSs. If run in *stealth* mode, the location of NIDS can be hidden from attacker. The NIDS is unable to perform analysis if traffic is encrypted [6]. In cloud environment, the attacks on hypervisor or VMs are detected by positioning NIDS at the cloud server which interacts with external network. However, it cannot detect attacks inside a virtual network contained by hypervisor. Cloud provider is responsible for installing NIDS in cloud [3].

B. Host based IDS

Hosts based IDSs (HIDS) collect information from a particular host and analyze it to detect intrusive events. The information may be system logs or audit trails of operating system. HIDS analyzes the information and if there is any change in the behavior of system or program, it reports to network manager that the system is under attack. The effectiveness of HIDS can be improved by specifying the features that provide it more information for detection. However, it requires more storage for information to be analyzed [6]. In the case of cloud computing network, it is possible to deploy HIDS on hypervisor, VM or host to analyze the system logs, user login information or access control policies and detect intrusion events. Cloud user is responsible for supervision of HIDS deployed at a VM while cloud provider is responsible for the deployment of HIDS on hypervisor [3]. HIDS is capable of analyzing encrypted traffic however; it is susceptible to DoS attack and can even be disabled. HIDS are commonly used to protect the integrity of software [6].

C. VMM/Hypervisor based IDS

Hypervisor provides a platform for communication among VMs. Hypervisor based IDSs is deployed at the hypervisor layer. It helps in analysis of available information for detection of anomalous activities. The information is based on communication at various levels like communication between VM and hypervisor, between VMs and communication within the hypervisor based virtual network [3].

D. Distributed IDS

A Distributed IDS (DIDS) comprises numerous IDSs (such as NIDS, HIDS) that are deployed across a large network to monitor the traffic for intrusive behavior. The participant IDSs can communicate with each other or with a centralized server. Each of these individual IDSs has its own two function components: detection component and correlation manager [14]. Detection component monitors the system or subnet and transmits the collected information in a standard format to the correlation manager. Correlation manager combines information from multiple IDS and generates high level alerts that correspond to an attack. Analysis phase makes use of signature based and anomaly based detection methods so DIDS can detect known as well as unknown attacks. In case of cloud, DIDS can be located at any of two positions: at processing server or at host machine [3].

V. DETECTION TECHNIQUES USED BY IDS

The most common detection techniques used by IDS are based on signatures of known attacks and behavior of users. However, in order to improve the performance of IDS, it is better to use a combination (hybrid) of these techniques. This is shown in Fig. 1 (in red orange). A detailed description of each is provided in the following sub sections:

A. Signature Based Detection

Signature based detection is performed by comparing the information collected from a network or system against a database of signatures. A signature is a predefined set of rules or patterns that correspond to a known attack. This technique is also known as misuse detection [15]. It can efficiently detect known attacks with negligible false alarms. Signature based method helps network managers with average security expertise to identify intrusions accurately. It is a flexible approach since new signatures can be added to database without modifying existing ones. However, it is unable to detect unknown attacks [6].

In Cloud environment, signature based intrusion detection method can be utilized at front-end (that is host) of cloud for detection of known attacks from external network. It can also detect both internal and external intrusions if deployed at back end (that is processing servers) of cloud.

However, it is unable to identify unknown attacks in cloud just like traditional networks [3]. Mazzariello et al. in [17], Bakshi et al. in [18], and Lo et al. in [2] have used signature based detection method to detect intrusions in cloud.

B. Anomaly Based Detection

Anomaly based detection compares current user activities against preloaded profiles of users or networks to detect abnormal behavior that may be intrusions. The profiles may be dynamic or static and correspond to the expected or benign behavior of users. To build a profile, regular activities of users, network connections, or hosts are monitored for a specific period of time [15], called *training period* [16]. Profiles are developed using various features like failed login attempts, number of times a file is accessed by a particular user over a particular time duration, CPU usage etc. [15]. Anomaly based detection is effective against unknown attacks. An attack detected by anomaly based technique can be used as a signature in signature based detection. However it produces a large number of false alarms due to irregular network and user behavior. Moreover, it also requires large data sets to train the system for normal user profiles [6].

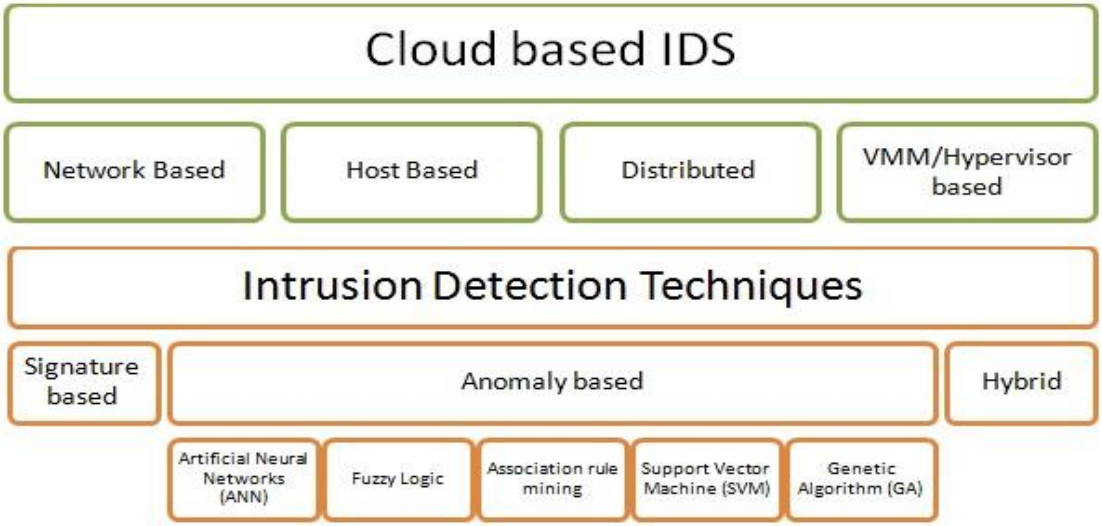

Fig. 1 Types of Cloud based IDS (green), Detection techniques used by IDS (red orange)

In Cloud, unknown attacks can be detected at different levels by using anomaly detection technique. Monitoring of intrusions becomes difficult due to large data flow at different levels (system, network) of cloud. A. Patel et al. in [20], Lee et al. in [21] and Dastjerdi et al. in [22] have used anomaly based intrusion detection system to identify intrusions in cloud.

Now we give a brief description of soft computing techniques mentioned in section III:

a) Fuzzy Logic: It is based on probability, uses values ranging between 0 and 1, and is used to define degree of anomaly in intrusion detection.

b) Artificial Neural Networks (ANN): In intrusion detection, ANN can be used for generalization of data from imperfect data [23]. It is also used to categorize data as being normal or anomalous [24].

c) Support Vector Machines (SVM): SVM [23] can be an effective way to detect intrusive events in case of limited data samples, where data dimensions will not change the accuracy.

d) Association rules: This technique helps in creation of new signatures which can be used to detect intrusions. Such intrusions consist of some known attacks or variation of known attacks.

e) Genetic Algorithm (GA): The network features selected by using GAs [25][26] can be applied in other techniques which improves the detection accuracy of IDS.

These techniques can be incorporated in traditional IDS to improve security in cloud environment.

C. Hybrid Detection

The efficiency of IDS can be significantly improved by combining signature based and anomaly based techniques which is called Hybrid detection technique. The motivation behind this combination is the ability to detect both known and unknown attacks using signature based and anomaly based detection techniques [14]. In cloud computing, Viera et al. in [21], C. N. Modi et al. in [5] have used hybrid detection techniques to increase the efficiency of IDS.

VI. Analysis of Existing Cloud based Intrusion Detection Systems (CIDS)

In this section, we will describe various CIDS and classify them into three types based on the intrusion detection technique used by each system. The types are *Signature based*, *Anomaly based* and *Hybrid*. We have investigated systems from each category and analyzed them to evaluate whether or not they meet the security requirements of cloud.

A. Signature Based IDS

a) C. C. Lo et al. has proposed and simulated an IDS that works in cooperative way to counter the DoS and DDoS attacks [2]. It consists of four components each with a specific role. The first one performs intrusion detection by capturing and analyzing the network packets. It instantly drops the packets exhibiting a correlation with the block table rules, or else the abnormal packets having no correspondence to these rules are forwarded to the alert clustering component which identifies the alert level of received suspicious packet. The third component blocks intrusion packets and sends alerts to other IDSs. The fourth component collects alerts from other IDSs and performs majority vote to make decision about packet. We can protect the system from single point of failure attack by deploying the proposed IDS. However, it cannot detect unknown attacks since it uses signature based detection techniques to detect intrusions.

b) C. Mazzariello et al. has tested the deployment of IDS at various positions in cloud to detect DoS attacks on virtual SIP-based hosts [17]. The authors have utilized Eucalyptus as the cloud and snort as network based IDS to perform the experiments. Two of the six physical machines are hosting eight virtual machines. Two security groups are created, each containing one SIP server, one Apache web server and many RTP –based agents. To generate background traffic, D-ITG is used. "Inviteflood" tool is used to generate the SIP flood traffic. The authors have considered two scenarios to evaluate the IDS performance based on its position in the cloud. Evaluation results have shown that detection of DoS attacks using single IDS instance placed close to the Cloud Controller (CC) will significantly increase the load on CC. Conversely, deployment of separate instance of IDS at each virtual machine affects only the CPU load of attacked VM and there is no significant impact on other VMs. The proposed technique is signature based so unable to detect unknown attacks.

c) A. Bakshi et al. has proposed and implemented a solution for detection of DDoS attacks [18]. The idea is to install IDS (e.g. snort) on a virtual switch which logs the incoming/outgoing traffic to be audited into a database. The IDS performs real-time detection of specific attacks (based on rules) by analyzing the network packets. If IDS observes a large number of packets from specific IP addresses (DDoS attack), it reports to virtual server which blocks IP addresses of all zombies that form the botnet. Moreover, the virtual server shifts the applications under attack to VMs hosted in a separate datacenter and routing tables are updated.

B. Anomaly Based IDS

a) A. Patel et al. has proposed an autonomic agent-based intrusion prevention system using the principles of autonomic computing [20]. The detection methodology is anomaly based. Autonomous sensors are used to monitor the network traffic and system activities (e.g. system calls, file access and modifications) for identification of suspicious incidents. The agents are reconfigurable at runtime with no need to restart them and the system has self-management properties with least human intervention. The prevention system controls these agents by issuing them high-level commands such as the provision of rules to prevent an imminent attack before it happens based on risk analysis and risk evaluation. A layered management model is used to achieve required features. The layers are: Resource Manager, Knowledge and Learning Manager, Risk Manager, Autonomic Element Manager, Autonomic Coordinator, and Integrated Interface.

b) J. H. Lee et al. has proposed a novel approach to detect intrusions based on the anomaly level of users for efficient utilization of resources [21]. The main component of the proposed system is authentication, authorization and accounting (AAA) module. When a user attempts to use cloud services, he is authenticated using AAA module. Upon successful authentication, the anomaly level of user is retrieved which is based on recent information about the user in the database. Consequently, AAA selects the appropriate IDS having security level relevant to the anomaly level of user. The selected IDS is deployed in host operating system (OS) and AAA asks it to assign guest OS for the user. When a guest OS is assigned to the user, a connection is set up between the guest OS and user data in storage center. The security levels of IDS are: High which includes all known attack patterns and a fraction of anomaly method where more security is needed, medium which provides somewhat strong security using all known attack patterns and low which makes use of selected known attack patterns that are more malicious, have high rate of occurrence and cause severe damages to system. So, the proposed method provides high speed of detecting attacks and more guest OS can be assigned since medium-level and low-level IDS use less resources. The proposed system also facilitates the system administrators by letting them audit the logs based on the anomaly level of users.

c) A.V. Dastjerdi et al. has proposed and implemented an intrusion detection system (IDS) which utilizes mobile agents (MA) to detect intrusions in cloud environment [22]. In the proposed model, each subnet of virtual machines (VM) contains an IDS which comprises four main modules: An agency that provides an environment to execute MAs. Static Agent Detector which observes the VMs and upon detection of some suspicious activity, it generates alert, logs information about it and sends alert ID to IDS Control Center (IDS CC). Then, IDS CC sends investigative MAs (IMA) to each agency that generated similar alerts. Each IMA can detect some particular intrusions. The task of IMA is to collect the proofs of an attack for further analysis by visiting all VMs and send the information back to IDS CC. Here, the alerting console compares the doubtful activity with a database of intrusions located in IDS CC and raises an alarm if match is found. A blacklist of all compromised VMs containing their names and identification is sent to all VMs apart from blacklisted VMs. There are three possible types of VM in proposed system: normal, compromised, and migrated. In order to stop

propagation of intrusions, compromised VMs must be banned from migration. The proposed model provides high flexibility and scalability by using MAs. It can detect even new attacks using data mining technique. Attacks on IDS CC are detectable using P2P model. However, when compared to client/server approach, the number of VMs to visit is limited to 6 hosts, and if the limit is exceeded, the network load starts increasing than for client/server design.

d) S. Bharadwaja et al. [29] has proposed a Virtual Machine Monitor (VMM) based technique to detect intrusions in a virtualized environment. The system "Collabra" is integrated with each VMM and acts as an interface between Dom0 of Xen based virtual network and VMM. It monitors the hyper-calls from guest Virtual Machines (VMs) to VMM and analyzes them for anomalies. The reason for using anomaly based detection method is lack of any familiar hyper-call attacks that can be used as signatures. So it can effectively detect unknown attacks. The system works in a collaborative manner since it can communicate with all instances of itself that are deployed on different VMMs. If an intrusion is detected, it instantly uses logical domain channels (LDC) to inform other instances about the features of attack and calls for sanitizing the particular VMM. The hyper-calls are classified as being normal or anomalous based on a threshold value. Collabra system provides two main security components: hyper-call integrity check where Collabra performs cross verification of each hyper-call initiated by a guest VM based on a message authentication code (MAC) and a specific policy for that call. The MAC is helpful in maintaining the integrity of a hypervisor based VM network. The hyper-call origin access where the origin of legitimate hyper-calls is identified by admin version of Collabra. Hyper-calls invoked by locations other than valid applications of guest VMs are marked as untrusted and the related instance of Collabra is informed about the details of such calls. The proposed system can detect collaborative and distributed attacks at the hypervisor layer in real time.

C. Hybrid IDS

a) Ms. Parag K. Shelke et al has proposed a multi-threaded NIDS to solve the problem of Cross Site Scripting (XXS) and DDoS attacks [19]. The proposed NIDS consists of three components each performing a specific role: The *capture module* collects the incoming and outgoing packets (UDP, TCP, ICMP, IP) and transmits to a common queue for evaluation. The *analysis and processing module* evaluates the received data packets by matching them against a knowledge base and a predefined set of rules. The multi-threaded processes in shared queue boost the performance of NIDS. The effective matching and evaluation helps in identification of malicious packets and alert generation. The *reporting module* generates alert reports based on information from shared queue. The third party service observing the entire scenario, instantly informs user about the attack details and provides a consultative report to the service provider. Although it is a novel approach however, the implementation details are not provided to prove the concept.

b) K. Viera et al. has proposed an Intrusion Detection System for Grid and Cloud Computing (GCCIDS) that works at middleware layer and can detect particular intrusions by using a combination of knowledge-based and behavior-based techniques [27]. In this system, every node can identify intrusions and generates alerts for other nodes. So intrusion detection process takes place in a cooperative manner. The four major components of the proposed architecture other than IDS service are: *the node* containing resources to be accessed equally through middleware, *the service* which helps in communication, *the event auditor* which collects data from different sources like service, log system, and node messages. The fourth component is the *storage service* which stores data to be analyzed by IDS service. The authors have evaluated the behavior-based system by measuring false positives and false negatives and concluded that false negatives are always more than false positives when same amount of data is used as input. On the other hand, they have evaluated the knowledge-based system by using audit data from log system and the communication system and concluded that it is possible to analyze the traffic in real-time if limited number of rules are used for comparison. K. Viera et al. has not given implementation details, however they intend to implement it in their future work.

c) In order to tackle both known and unknown attacks, C. N. Modi et al. has proposed and implemented a Network IDS which uses Snort to detect known attacks and Bayesian classifier to detect unknown attacks [5]. The major components of the proposed system are: *Packet Preprocessing*, which takes network packets and eliminates the information that does not associate to detection. *Analyzer*, comprising Bayesian classifier, Snort, and Alert Log, uses signature based or anomaly based detection method to evaluate the packet as being normal or intrusion and if it is an intrusion, records the intrusion using Alert Log and notifies NIDS on other servers which store it in their storage. The Knowledge base and Behavior base present in *Storage* module, store rules of known attacks and normal/intrusion network events respectively. When network packets are captured, first of all, Snort is used for detection and intrusion events are stored in alert database. Next, anomaly detection is performed by first preprocessing the non-intrusion packets and then using Bayesian classifier to calculate their class label (intrusion or normal) by keeping in view the behavior base and finally logging the calculated intrusions into alert database. NIDS set up in all servers work in a collaborative manner by adding the alerts into their knowledge base and thus making detection of unknown attacks easier. In this technique, signature based detection is followed by anomaly based detection, resulting in better detection time since anomaly detection technique detects just unknown attacks. Moreover, detection rate is improved by sending alert to other NIDS deployed in cloud environment.

d) S. N. Dhage et al. [28] has proposed an IDS scheme in which the IDS controller deploys a separate instance of IDS between the user and cloud service provider (CSP) when any user needs to access a cloud service. IDS instance observes all

activities of the user and sends a log of complete session to IDS controller. This information is used to maintain samples of user's activities which are stored in Knowledge Base and help IDS controller in identification of that user on next session and detection of intrusions since Knowledge Base can also discover new samples using neural networks. Different users may also be assigned IDS having different set of rules according to the requirements of each user. The IDS instance should be installed on each layer of cloud i.e. system, platform and application. The proposed intrusion detection techniques include; Signatures, several incorrect passwords for an account, violation of Access rights, and many more. The proposed IDS is able to detect unknown attacks using neural networks, however it is a theoretical model and authors intend to implement it using Eucalyptus cloud.

Now we provide analytical study of covered techniques in the form of a table. (See Table I)

VII. CONCLUSION

The security of Cloud computing model must be considered primarily for its success. In this paper, we have described various intrusions that affect CIA of cloud. Then we have comprehensively illustrated different types of IDS in cloud environment. A detailed description of various intrusion detection techniques is also provided. We have provided the summary in the form of figures and table that are helpful in easily understanding the whole scenario. IDS is the best solution to identify intrusions thus improving the security of cloud. We have analyzed some latest research works that have been proposed to strengthen the cloud security using IDS. The analysis shows that although different IDS techniques have already been proposed which help in detection of intrusions in cloud but they don't provide complete security. Each design lacks some features so we suggest that various detection mechanisms like signature based, anomaly based and soft computing techniques should be integrated to achieve the desired level of security in cloud. Cloud security can be greatly enhanced by utilizing soft computing techniques. However, there are still several challenges and open issues to be considered. For example, integration of IDS in VMs degrades the performance to some extent, high number of false alarms generated by anomaly based techniques, large amount of resources consumed by IDS. Lee et al. [21] has proposed a system to solve the issue of unnecessary resource consuming however, they have not provided any experimental results. In the table, we have provided the limitations of each technique. So these security challenges must be dealt before a standard framework for the security of cloud can be recommended.

TABLE I. ANALYSIS OF CLOUD BASED IDS

Features / References	Detection Technique	IDS Type	Positioning	Detection Time	Data Source	Attacks covered	Limitations/ Challenges
CIDS for Cloud Computing Networks, 2010 [2]	Signature based	Distributed	Each Cloud region	Real time	Network traffic, signatures of known attacks	Protects system from single point of failure, DoS and DDoS	Can't detect unknown attacks, High computational overhead
Securing cloud from DDOS Attacks using IDS in VMs, 2010 [18]		Network based	Virtual Switch	Real time	Network packets, signatures of known intrusions	Secures VMs from DDoS attacks	Detects only known attacks
Integrating a NIDS into an Open Source Cloud Computing Environment, 2010 [17]		Network based	At each node	Real time	Network traffic, normal usage of resources like CPU	Only Known attacks particularly SIP flooding	can't detect unknown attacks,
Autonomic Agent-Based Self-Managed IDPS, 2010 [20]	Anomaly based	Host based	N/A	Real time	Network traffic, System activities (system calls etc.)	Can detect all types of attacks in real-time	Implementation details are not given
Multi-level IDS and Log Management in CC, 2011 [21]		Host based	At each guest OS	Real time	User behaviors, known attack patterns	Can detect both known and unknown attacks at a fast rate	Consumes more resources for high level users
Distributed Intrusion Detection in Clouds using MAs, 2009 [22]		Distributed	At each VM	Real time	Audit data, known intrusion patterns, system logs	Can detect both known and unknown attacks	There is a limit on the number of VMs to be visited
Collabra: Xen Hypervisor based Collaborative IDS, 2011 [29]		VMM based, Distributed	At each VMM	Real time	Audit data, anomaly database	Can detect hyper-call based attacks on VMM and host OS	Cannot detect other types of attacks

IDS for Cloud Computing, 2012 [19]	Hybrid	Distributed	At the processing server	Real time	Audit data, user profiles, signatures of known intrusions	Can help CSP to improve its quality of service, detects unknown attacks	The proposed idea is theoretical, No implementation provided
Bayesian Classifier and Snort based NIDS in Cloud Computing, 2012 [5]		Network based	At the processing servers	Real time	Network packets, known attack signatures, prior events	Detects all types of attacks	Complexity increased due to integration of both, signatures and anomalies
IDS in Cloud Computing Environment, 2011 [28]		Host based and Network based	At each node	Real time	Logs of user activities, signatures of known attacks	Can detect all known attacks, may detect unknown attacks using ANN	Experimental results are not given
GCCIDS, 2010 [27]		Host based	At each node	Real time	Audit data, user profiles	Known attacks, Unknown attacks using ANN	Accurate detection requires more training time, there is a limit on number of rules.

REFERENCES

[1] P. Mell, T. Grance, "The NIST Definition of Cloud Computing ", Special Publication 800-145, Sep. 2011.

[2] C. C. Lo, C. C. Huang, J. Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", 39th International Conference on Parallel Processing Workshops 2010, pp. 280-284.

[3] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan, "A Survey of Intrusion Detection Techniques in Cloud", Journal of Network and Computer Applications 36 (2013), pp. 42–57.

[4] R. Quick, "5 reasons enterprises are frightened of the cloud", http://thenextweb.com/insider/2013/09/11/5-reasons-enterprises-are-frightened-of-the-cloud, 2013.

[5] C. N. Modi, D. R. Patel, A. Patel, R. Muttukrishnan, "Bayesian Classifier and Snort based Network Intrusion Detection System in Cloud Computing", Third International Conference on Computing, Communication and Networking Technologies, 26th-28th July 2012.

[6] R. Bace, P. Mell, "Intrusion Detection Systems", National Institute of Standards and Technology (NIST), Technical Report, 800-31, 2001.

[7] U. Oktay, O. K. Sahingoz, "Proxy Network Intrusion Detection System for Cloud Computing" , ISBN: 978-1-4673-5613-8, 2013, IEEE, pp. 98-104.

[8] S. T. King, P. M. Chen, Y-M. Wang et al., "SubVirt: Implementing malware with virtual machines", 2006 IEEE symposium on security and privacy, 2006, pp. 314–27.

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

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

[11] NIST: National Vulnerability database, http://web.nvd. nist.gov/view/vuln/detail?vulnId=CVE-S2009-3733; 2011.

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

[13] M. Slaviero, "Black Hat presentation demo vids", Amazon, http://www.sensepost. com/blog/3797.html, 2009.

[14] A. Patel, M. Taghavi, K. Bakhtiyari, J. C. Ju´nior, "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Overview", Journal of Network and Computer Applications 36 (2013), pp. 25–41.

[15] H. J. Liao, C. H. R. Lin, Y. C. Lin, K. U. Tung, "Intrusion Detection System: A Comprehensive Review" , Journal of Network and Computer Applications 36 (2013), pp. 16-24.

[16] K. Scarfone, P. Mell, "Guide to Intrusion Detection and Prevention Systems", National Institute of Standards and Technology (NIST), Technical Report, 800-94, Feb. 2007.

[17] C. Mazzariello, R. Bifulco and R. Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment", 2010 Sixth International Conference on Information Assurance and Security, pp. 265-270.

[18] A. Bakshi, Yogesh B, "Securing cloud from DDOS Attacks using Intrusion Detection System in Virtual Machine", 2010 Second International Conference on Communication Software and Networks, pp. 260-264.

[19] Ms. P. K. Shelke, Ms. S. Sontakke, Dr. A. D. Gawande, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012, pp. 67-71.

[20] A. Patel, Q. Qassim, Z. Shukor, J. Nogueira, J. Júnior and C. Wills, "Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System", *Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)*, pp. 223-234.

[21] J. H. Lee, M. W. Park, J. H. Eom, T. M. Chung, "Multi-level Intrusion Detection System and Log Management in Cloud Computing", ICACT, 2011, pp. 552-555.

[22] A. V. Dastjerdi, K. A. Bakar, S. G. H. Tabatabaei, "Distributed Intrusion Detection in Clouds using Mobile Agents", Third International Conference on Advanced Engineering Computing and Applications in Sciences, 2009, pp. 175-180.

[23] J. Han, M. Kamber, "Data Mining: Concepts and Techniques", 2nd edition, Morgan Kaufmann publishers, 2006.

[24] L. M. Ibrahim, "Anomaly Network Intrusion Detection System based on Distributed Time-delay Neural Network", Journal of Engineering Science and Technology, 2010, 5(4), pp. 457-471.

[25] Y. Dhanalakshmi, I. Ramesh Babu, "Intrusion Detection using Data Mining along Fuzzy Logic and Genetic Algorithms", International Journal of Computer Science and Security, 2008, 8(2), pp. 27-32.

[26] W. Li, "A Genetic Algorithm Approach to Network Intrusion Detection", SANS Institute, 2004.

[27] K. Vieira, A. Schulter, Carlos B. Westphall, and C. M. Westphall, "Intrusion Detection for Grid and Cloud Computing", IEEE Computer Society, (July/August 2010), pp. 38-43.

[28] S. N. Dhage, B. B. Meshram, R. Rawat, S. Padawe, M. Paingaokar, A. Misra , "Intrusion Detection System in Cloud Computing Environment", *International Conference and Workshop on Emerging Trends in Technology (ICWET 2011), pp. 235-239.*

[29] S. Bharadwaja, W. Sun, M. Niamat, F. Shen, "Collabra: A Xen Hypervisor based Collaborative Intrusion Detection System", Eighth International Conference on Information Technology: New Generations, 2011, pp. 695-700.