A Review on Intrusion Detection Techniques for Cloud Computing and Security Challenges

Snehal G. Kene
Department of Computer Science and Engineering
G. H. Raisoni College of Engineering,
Nagpur(MS), India
e-mail: snehalkene@gmail.com

Deepti P. Theng
Department of Computer Science and Engineering
G. H. Raisoni College of Engineering,
Nagpur(MS), India
e-mail: dipti.theng@raisoni.net

***Abstract*—** Nowadays, Cloud Computing is the first choice of every IT organization because of its scalable and flexible nature. However, the security and privacy is a major concern in its success because of its open and distributed architecture that is open for intruders. Intrusion Detection System (IDS) is the most commonly used mechanism to detect various attacks on cloud. This paper shares an overview of different intrusions in cloud. Then, we analyze some existing cloud based intrusion detection systems with respect to their various types, positioning, detection time, detection techniques, data source and attacks. The analysis also provides limitations of each technique to determine whether they fulfill the security needs of cloud computing environment or not. We highlight the deployment of IDS that uses multiple detection methods to manage with security challenges in cloud.

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

I. INTRODUCTION

As Cloud Computing is the rapidly growing field of IT. Cloud Computing is defined as an Internet based computing in which virtually shared servers that is data centers provide software, platform, infrastructure, policies and many resources [1]. A cloud data center can be defined from a different perspectives, and the most popular are categorized by IaaS, PaaS, and SaaS proposed by the NIST [2]. SaaS, systems offer complete online applications that can be directly executed by their users. IaaS, allows their customers to have access to whole virtual machines. PaaS offers development and deployment tools, languages and APIs used to build and run applications like Google App Engine, Microsoft's Azure. These services are provided by the Internet. There are four deployment models for cloud computing: public, private, community and hybrid cloud. Public cloud is proposed to be used by public and managed by a business association. Private cloud is deployed for a particular association having multiple users and managed by that particular association. Community cloud is developed for the particular group of users from organizations having same goals. It can be managed by any association within that group or a third party user. Hybrid cloud consists of two or more different cloud infrastructures [3].

The main objective of the cloud computing is that the customers use and pay only for what they want. But as more and more information of individuals and companies are placed in the cloud data centers, the questions arise regarding to the safety and security of cloud environment. Cloud Computing can be easily targeted by attackers [4]. The common network attacks affect the cloud security at the network layer which includes: Address Resolution Protocol (ARP) spoofing, IP spoofing, port scanning, man-in-middle attack, Routing Information Protocol (RIP) attack, Denial of Service (DoS) and Distributed Denial of Service (DDoS) [5]. Therefore, providers must protect the systems against both insiders and outsider attacks. The traditional network security channels like firewall can be used to stop many outsider attacks but attacks from within the network as well as complicated outsider attacks such as DoS and DDoS attacks can't be control easily by using such mechanism [5]. To overcome such problems, an intrusion detection system (IDS) comes into play. The IDS plays very important role in the security of cloud and instead of detecting only known attacks, it can detect many known and unknown attacks [6]. IDS are defined to preserve the confidentiality, integrity, and availability of network [7]. IDS could be software, hardware or a combination of both. It captures the data from the network under examination and notify to the network manager by mailing or logging the intrusion event [8]. Rest of the paper is structured as follows: Section II describes the literature survey on cloud computing attacks, types of cloud based IDS, detection techniques used by IDS and analysis of

978-1-4788-7225-8/15/$31.00 ©2015 IEEE

existing IDS. Section III concludes our work and section IV contains references.

II. LITERATURE REVIEW

The existing IDS are deployed in traditional manner such as firewall which has lack of scalability and self-adaptability. Moreover, they are not deterministic which makes them unsuitable for cloud environment [9]. To overcome these drawbacks a new IDS have been developed to fulfill the cloud security requirement.

A. Intrusions in Cloud

An intrusion can be anything that can harm a system or a network. The most common attacks that affect the cloud are as follows.

1. Virtual Machine Attacks

Attackers effectively control the virtual machines by compromising the hypervisor. The most common attacks on virtual layer are SubVir, BLUEPILL, and DKSM which allow hackers to manage host through hypervisor. Attackers easily target the virtual machines to access them by exploiting the zero-day vulnerabilities in virtual machines [10] this may damage the several websites based on virtual server [11].

2. U2R (User to root attacks)

The attacker may hack password to access a genuine user's account which enables him to obtain information about a system by exploiting vulnerabilities. This attack violates the integrity of cloud based systems [4].

3. Insider Attacks

The attackers can be authorized users who try to obtain and misuse the rights that are assigned to them or not assigned to them [4].

4. Denial of Service (DoS) attack

In cloud computing, the attackers may send huge number of requests to access virtual machines thus disabling their availability to valid users which is called DoS attack [4]. This attack targets the availability of cloud resources.

5. Port Scanning

Different methods of port scanning are SYN, ACK, TCP, FIN, UDP scanning etc. In cloud computing environment, attackers can determine the open ports using port scanning and attack the services running on the same ports [4]. This attack may loss the confidentiality and integrity on cloud.

6. Backdoor path attacks

Hackers continuously access the infected machines by exploiting passive attack to compromise the confidentiality of user information. Hacker can use backdoor path to get control of infected resource launches DDoS attack [4]. This attack targets the privacy and availability of cloud users.

B. Types of Intrusion Detection System in Cloud Computing

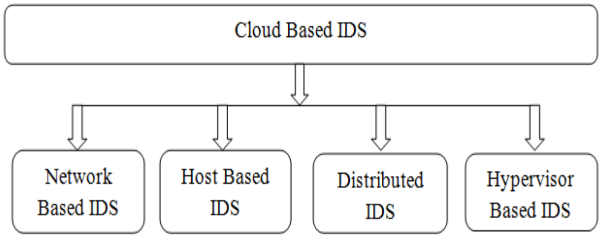

Fig. 1 Types of Cloud based IDS

In the Cloud computing environment, the deployment of already obtainable intrusion detection system and prevention systems (ID/PS) can't succeed the specified level of security and performance because the architecture of cloud computing concept which is different from existing computing methods like Grid computing. A. Patel et al. [9] have introduced the need of IDPS. For this, authors recommended the use of four new ideas namely; involuntary computing, fuzzy theory, ontology, and risk management. Fuzzy logic works on the basis of degrees between 0 and 1 or true and false. It is a probabilistic approach reaches a conclusion rather than using correct values.

The detection techniques used by IDS can be signature based, anomaly based and hybrid technique. The integration of soft computing techniques like Fuzzy Logic, Support Vector Machines (SVM), Artificial Neural Networks (ANN), association rules and Genetic Algorithms (GA) or a hybrid combination of any of these, increase the performance of signature based or anomaly based IDS [4]. There are four types of Cloud computing based IDS. These types are shown in Fig. 1 We will explain each of them in the following subsections.

1. Network based IDS (NIDSs)

NIDS capture the traffic from network and analyze that traffic to detect possible intrusions like DoS attacks, port scanning, etc. NIDS collects the network packets and find out their relationship with signatures of known attacks or compare the user's current behavior with already known attacks in real-time.

2. Host based IDS (HIDS)

HIDS gather the information from a particular host and analyze it to detect unauthorized events. The information can be system logs of operating system. HIDS analyzes the information, if there is any change in the behavior of system or program; it instantly report to network manager that the system is in danger. HIDS are mainly used to protect the integrity of software [7].

3. Hypervisor based IDS

Hypervisor provides a level for interaction among VMs. Hypervisor based IDSs is placed at the hypervisor layer. It helps in analyze the available information for detection of anomalous actions of users. The information is based on communication at multiple levels like communication between VMs, VM and hypervisor, and communication within the hypervisor based virtual network [4].

4. Distributed IDS (DIDS)

A Distributed IDS contains number of IDSs such as NIDS, HIDS which are deployed over the network to analyze the traffic for intrusive detection behavior. Each of these individual IDSs has its two components: detection component and correlation manager [9]. Detection component examine the system's behavior and transmits the collected data in a standard format to the correlation manager. Correlation manager combines data from multiple IDS and generate high level alerts that keep up a correspondence to an attack. Analysis phase makes use of signature based and anomaly based detection techniques so DIDS can detect known as well as unknown attacks.

C. Analysis of Existing Intrusion Detection Techniques Used by IDS

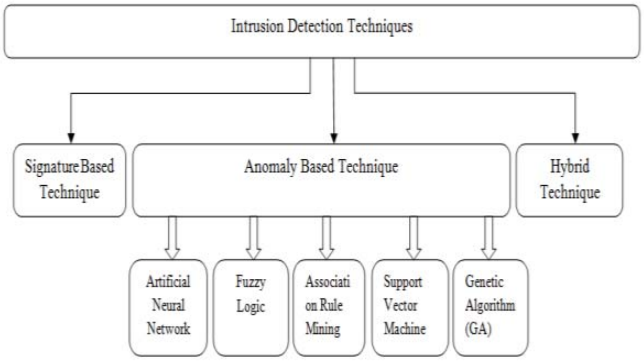

Fig. 2 Types of Intrusion Detection Techniques

The most common intrusion detection techniques used by IDS are based on behavior of users and signatures of known attacks. To improve the performance of IDS, it is better to use a combination of these techniques. This is shown in Fig. 2. Each technique is described in the following sub sections:

1. Signature Based Detection

Signature based detection is performed by comparing the known information with the database of signatures. A signature can be previously defined set of rules or patterns that are related to known attacks. Signature based technique is also recognized as misuse detection technique [12]. However, it is unable to identify unknown attacks in cloud [4]. Mazzariello et al. in [13], Bakshi et al. in [14], and Lo et al. in [3] have used signature based detection method to detect intrusions in cloud.

a) C. C. Lo et al. has proposed and implement IDS that works in supportive way to oppose the DoS and DDoS attacks [3]. It consists of four components. The first component performs intrusion detection by collecting and analyzing the network packets. The second component immediately drops the packets and check it whether it is correspondence with the block table rules or not, if packets having no autonomic element manager, autonomic coordinator, and correspondence to these rules are forwarded to the alert clustering module which generates alert for suspicious packet. The third component blocks the suspicious packets and sends alerts to other IDSs. The fourth component collects alerts and makes decision about packet. We can protect the system from single point of failure attack by deploying the above proposed IDS. However, it cannot detect unknown attacks since it uses signature based detection techniques to detect intrusions.

b) C. Mazzariello et al. have tested the deployment of IDS at different positions in cloud to detect DoS attacks [19]. The authors have considered two scenarios to calculate the IDS performance based on its position in the cloud. Calculation results have shown that detection of DoS attacks using single IDS instance located close to the Cloud Controller (CC) which will significantly increase the load on CC. On the other hand, deployment of split instances 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 [14]. The idea is to deploy the IDS on a virtual switch which collects logs of incoming and outgoing traffic and store into a database. The IDS detects particular attacks (based on rules) by analyzing the network packets. If IDS observes a large number of packets from same IP addresses (DDoS attack), it immediately reports to virtual server which blocks that particular IP addresses of all zombies that form the botnet.

2. Anomaly Based Detection Technique

Anomaly based detection technique compares current user activities against previously loaded logs of users. It produces a large number of false alarms because of irregular network and user behavior. It also requires huge data sets to train the system for normal user profiles [7].

In anomaly detection system, unknown attacks can be detected at different levels. Monitoring intrusions from large data becomes difficult at different levels (system, network) of cloud. A. Patel et al. in [16], Lee et al. in [17] and Dastjerdi et al. in [18] have used anomaly based intrusion detection system to detect intrusions in cloud.

a) A. Patel et al. have projected an involuntary agent-based intrusion prevention system using the principles of involuntary computing [16]. They used autonomous sensors to monitor the network traffic and system activities for identify the suspicious incidents. The system has self-management properties with less human interaction therefore the agents are reconfigurable at runtime with no need to restart them. The prevention system controls these agents to prevent attacks which are about to happen 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.

b) J. H. Lee et al. has proposed a new approach for detecting intrusions based on the anomaly level for efficient utilization of resources [17]. The main factor of the proposed system is authorization, accounting and authentication (AAA) module. When a user starts to use cloud services, he is authenticated using AAA module. Accordingly, AAA selects the suitable IDS which are having security level applicable to the anomaly level of user. The IDS which is selected by AAA is deployed in host operating system (OS) and asks it to assign guest OS for the user. When a guest OS is assigned, a connection is set up between the users data in storage center and guest OS. The IDS includes all known attack patterns and an anamaly method where more security is required. IDS provides strong security using all known attack patterns and low security which use selected known attack patterns that are more malicious. So, the proposed method provides high speed of security for detecting attacks.

3. Hybrid Detection Technique

The hybrid intrusion detection system is the combination of signature and anomaly based detection method which is called as hybrid detection technique. The idea behind the implementation of hybrid detection is to detect both known and unknown attacks based on signature and anomaly detection techniques [9]. Viera et al. in [17], C. N. Modi et al. in [5] have used hybrid detection techniques to improve the efficiency of IDS.

a) K. Viera et al. have projected IDS for Grid and Cloud Computing (GCCIDS). IDS works at middleware layer and it can detect specific intrusions by using a combination of knowledge and behavior based techniques [13]. In this system each node identifies the intrusion and generates alert to another nodes present in the system since the system works in cooperative manner. The authors have proposed the behavior based system by measuring false positives and false negatives and concluded that false negatives are always more than false positives when similar quantity of data is used as input. On the other hand, they have evaluated the knowledge based system by using audit data from system log and communication system and concluded that it is possible to analyze the traffic in real-time if inadequate number of rules are used for comparison. Viera et al. has not specified implementation details.

b) C. N. Modi et al. has proposed and implemented a Network intrusion detection system (NIDS) which uses Snort to detect known attacks and Bayesian classifier to detect unknown attacks [5]. NIDS deployed in all servers work in a collaborative approach by generating alerts into knowledge base and thus making detection of unknown attacks easier. In the given technique, signature based detection is followed by anomaly based detection, since it detects just unknown attacks. However, detection rate is increased by sending alert to other NIDS deployed in cloud environment.

Now we provide analytical study of above techniques in tabular format.

Table I. Analysis of Intrusion Detection Techniques in Cloud Computing

Features References	Detection Technique	IDS Type	Positioning	Detection Time	Data Source	Attacks covered	Limitations/ Challenges
CIDS for Cloud Computing Networks, 2010 [3]	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 [14]		Network based	At each 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 [13]		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-		Host based	N/A	Real time	Network	Can detect	Implementation details are

Based Self-Managed IDPS, 2010 [16]	Anomaly based				traffic, System activities (system calls etc.)	all types of attacks in real-time	not given
Multi-level IDS and Log Management in CC, 2011 [17]		Host based	At each guest OS	Real time	User behaviours, known attack patterns	Can detect known and unknown attacks at a fast rate	Consumes more resources for high level users
Distributed Intrusion Detection in Clouds using MAs,2009 [18]		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 [21]		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 [15]	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
GCCIDS, 2010 [19]		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.
IDS in Cloud Computing Environment, 2011 [20]		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
Bayesian Classifier and Snort based NIDS in Cloud Computing, 2012 [4]		Network based	At the processing server	Real time	Network packets, known attack signatures, prior events	Detects all types of attacks	Complexity increased due to integration of both, signatures and anomalies

III. CONCLUSION

In this paper, we have described number of intrusions that affect confidentiality, integrity, and availability of cloud. We have comprehensively described different types of IDS that are used by cloud environment. We have provided the summary of intrusion detection techniques in the form of figures and table that are helpful in easily understanding the whole scenario cloud computing. We analyze the different techniques of IDS this 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.

REFERENCES

[1] Shefali Singh, Krati Saxena, Zubair Khan "Intrusion Detection Based On Artificial Intelligence Techniques", International Conference Of Advance Research And Innovation (Icari-2014).

[2] Zhen Chen, Wenyu Dong, Hang Li, Peng Zhang, Xinming Chen, And Junwei Cao"Collaborative Network Security In Multi-Tenant Data Center For Cloud Computing", Tsinghua Science And Technology 1, February 2014.

[3] 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.

[4] 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.

[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. 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.

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

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

[9] 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.

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

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

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

[13] 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.

[14] 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.

[15] 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

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] Theng, D.; Hande, K.N., "VM Management for Cross-Cloud Computing Environment," Communication Systems and Network Technologies (CSNT), 2012 International Conference on , vol., no., pp.731,735, 11-13 May 2012

[23] Theng, D., "Efficient Heterogeneous Computational Strategy for Cross-Cloud Computing Environment," Emerging Research in Computing, Information, Communication and Applications (ERCICA), 2014 Second International Conference on, vol., no., pp.8,17, 1-2 August 2014

[24] Gourkhede, M.H.; Theng, D.P., "Analysing Security and Privacy Management for Cloud Computing Environment,"Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on , vol., no., pp.677,680, 7-9 April 2014

[25] Gourkhede, M.H.; Theng, D.P., "Preserving Privacy and Illegal Content Distribution for Cloud Environment," International Journal of Computing and Technology (IJCT), 2014, vol., no.1, issue 3, pp.142,148, May 2014.