IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-6, Issue-3 E-ISSN: 2347-2693

An analysis On Security Concerns and Their Possible Solutions in Cloud Computing Environment

Naveen Chandra1, Parag Rastogi2*, Amit Asthana3

[1] Department of CSE, SITE, Swami Vivekanand Subharti University, Meerut (UP), India
[2*]Department of CSE, SITE, Swami Vivekanand Subharti University, Meerut (UP), India
[3]Department of CSE, SITE, Swami Vivekanand Subharti University, Meerut (UP), India

Corresponding Author: parag0305@gmail.com, Tel.:+91-9568390091

Available online at: www.ijcseonline.org

Received: 19/Feb//2018, Revised: 25/Feb2018, Accepted: 17/Mar/2018, Published: 30/Mar/2018

Abstract- Cloud computing offers services with much flexibility and very less infrastructure because of the distributed structure of cloud computing, this technology is used by an increasing number of end users. On the other hand, cloud computing presents an added level of risk because clouds are distributed in nature, so it becomes an easy targets for the intruders to exploit the vulnerabilities of the network. Therefore in this paper we have discussed the need of security mentioning different types of attacks which affect the availability, confidentiality and integrity of resources and services in cloud computing environment and suggested the cloud providers to protect the user data and information from inside or outside attacks by installing an intrusion detection and prevention system.

Keywords- Cloud Computing, Attacks, Intrusion Detection System, Intrusion Prevention System.

I. INTRODUCTION

Cloud Computing:

Cloud computing provides the next generation of internet based, highly scalable distributed computing system in which computational resources are offered 'as services'. The computing environment composed of IT components (hardware, software, networking, and services) as well as the processes around the deployment of these elements that together enable us to develop and deliver cloud services via the Internet or a private network.

Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet.

While moving from traditional local computing paradigm, new security and privacy challenges emerge because of the distributed nature of cloud computing. Cloud computing organizations have to provide a high quality service and protect the users' sensitive data, to prevent these attackers; firewall mechanism and/or Intrusion Detection are effective solutions to resist them. They can provide additional protection mechanisms on the cloud systems' distributed environments. IDS send an alert message to a person to trigger some actions for preventing these attacks.

Cloud service delivery models:

There are various Cloud service delivery models that are developed which can be divided into the following three layers:

Software as a Service (SaaS):

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). SaaS is a model for which the applications are hosted as services to a customer who access it via the Internet. When the software is hosted off-site, the customer does not have to maintain it.

Platform as a Service (PaaS):

The capability provided to the consumer is to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services. On the contrary to SaaS, PaaS delivers the cloud services differently. As the name suggests, PaaS supplies all the resources required to build applications and service completely from the Internet without having to download or install any kind of software. The services provided in PaaS model include application design, development testing, deployment, hosting, web service integration and database integration.

Infrastructure as a Service (IaaS):

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Before analyzing security challenges in Cloud Computing, we need to understand the relationships and dependencies between these cloud service models. PaaS as well as SaaS are hosted on top of IaaS; thus, any breach in IaaS will impact the security of both PaaS and SaaS services, but also it may be true on the other way around. However, we have to take into account that PaaS offers a platform to build and deploy SaaS applications, which increases the security dependency between them. As a consequence of these deep dependencies, any attack to any cloud service layer can compromise the upper layers. Each cloud service model comprises its own inherent security flaws; however, they also share some challenges that affect all of them. These relationships and dependencies between cloud models may also be a source of security risks. A SaaS provider may rent a development environment from a PaaS provider, which might also rent an infrastructure from an IaaS provider. Each provider is responsible for securing his own services, which may result in an inconsistent combination of security models. It also creates confusion over which service provider is responsible once an attack happens.

Cloud deployment models:

These are commonly known as Public, Private, and Hybrid models. The following sections use the National Institute of Standards and Technology definition of cloud to introduce these different types of cloud.

Public cloud:

According to NIST, a public cloud is one in which the infrastructure is open to the general public for consumption. Due to the nature of public clouds, they are exposed to a higher degree of risk.

Private cloud:

According to NIST, a private cloud is provisioned for exclusive use by a single organization comprising multiple consumers, such as business units. It may be owned, managed, and operated by the organization, a third-party, or some combination of them.

Community cloud: NIST defines a community cloud as one whose infrastructure is provisioned for the exclusive use by a specific community of consumers from organizations that have shared concerns. For example, mission, security requirements, policy, and compliance considerations. It may be owned, managed, and operated by one or more of the organizations in the community, a third-party, or some combination of them. Hybrid cloud : The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

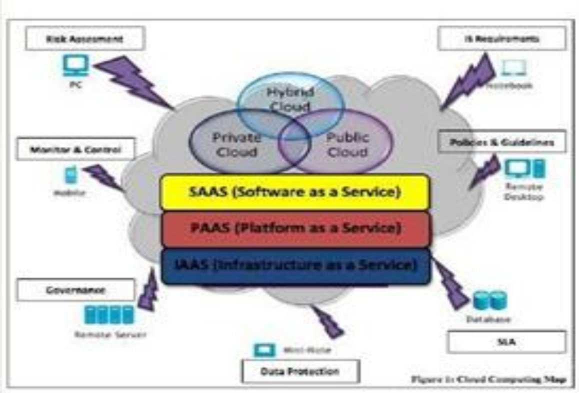

Fig 1: Cloud Computing Environment

The rest of this paper is organized as follow: Portion I contains the introduction of the Cloud Computing, its environment and the delivery models of Cloud service, portion II contains the need of security in Cloud Computing environment, portion III describes the various attacks in Cloud Computing, portion IV contains the overview of Host based IDS, Network based IDS, and Distributed IDS in a Cloud System. Portion V contains the overview of intrusion prevention in Cloud Computing, portion VI contains the detection techniques used by IDS, portion VII describes the challenges in IDS and in the last portion conclusion and future work are presented.

II. NEED OF SECURITY IN CLOUD COMPUTING ENVIRONMENT

While moving from traditional computing paradigm to cloud computing paradigm new security and privacy challenges has emerged. Security of the cloud computing system can be thought in two dimensions: physical security and cyber security.

Physical security concerns the physical properties of the system. For example, a data center, which is owned by provider infrastructure, has to realize security standards and hold security certifications globally; supervision and manageability on security preventions, incombustibility, uninterrupted power supplies, precautions for natural disasters (earthquake, flood, fire etc.) are indispensable. However twenty four hours and seven days monitoring for heat, humidity and air condition systems and also some biometric entrance systems may help for the business continuity.

Cyber security defines the prevention of system from cyber world. There is a risk of cyber security attacks on services of cloud computing system. These attack can use huge amounts of computing resources, disables their usage by consumer efficiently. In this section mostly known attack types are detailed.

Attacks in cloud computing

Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks.

Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging. When the Cloud Computing operating system notices the high workload on the flooded service, it will start to provide more computational power (more virtual machines, more service instances) to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold. In that sense, the Cloud system is trying to work against the attacker (by providing more computational power), but actually—to some extent—even supports the attacker by enabling him to do most possible damage on a service's availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all n servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service.

Need of security in cloud computing environment

While moving from traditional computing paradigm to cloud computing paradigm new security and privacy challenges has emerged. Security of the cloud computing system can be thought in two dimensions: physical security and cyber security.

Physical security concerns the physical properties of the system. For example, a data center, this is owned by provider infrastructure, has to realize security standards and hold security certifications globally, supervision and manageability on security preventions, incombustibility, uninterrupted power supplies, precautions for natural disasters (earthquake, flood, fire etc.) are indispensable. However twenty four hours and seven days monitoring for heat, humidity and air condition systems and also some biometric entrance systems may help for the business continuity.

Cyber security defines the prevention of system from cyber world. There is a risk of cyber security attacks on services of cloud computing system. These attack can use huge amounts of computing resources, disables their usage by consumer efficiently. In this section mostly known attack types are detailed.

II. ATTACKS IN CLOUD COMPUTING Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks.

Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging. When the Cloud Computing operating system notices the high workload on the flooded service, it will start to provide more computational power (more virtual machines, more service instances) to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold. In that sense, the Cloud system is trying to work against the attacker (by providing more computational power), but actually—to some extent—even supports the attacker by enabling him to do most possible damage on a service's availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all n servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service.

Attacks on virtualization

There are mainly two types of attacks performed over virtualization: VM Escape and Rootkit in hypervisor.

VM Escape: In this type of attack, an attacker's program running in a VM breaks the isolation layer in order to run with the hypervisor's root privileges instead with the VM privileges. This allows an attacker to interact directly with the hypervisor. Therefore, VM Escape from the isolation is provided by the virtual layer. By VM Escape, an attacker gets access to the host OS and the other VMs running on the physical machine.

Rootkit in Hypervisor: VM-based rootkits initiate a hypervisor compromising the existing host OS to a VM. The new guest OS assumes that it is running as the host OS with the corresponding control over the resources, however, in reality this host does not exist. Hypervisor also creates a covert channel to execute unauthorized code into the system. This allows an attacker to control over any VM running on the host machine and to manipulate the activities on the system. This type of intrusion can be realized with writing an excessive amount of data to a statically defined buffers' capacity, and the information is captured by intruders from this overflowed data. An attacker who owned the account and password information of an authorized user can hold the access privilege to servers and also to virtual machines.

Man-in-the Middle attack:

If secure socket layer (SSL) is not properly configured, then any attacker is able to access the data exchange between two parties. In Cloud, an attacker is able to access the data communication among data centers. Proper SSL configuration and data communication tests between authorized parties can be useful to reduce the risk of Man-in-the-Middle attack.

Backdoor channel attack

It is a passive attack, which allows hackers to gain remote access to the compromised system. Using backdoor channels, hackers can be able to control victim's resources and can make it a zombie for attempting a DDoS attack. It can also be used to disclose the confidential data of the victim. Better authentication and isolation between VMs can provide protection against such attacks.

Port scanning: An attack that identifies open, closed and filtered ports on a system. In port scanning, intruders can seize information with the help of open ports like services that run on a system, IP and MAC addresses which belong to a connection and router, gateway and firewall rules. TCP, UDP, SYN/FIN/ACK and Window scanning are the most common scanning attacks. Port scanning is not used by its own, an intruder realize the actual attack after getting information about open ports and running services.

III. INTRUSION DETECTION IN CLOUD COMPUTING

Intrusion Detection Systems (IDSs) are one of the practical solutions to resist these attacks. IDSs are systems that realize intrusion detection, log detected information, alert or perform predefined procedures. They can be either hardware or software that includes whole observed computing entities. It does not mean every detected suspicious event is an intrusion. Some unexpected events can occur rarely, and it is a crucial point to decide if they are an intrusion or not. Mainly there are three types of IDS in cloud computing systems: Host based IDS, Network based IDS, and Distributed IDS.

Host based IDS: Host audit sources are the only way to gather information on the activities of the users of a given machine. Thus, Host Intrusion Detection Systems (HIDS) are present on each host that requires monitoring and collects data concerning the operation of this host. This usually consists of log files, network traffic to and from the host, or information on processes running on the host. HIDS can determine if an attempted attack was indeed successful and can detect local attacks, privilege escalation attacks, and attacks that are encrypted. However, such systems can be difficult to deploy and manage, especially when the number of hosts needing protection is large. Furthermore, these systems are unable to detect attacks against multiple targets on the network. Host based Intrusion Detection System (HIDS) involves software or agent components, which monitors the dynamic behavior and state of the computer system. HIDS software runs on the server, router, switch or network machines. The agent version has to report to a console or it can run on together on the same host. Like buffer overflow, rootkit, format string etc. The software creates log files of the system in the form of sources of data. The host based IDS looks at communication traffic and checks the integrity of system files to keep an eye on suspicious processes. Host based IDS doesn’t provide good real time response.

Network based IDS: Network Intrusion Detection Systems (NIDS) monitor the traffic on the network containing the hosts to be protected and are usually run on a separate machine, called a sensor. NIDS are able to monitor a large number of hosts with relatively little deployment cost and are able to identify attacks to and from multiple hosts. However, they are unable to detect whether an attempted attack was successful, and are unable to deal with local or encrypted attacks.

Network based Intrusion detection system (NIDS) attempts to discover unauthorized access to a computer network by capturing the network traffic packets such as TCP, UDP and IPX/SPX and analyzes the content against a set of rules. Like Eavesdropping, data modification, identity or IP Address Spoofing, Denial-of-Service (DoS) attacks, Man-in-the-Middle Attack etc. NIDS consist of a set of single-purpose sensors that are placed at various points in the network. These sensors monitor and analyze network traffic and send report of attack to the centralized console. The deployment of NIDS has a minute effect on the performance of the network.

Distributed IDS

Distributed Intrusion Detection System (DIDS) is a intrusion detection system in a distributed environment such as grid and cloud computing. The DIDS uses multiple IDSs to protect a distributed system. Distributed IDSs (DIDSs) are based on distributed IDS entities located on different locations within the network, which monitor separately and communicate and cooperate with each other. The DIDS allows computation load and diagnostic responsibilities to be distributed throughout the network. It can provide the foundation for a complete solution to the complexities of real-time detection, while maintaining fault tolerance behavior. It allows early detection of planned and coordinated attacks, thereby allowing network administrators to take preventive measures. DIDS also helps to control the spreading of worms, improves network monitoring, incident analysis, attack tracing and so on. Also, it has scalability to detect general attacks or a specific attack, in addition to providing significant advantages in flexibility, extendibility, and resistance to compromise.

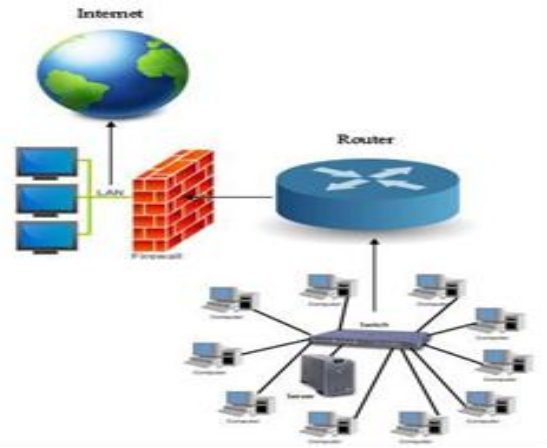

Fig 2: Process of HIDS

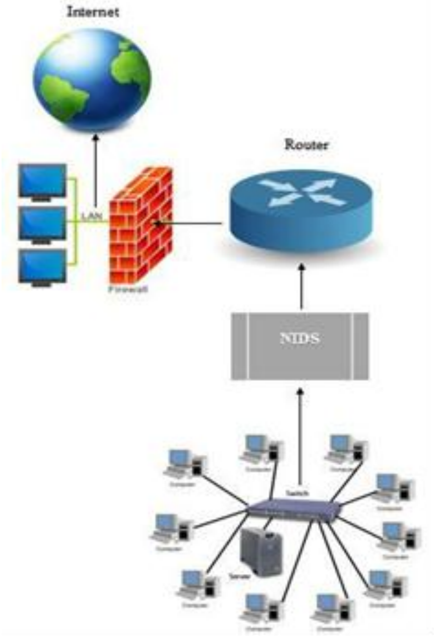

Fig 3: Process of NIDS

V. INTRUSION PREVENTION SYSTEM IN CLOUD COMPUTING

\An Intrusion Prevention System (IPS) holds all capabilities of IDSs and plus prevention characteristics. The IPS often sits directly behind the firewall and is provides a complementary layer of analysis that negatively selects for dangerous content. Unlike its predecessor the Intrusion Detection System (IDS)—which is a passive system that scans traffic and reports back on threats—the IPS is placed inline (in the direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network. Specifically, these actions include:

•Sending an alarm to the administrator
•Dropping the malicious packets
•Blocking traffic from the source address
•Resetting the connection

As an inline security component, the IPS must work efficiently to avoid degrading network performance. It must also work fast because exploits can happen in near real-time. The IPS must also detect and respond accurately, so as to eliminate threats and false positives (legitimate packets misread as threats).

VI. 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.

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. 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.

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

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 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.

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.

VII. CHALLENGES IN INTRUSION DETECTION SYSTEM

There are few shortcomings which are inherent when IDSs are constructed. The few common shortcomings are:

Lack of Efficiency IDSs are often required to evaluate events in real time. This requirement is difficult to meet when faced with a very large number of events as is typical in today's networks.

High Number of False Positives Most IDSs detects attacks throughout an enterprise by analyzing information from a single host, a single application, or a single network interface, at many locations throughout the network. False alarms are high and attack recognition is not perfect.

Limited Flexibility Intrusion detection systems have typically been written for a specific environment and have proved difficult to use in other environments that may have similar policies and concerns. The detection mechanism can also be difficult to adapt to different patterns of usage.

Range of Attacks As new attacks are conceived, IDSs must be updated to discover them. While new attacks are added frequently, old ones can seldom be dropped.

End-to-end Encryption With security improvements in communications protocols, the ability to encrypt traffic on an end-to-end basis are on the rise.

High Speed Communications Higher communication traffic rates directly affect the processing speed needed to analyze packet content, potentially resulting in lost packets.

VIII. CONCLUSION

Cloud computing provides internet based distributed computing environment where computational resources are offered 'as services' such as software, platform, storage and information which are provided to customers on demand, due to which it becomes an easy targets for the intruders to exploit the weakness of the network. Cloud Computing has the potential to become a frontrunner in promoting a secure, virtual and economically feasible IT solution in the future. In this paper, we have discussed each of the three cloud models, their security risks and covered the study of intrusion detection and prevention system and we reached to the conclusion that the existing IDS are not the solution to all security concerns and we need to propose some new techniques or methods which enhances the security performance and to find out the new types of attacks in cloud computing environment. The same becomes the future work of this paper.

REFERENCES

[1] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp. 347-358.

[2] Zhang S, Zhang S, Chen X, Huo X(2010) Cloud Computing Research and Development Trend in Second International Conference on Future Networks, Sanya, Henan, China, IEEE Computer Society, Washington, DC, USA, pp. 93-97

[3] B R. Kandukuri, R. Paturi V.and A. Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Services Computing, Sep 21-25,2009, Bangalore, India, pp. 517-520.

[4] E. H. Spafford and D. Zamboni, "Intrusion Detection Using Autonomous Agent," Computer Networks, Vol. 34, Issue 4, 2000, pp. 547-570.

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

[6] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Clouding Computing Networks," 2010, 39th International Conference on Parallel Processing Workshops, pp. 280-284.

[7] Anna Lenart, "ERP in the Cloud- Benefits and Challenges,"Springer Verlag Berlin Heidelberg, 2011, pp. 39-50.

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

Authors Profile

Naveen Chandra is currently a Ph.d Scholar in Department of Computer Science and Engineering, Swami Vivekanad Subharti University, Meerut, UP, India. His area of interest include Cloud Computing and IoT.

Parag Rastogi is currently working as Assistant Professor at Department of Computer Science and Engineering, Swami Vivekanand Subharti University, Meerut, UP, India. He has done M. Tech (CS), M.Sc. in Computer Science and B.Tech (CSE). He is a life member of ISTE and IAENG. His areas of interest include Artificial Intelligence, Software Testing and Cloud Computing.

Dr.Amit Asthana is currently working as Associate Professor at Department of Computer Science and Engineering, Swami Vivekanand Subharti University, Meerut, UP, India. He has done Ph.D. (CS)