ijesm
Consulting, help, education
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

CLOUD COMPUTING: SECURITY ISSUES AND ITS DETECTION METHODS

Akanksha Parashar and Archana Borde
Asst. Professor, Dept. of CSE,
RKDF College of Technology and Research, Bhopal, (M.P.)-India

ABSTRACT

Security provides to many organizations is a big deal at a present scenario. Cloud computing is a technology that uses the internet where data is stored and maintain in the data center of a cloud provider like Google, Amazon , IBM and Microsoft etc. cloud computing system provides various services to user with best affords but they faces many difficulties regarding security problems. and users also afraid towards security own data that is whether clouds providers are able to maintain data integrity , confidentiality as well as authentication.it is necessary that cloud computing providers are aware their users from inside or outside attacks by installing an intrusion detection and prevention system. In this paper we can define different types of attacks and provides the most suitable countermeasures for them. Additionally the paper also introduces related IDS models to detect & prevent these type of attacks.

Key words: Cloud computing, Security, Threats, countermeasures and IDS

INTRODUCTION

Cloud computing is not an innovation, but a means to constructing IT services that use advanced computational power and improved storage capabilities.Cloud computing provides computation, software applications, data access, data management and storage resources without requiring cloud users to know the location and other details of the computing infrastructure. cloud computing is a technology that uses the internet and center remote servers to maintain data and application .cloud computing allows consumer and businesses to use applications without installation and access their personal files at any computer with internet access.

***Corresponding Author**
Email – akanksha.parashar1@gmail.com
archana.borde11@gmail.com

Cloud Computing Threats

Threat: is an actor who wants to attack assets in the cloud at a particular time with a particular goal in mind, usually to inflict his own financial gain and consequentially financial loss of a customer.Before deciding to migrate to the cloud, we have to look at the cloud security vulnerabilities and threats to determine whether the cloud service is worth the risk due to the many advantages it provides. The following are the top security threats in a cloud environment:

Ease of Use: The cloud services can easily be used by malicious attackers, since a registration process is very simple, because we only have to have a valid credit card. In some cases we can even pay for the cloud service by using PayPal, Western Union, Payza, Bitcoin, or Litecoin, in which cases we can stay totally anonymous. The cloud can be used maliciously for various purposes like spamming, malware distribution, botnet C&C servers, DDoS, password and hash cracking.

Secure Data Transmission: When transferring the data from clients to the cloud, the data needs to be transferred by using an encrypted secure communication channel like SSL/TLS. This prevents different attacks like MITM attacks, where the data could be stolen by an attacker intercepting our communication.

Insecure APIs: Various cloud services on the Internet are exposed by application programming interfaces. Since the APIs are accessible from anywhere on the Internet, malicious attackers can use them to compromise the confidentiality and integrity enterprise customers. An attacker gaining a token used by a customer to access the service through service API can use the sametoken to manipulate the customer's data. Therefore it's imperative that cloud services provide a secure API, rendering such attacks worthless.

Malicious Insiders: Employees working at cloud service provider could have complete access to the company resources. Therefore cloud service providers must have proper security measures in place to track employee actions like viewing a customer's data. Since cloud service provides often don't follow the best security guidelines and don't implement a security policy, employees can gather confidential information from arbitrary customers without being detected.

Shared Technology Issues: The cloud service SaaS/PasS/IaaS providers use scalable infrastructure to support multiple tenants which share the underlying infrastructure. Directly on the hardware layer, there are hypervisors running multiple virtual machines, themselves running multiple applications.

On the highest layer, there are various attacks on the SaaS where an attacker is able to get access to the data of another application running in the same virtual machine. The same is true for the lowest layers, where hypervisors can be exploited from virtual machines to gain access to all VMs on the same server (example of such an attack is Red/Blue Pill). All layers of shared technology can be attacked to gain unauthorized access to data, like: CPU, RAM, hypervisors, applications, etc.

Data Loss: The data stored in the cloud could be lost due to the hard drive failure. A CSP could accidentally delete the data, an attacker might modify the data, etc. Therefore, the best way to protect against data loss is by having a proper data backup, which solves the data loss problems. Data loss can have catastrophic consequences to the business, which may result in a business bankruptcy, which is why keeping the data backed-up is always the best option.

Data Breach: When a virtual machine is able to access the data from another virtual machine on the same physical host, a data breach occurs – the problem is much more prevalent when the tenants of the two virtual machines are different customers. The side-channel attacks are valid attack vectors and need to be addressed in everyday situations. A side-channel attack occurs when a virtual machine can use a shared component like processor's cache to access the data of another virtual machine running on the same physical host.

Account/Service Hijacking: It's often the case that only a password is required to access our account in the cloud and manipulate the data, which is why the usage of two-factor authentication is preferred. Nevertheless, an attacker gaining access to our account can manipulate and change the data and therefore make the data untrustworthy. An attacker having access to the cloud virtual machine hosting our business website can include a malicious code into the web page to attack users visiting our web page – this is known as the watering hole attack. An attacker can also disrupt the service by turning off the web server serving our website, rendering it inaccessible.

Unknown Risk Profile: We have to take all security implications into account when moving to the cloud, including constant software security updates, monitoring networks with IDS/IPS systems, log monitoring, integrating SIEM into the network, etc. There might be multiple attacks that haven't even been discovered yet, but they might prove to be highly threatening in the years to come.

Denial of Service: An attacker can issue a denial of service attack against the cloud service to render it inaccessible, therefore disrupting the service. There are a number of ways an attacker can disrupt the service in a virtualized cloud environment: by using all its CPU, RAM, disk space or network bandwidth.

Lack of Understanding: Enterprises are adopting the cloud services in every day operations, but it's often the case they don't really understand what they are getting into. When moving to the cloud there are different aspects we need to address, like understanding how the CSP operates, how the application is working, how to debug the application when something goes wrong, whether the data backups are already in place in case the hard drive dies, etc. If the CSP doesn't provide additional backup of the data, but the customer expects it, who will be responsible when the hard drive fails? The customer will blame the CSP, but in reality it's the customer's fault, since they didn't familiarize themselves enough with the cloud service operations – the result of which will be lost data.

User Awareness: The users of the cloud services should be educated regarding different attacks, because the weakest link is often the user itself. There are multiple social engineering attack vectors that an attacker might use to lure the victim into visiting a malicious web site, after which he can get access to the user's computer. From there, he can observe user actions and view the same data the user is viewing, not to mention that he can steal user's credentials to authenticate to the cloud service itself.

Security awareness an often overlooked security concern.

Cloud computing vulnerabilities

Vulnerability: is a weakness that can be exploited by the attacker for his own personal gain. A weakness can be present in software, environments, systems, network, etc.

When deciding to migrate to the cloud, we have to consider the following cloud vulnerabilities:

Session Riding: Session riding happens when an attacker steals a user's cookie to use the application in the name of the user. An attacker might also use CSRF attacks in order to trick the user into sending authenticated requests to arbitrary web sites to achieve various things.

Virtual Machine Escape: In virtualized environments, the physical servers run multiple virtual machines on top of hypervisors. An attacker can exploit a hypervisor remotely by using a vulnerability present in the hypervisor itself – such vulnerabilities are quite rare, but they do exist. Additionally, a virtual machine can escape from the virtualized sandbox environment and gain access to the hypervisor and consequentially all the virtual machines running on it.

Reliability and Availability of Service: We expect our cloud services and applications to always be available when we need them, which is one of the reasons for moving to the cloud. But this isn't always the case, especially in bad weather with a lot of lightning where power outages are common. The CSPs have uninterrupted power supplies, but even those can sometimes fail, so we can't rely on cloud services to be up and running 100% of the time. We have to take a little downtime into consideration, but that's the same when running our own private cloud.

Insecure Cryptography: Cryptography algorithms usually require random number generators, which use unpredictable sources of information to generate actual random numbers, which is required to obtain a large entropy pool. If the random number generators are providing only a small entropy pool, the numbers can be brute forced. In client computers, the primary source of randomization is user mouse movement and key presses, but servers are mostly running without user interaction, which consequentially means lower number of randomization sources. Therefore the virtual machines must rely on the sources they have available, which could result in easily guessable numbers that don't provide much entropy in cryptographic algorithms.

Data Protection and Portability: When choosing to switch the cloud service provider for a cheaper one, we have to address the problem of data movement and deletion. The old CSP has to delete all the data we stored in its data center to not leave the data lying around.

Alternatively, the CSP that goes out of the business needs to provide the data to the customers, so they can move to an alternate CSP after which the data needs to be deleted. What if the CSP goes out of business without providing the data? In such cases, it's better to use a widely used CSP which has been around for a while, but in any case data backup is still in order.

CSP Lock-in: We have to choose a cloud provider that will allow us to easily move to another provider when needed. We don't want to choose a CSP that will force us to use his own services, because sometimes we would like to use one CSP for one thing and the other CSP for something else.

Internet Dependency: By using the cloud services, we're dependent upon the Internet connection, so if the Internet temporarily fails due to a lightning strike or ISP maintenance, the clients won't be able to connect to the cloud services. Therefore, the business will slowly lose money, because the users won't be able to use the service that's required for the businessoperation. Not to mention the services that need to be available 24/7, like applications in a hospital, where human lives are at stake.

Intrusion Detection in cloud computing

Intrusion detection are one of the practical solutions to resist these attacks. IDSs are systems that realize intrusion detection,log detected informationalert or perform predefined proceduresThey 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.

A.Host-based Intrusion Detection Systems

Host Based IDSs analyze the suspicious activities like system call, processes or thread, asset and configuration access by observing the situation of host. It is especially used to protect valuable and private information on serversystems. HIDSs are able to assign as NIDS if they are installed on a single host and configured to detect network activities. HIDS is composed of sensors located on servers or workstations which are madeto prevent the attacks to a host. An HIDS is not just monitor network traffic, it can also race more and settle with local settings of an OS and log records.

B.Network-based Intrusion Detection Systems

Network-based IDSs (NIDS) observe, monitor and analyses the specified and pre-identified network traffic. It can detect different situations based on

specified points and generally located between the end point devices like routers, firewalls. A NIDS is an intrusion detection system that attempts to discover unauthorized access to a network by analyzing traffic on the network for signs of malicious activities and events. Network traffic stacks on different layers and every layer delivers the data coming from a layer to another layer. OSI reference model and TCP/IP model define how these layers works and manages the traffic.

C.Distributed Intrusion Detection Systems

Distributed Intrusion Detection System (DIDS) is the way of intrusion detection in a distributed environment such as grid and cloud computing . All the components in the distributed area communicate eachother with an agent-based approach. There are three fundamental components and assignments are similar to other types of IDSs' components. Main subject in DIDSs deal whole system like a traditional network or host . DIDS components do not have a worldwide accepted standard, but there are network and host based sensor components, detection engine and management component.

D.Network Behavior Analysis Intrusion Detection

Network Behavior Analysis Intrusion Detection (NBAD) is an intrusion detection methodology which is providing to decide if the network traffic is suspicious or not by the statistical data and formal situation of network traffic Sensors detect DoS attacks with the help of to be aware of the network traffic and unexpected application services andrule violations by scanning the network. Traditional NIDSs and NBAD systems share some common components like sensors and management consoles, but NBAD systems generally do not have database servers, unlike the traditional NIDSs. NBAD systems work to decide in the case ofunexpected data traffic.it is generally efficient to detect DOS, attacks and worms.

INTRUSION PREVENTIONSYSTEMS

An Intrusion Prevention System (IPS) holds all capabilities of IDSs and plus prevention characteristics . IPSs can interfere most of the component in prevented environment. In a nutshell, security of a system has some
traditional steps. There will be a firewall, IDS, IPS and guard system behind modem, router or switches where ever it is needed. IPSs can change configurations ofmanageable computing entities. If an intrusion detected by the mechanism, a firewall rule can be applied, a routing configuration can be changed, or a virtual machine can be
isolated among security procedures.In cloud computing, intrusion detection and prevention transactions and processes are a challenging issue because of many reasons. Fundamentally, because of the distributed nature of the cloud computing systems, all monitored and prevented resources are takenplace in many different locations. Sometimes, they will bein different countries. So that, intrusion detection sensors placement, collecting
intrusion data, analyzing by detection engines and interfering for prevention precautions are not easy to implement and apply. At the same time, load balancing, allocation of CPU and memory, deciding for positive and negative rates, bandwidth usage and so the whole price because of pay per usage model is the areas to be overcome.

Proxy Network Intrusion Detection System for Cloud Computing is introduced to minimize expenditures of hardware usage.

NIDS in a virtualization based cloud environment by putting on intrusion detection assignment on a different entity in the network. So the expenditures of hardware usage (CPU and memory) aimed to be reduced. Studies and models must study and concentrate for the most effective and proactive detection and prevention approaches.

CONCLUSION

Cloud computing is a emerged technology & it is widely accepted computing paradigm all around the world by its advantage on quick deployment & cost efficiency but inspite of these advantages cloud computing is not suitable for security & privacy concerns. This paper represents security issues of cloud computing in terms of attacks types & provides detection methods by means of intrusion detection and prevention system.

REFERENCES

[1] U. Oktay and O.K. Sahingoz"Attack Types and Intrusion Detection Systems in Cloud Computing ".6th, IISCCTurkey.

[2] Vahid Ashktorab2, Seyed Reza Taghizadeh1 Security Threats and Countermeasures in Cloud Computing , *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.comVolume 1, Issue 2, October 2012

[3]Mahbub Ahmed, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010, Australia.

[4] Siani Pearson. Taking Account of Privacy when Designing Cloud Computing Services. *CLOUD '09: Proceedings of the 2009ICSE Workshop on Software Engineering Challenges of Cloud Computing*, pages 44-52.
May 2009

[5]Jianfeng Y; Zhibin C; (2010), "Cloud Computing Research and Security Issues", IEEE 2010

International Conference onComputational Intelligence and Software Engineering (CiSE), pp1, 10-12 Dec 2010.
[6]Karamjit Singh, Karamjit Singh, NavdeepKaur "Security issues occur in Cloud Computing and there Solutions" International Journal on Computer Science and Engineering (IJCSE)
[7] Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems Harley Kozushko Thursday, September 11, 2003Independent Study.
[8] Liazhu Dai and QinZhou, A PKI-based Mechanism for Secure and Efficient Access to Outsourced Data, 201O InternationalConference on Networking and Digital Society 640-643

[9] William Stallings: Cryptography and Network Security [book style].

[10]P. Mell and T. Grance, "The NIST Definition of Cloud ComputingNIST Special Publication 800-145 (SP800-145)," National Institute of Standards and Technology, Gaithersburg, September 2011.
[11]U. Tupakula V. Varadharajan and N. Akku, "Intrusion Detection Techniques for Infrastructure as a Service Cloud," Proc. IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, Sydney, 2011, pp. 744- 751.