International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2016, pp. 317-323
e-ISSN:2278-621X

SECURITY ISSUES RELATED TO CLOUD COMPUTING

Avin Pereira, ShubhamChavan and Mithun D'Souza

Dept. of Software Technology AIMIT, St. Aloysius College, Mangalore
Dept. of Software Technology AIMIT, St. Aloysius College, Mangalore
Dept. of MCA AIMIT, St. Aloysius College, Mangalore

Abstract— Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet.This paper aims to present information about the most recent threats, attacks on cloud computing and we also discuss Various categories of security measures such as trust, identity management, software isolation, data protection, confidentiality and availability.

Keywords—Cloud data security, Data concealment, Data Encryption, Encryption algorithm, Threats and Attacks on the Cloud

I. INTRODUCTION

The cloud computing is the next stage in the Internet's growth, providing the means finished which everything — from computing power to computing infrastructure, applications, business processes to personal partnership — can be delivered to you as a service wherever and whenever you need. Cloud Computing seems as a movement of architecture and its main objective is to provide safe, quick, suitable data storage and net computing service, with all computing resources visualized as services and delivered over the Internet.The cloud improves partnership, agility, scalability, accessibility, ability to adapt to variations according to demand, accelerate development work, and provides potential for cost reduction through enhanced and effective computing.

In RFC 2828 [4], threat is identified as A potential for violation of security, which exists when there is a situation, capability, action, or event that could breach security and cause harm. On the other hand, the same RFC identifies an attack as an attack on system security that derives from a smart threat, i.e., an intellectual act that is a deliberate attempt to evade security services and violate the security policy of a system. In general, computer security identifies three main objectives:

- ✓ *Confidentiality*: Promising that data is available only to entitled entities and no unauthorized access to data can be obtained.
- ✓ *Integrity*: Assuring that data has not been altered in any way. while it is stored or while its transport over the network.
- ✓ *Authentication*: Assuring the identity of the entity involved in the communication.

.

II. SERVICE MODELS OF CLOUD COMPUTING IS DIVIDED INTO THREE CATEGORIES:

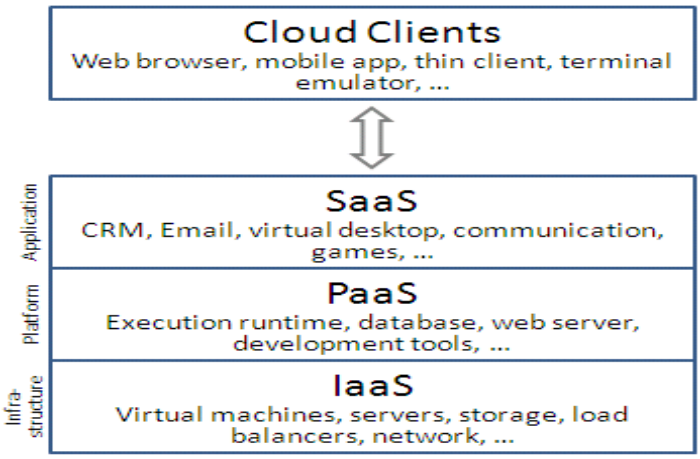

Figure 1. Cloud Models or Layers

- IaaS (Infrastructure as a Service), it completely distracted the hardware working behind it and allowed users to consume infrastructure as a service without any awkwardness about the underlying complications.
- PaaS (Platform as a Service), it builds upon IaaS and provides clients with access to the basic operating software and optional services to develop and use software applications without software installation.
- SaaS (Software as a Service) allows the user to access online applications and software that are hosted by the service providers.

Securing data is always of vital importance and because of the critical nature of cloud computing and large amounts of complex data it carries, the need is even important.

III. THREATS

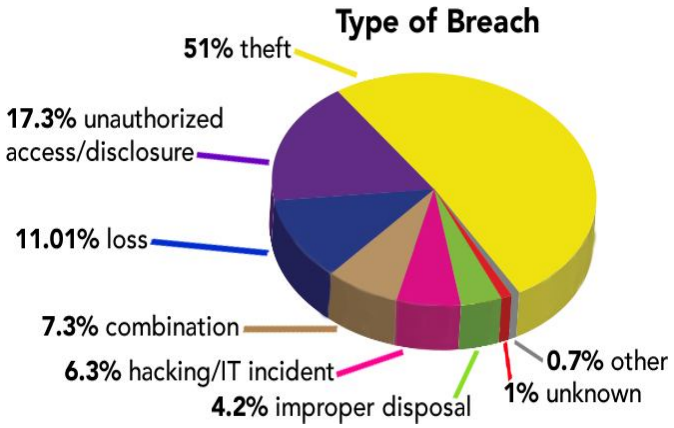

Figure 2. Types of Breaches

A. Data breaches:

Cloud computing face many threats when compared outdated business networks, but due to the large amount of data stored on cloud servers, providers(ISP) become the favorite target. The

brutality of damage tends to depend on the sensitivity of the amount of data exposed. Exposed personal financial information tends to get the headlines, but breaches involving health information, trade secrets, and intellectual property can be more devastating and disturbing. When a data breach occurs, business companies have to face fines, or they may face complaints or criminal charges. Breach surveys and customer notifications can increase significant costs. Unintended effects, such as brand damage and loss of business, can impact organizations for years.One way of removing data breaches is to encrypt all of the client's data. However, if the encryption key is lost, the client would have a complete data loss. Thus, the client wouldneed to have a backup copy of the data, somewhere else, or even o□ine backup.

B. Data Loss:

A data breach is the result of a malicious and probably intrusive action. Data loss may occur when a disk drive dies without its owner having created a backup. It occurs when the owner of the encrypted data loses the key that unlocks it. Small amounts of data were lost for some Amazon Web Service customers as its EC2 cloud suffered "a remirroring storm" due to human operator error on Easter weekend in 2011.And a data loss could occur on intentionally in the event of a malicious attack.

C. *Shared Technology Issues:*

The cloud facility SaaS/ PaaS/ IaaS providers use accessible infrastructure to support multiple occupants which share the underlying infrastructure. Directly on the hardware layer, there are hypervisors running several virtual technologies, themselves running numerous applications.On the main layer, there are various attacks on the SaaS where an attacker is able to get access to the data of additional application running in the similar virtual machine. The same is true for the lowermost 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.The brutality of this threat has dropped over the past few years. This drop is due to more precise configuration and segregation by the hardware manufacturers and the cloud service providers. This threat exists in IaaS, SaaS, and PaaS models. The justification of this threat is to be done by the cloud service provider. Keeping systems updated and giving high attention to configuration can reduce the probability of manipulating such vulnerability.

D. Denial of Service:

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

E. IP Spoofing:

IP spoofing, also known as IP address counterfeit or a host file hijack, is a hijacking technique in which a cracker pretends to be a trusted host to hide his identity, spoof a Web site, hijack browsers, or gain access to a network. Here's how it works: The hijacker obtains the IP address of a genuine host and modifies packet headers so that the valid host appears to be the source.A well-known method in the analysis of network traffic. In fact, the attacker sends a message to mainframe user who is dependable, then the system acquires the users IP address, and creates some changes in the packet like header, then sends a package that looks the main package of system user. [2]

F. Insecure Cryptography

Cryptography algorithms usually require random number generators, which use random 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 certainly means lower number of randomization sources. Therefore, the virtual machines must rely on the sources they have available, which could result in effortlessly guessable numbers that don't provide much entropy in cryptographic algorithms.

IV. ATTACKS ON CLOUD COMPUTING

Cloud Computing as any otherplatform, is a target for many attacks. These attacks have different aims starting from stealing of sensitive information to complete System failure.It is vital that these attacks are identified clearly and their mitigation techniques.

A. *Denial-of-Service*

Simply put, a DDoS attack is a nasty attempt to bring down systems, Web-based applications, and/or services by overwhelming these resources with too much data or harming them in some other way. Unlike a denial-of-service (DoS) attack where the source is just a singular computer and connection, a DDoS attack is from multiple sources, and is capable of causing great consequences to a company's brand, status and bottom line.DDoS attacks are designed to target any aspect of a business and its resources, and can easily:

- disable a specific computer, service or an entire network
- target alarms, printers, phones or laptops
- hit system resources like bandwidth, disk space, processor time or routing information
- execute malware that affects processors and triggers errors in computer microcode's
- exploit operating system vulnerabilities to drain system resources
- crash the operating system

i. Volumetric Attacks (connectionless)

Also, known as "floods," the goal of this type of attack is to cause congestion and send so much traffic that it overwhelms the bandwidth of the site. Attacks are naturally performed using botnets, an army of computers infected with malicious software and controlled as a collection of the hacker.

ii. TCP State-Exhaustion Attacks

This type of attack focuses on actual web servers, firewalls and load balancers to disrupt connections, resulting in exhausting their finite number of concurrent connections the device can support.

iii. Application Layer Attacks (connection-based)

This type of attack, also known as Layer 7 attacks, specifically targets weaknesses in an application or server with the goal of establishing a connection and exhausting it by monopolizing the processes and transactions. These sophisticated threats are harder to detect because not many machines are required to attack, generating a low traffic rate that appears to be legitimate.Additionally, an attack can also be a combination of the three types listed above, which makes it even more challenging for organizations to combat.

B. *Man in the cloud Attack*

One of the most common attacks witnessed in 2015 is Man-in-the-Cloud attack, which is an attack that targets file storage/management applications such as drop box and google drive. The attack depends on manipulating the applications synchronization protocols and end-user confirmation token. The attack is built on accessing a targeted victim account by authenticating as the victim without the need to crack their password; which delays the detection process. Cloud file storage and management applications perform user authentication by implementing different mechanisms such as encryption. Man in the Cloud attack comes in various forms such as:

i. *Account Sharing*: This is when an attacker shares the victims account, authenticating as the victim being able to access all the synchronized files and probably operating them.

ii. Credential Swapping: The attacker swaps his verification/synchronization token with the victim's tokens. As a result, the victim is being misled to use the attacker account as if it was his. Authors simulate the Man in the cloud by creating a script.

C. *OpenStack Components Attack*

The main components identified as the core of OpenStack can be separately targeted by attackers due to existing vulnerabilities that can be exploited. Due to unperceived issues, the components couldn't have deployed on the system and therefore none of the vulnerabilities could be verified or attacks could be tested. However, the examples of documented cases are listed below.

i. *Nova:* Nova is the OpenStack compute written in python and it uses the fabric controller. It is considered the main part of the IaaS system as it manages and automates pools of computer resources [1]. Attackers can exploit Nova's network configuration to reach the host on the same virtual network. Booted instances can be used to check the address of the gateway and then connect to the SSHD service on the host system [2].

ii. *Horizon:* Horizon is the recognized implementation of the OpenStack console. It provides the user with an interface to which it allows access to OpenStack services [1]. The attacker can exploit the default settings in the horizon which uses the signed cookie to store the session state on the client side and steal the cookie using sniffing techniques or gaining access to the target system. The attacker can then use the stolen cookie to satirize the target [3].

D. *Throttling*

The process of limiting resource usage to keep a particular process from bogging down and/or crashing a system. Relevant as a countermeasure in DoS attacks, where an attacker attempts to crash the system by overloading it with input.

E. *SQL injection*

Failure to validate input in case where the input is used to construct a SQL statement or will modify the construction of a SQL statement in some way. If the attacker can influence the creation of a SQL statement, he or she can gain access to the database with privileges otherwise privileges are unavailable, and use this in order to steal or modify information or destroy data.

F. *Brute force attacks.*

Attacks that use the raw mainframe processing power to try different variations of any variable that could expose a security hole. For example, if an attacker knew that access required an 8-character username and a 10-character password, the attacker could iterate through every

possible (256 multiplied by itself 18 times) combination in order to attempt to gain access to a system. No intelligence is used to filter or shape for likely combinations.

V. COUNTER MEASURES AGAINST THREATS AND ATTACKS

A. *Auditing and Logging*

- ✓ Utilize application instrumentation to uncover conduct that can be observed.
- ✓ Throttle logging.
- ✓ Strip delicate information before logging.

B. *Authentication*

- ✓ Utilize solid secret key approaches.
- ✓ Try not to store qualifications in an uncertain way.
- ✓ Utilize confirmation instruments that don't require clear content qualifications to be disregarded the system.

C. *Authorization*

- ✓ Attach confirmation to approval on a similar level.
- ✓ Secure framework assets against framework characters.
- ✓ Failing to limit database access to specified stored procedures.
- ✓ Using inadequate separation of privileges.
- ✓ Connection pooling. Permitting over privileged accounts.

D. *Configuration Management*

- ✓ Using insecure custom administration interfaces. [5]
- ✓ Failing to secure configuration files on the server. [5]
- ✓ Storing sensitive information in the clear text. [5]
- ✓ Having too many administrators. [5]

E. *Communication*

- ✓ Use message security or transport security to encrypt your messages. [5]
- ✓ Use proven platform-provided cryptography. [5]
- ✓ Periodically change your keys. [5]
- ✓ Use any platform-provided replay detection features. [5]

F. *Cryptography*

- ✓ Do not develop and use proprietary algorithms (XOR is not encryption. Use established cryptography such as RSA).[5]
- ✓ Avoid key management. [5]
- ✓ Use the RNGCryptoServiceProvider method to generate random numbers [5]

G. *Session Management*

- ✓ Passing session IDs over unencrypted channels.
- ✓ Permitting prolonged session lifetime.
- ✓ Having insecure session state stores. Placing session identifiers in query strings.

VI. CONCLUSION

In this paper, we present information about the most recent threats, attacks on cloud computing and also discussed about Various categories of security measures such as trust, identity management, software isolation, data protection, confidentiality and availability.We need more strict encryption techniques that is able to counter all these attacks. We arrive at a conclusion that as the cloud has increased in its popularity its number of vulnerabilities has also increased hence rendering it to defenseless against the attacks and we need more defensive algorithms that is able to mitigate these threats.

REFERENCES

[1] 'OpenStack Docs: Developers'. [Online]. Available: http://docs.openstack.org/developer/openstack-projects.html

[2] KINDER,' OPENSTACK SOURCE CLOUD COMPUTING SOFTWARE NOVA NETWORK CONFIGURATION ALLOWS GUEST VMS TO CONNECT TOHOSTSERVICES',OPENSTACKCLOUD SOFTWARE,2015.[ONLINE].AVAILABLE: JUNE/038664.

[3] Lists. Open stack. org,' Open Stack Open Source Cloud Computing Software Session-fixation vulnerability in horizon when using the default signed cookie sessions',2014.[online].Available:June/007990.html

[4] Shirey, R.: Rfc 2828: Internet security glossary. The Internet Society, 2000.

[5] D.KishoreKumar,G. VenkatewaraRao,G.Srinivasa Rao, "Cloud Computing:An Analysis, of its challenges & security issues",International Journal of Computer Scaience and Network(IJCSN),Vol1.No.5,October 2012,

[6] https://blogs.msdn.microsoft.com/jmeier/2010/07/08/cloud-security-threats-and-countermeasures-at-a-glance/