Volume 5, Issue 4, April 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Issues at Different Levels in Cloud Computing

Dr. Rajesh Pathak
Head of Department,
Computer Science & Engineering,
Uttar Pradesh Technical University, India

Priya Sharma
Research Scholar, M. Tech.,
Computer Science & Engineering,
Uttar Pradesh Technical University, India

Abstract— Information Technology infrastructure continues to grow with growing technology. The use of mobile devices and computer has increased due to the innovation of the Internet. Nowadays, many persons in the world use these devices. Every Internet user is accessing cloud services either directly or indirectly without aware of security aspects Cloud computing is not just a service of computing or how the computing service is delivered. Cloud computing has raised with a assurance to decrease the cost of computing implementation and deliver the computing as service, where the client only pay for what he needed and want to used. Security and privacy is the main hurdle in the cloud environment because of its open and distributed architecture. In this paper we discussed the security issues at level in cloud.

Keywords— Cloud Computing, Threats, Security in cloud, Risks in cloud, Cloud management.

I. INTRODUCTION

Cloud computing is a new computing model, which comes from the concept of grid computing, distributed computing, virtualization technology and other computing technologies[1]. The cloud computing changes the style of software .The data can be stored in the cloud environment can be accessed from anywhere anytime due to the distributed architecture of cloud environment. Now a day most of the small and medium business organisation tending towards the cloud platform and putting their application and data in to the cloud.

NIST (National Institute Of Standard & Technology) [5] defines Cloud Computing as a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources such as (network, servers, storage, applications and services) that can be rapidly provisioned and reduced with minimal management effort or service provider interaction.

NIST [5], defines cloud computing by describing five essential characteristics, three cloud service models & four deployment model as shown in Fig. 1.

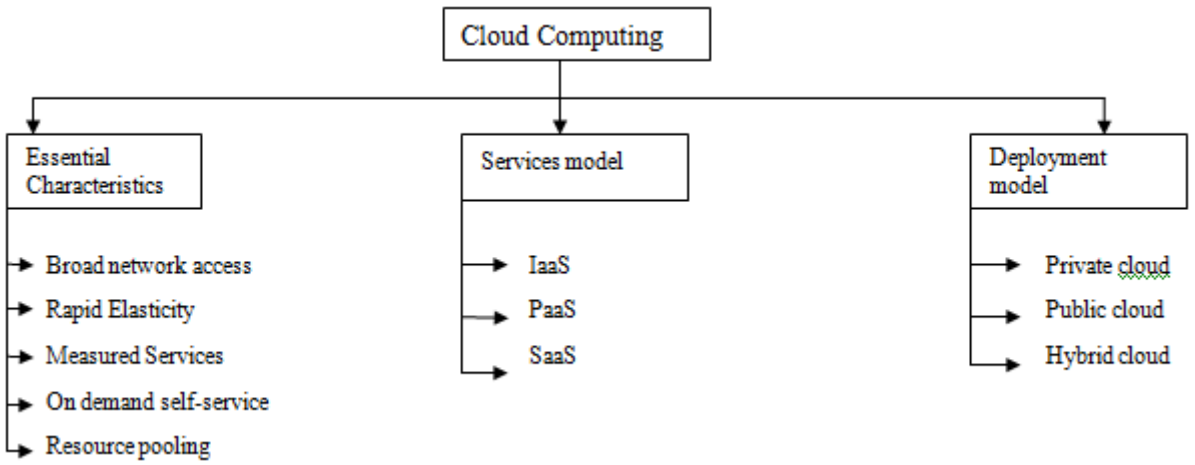

Figure 1

The Cloud Computing model can be seen as a combination of three service delivery models and three deployment models [6].

The deployment models are:

- **Private cloud:** a cloud platform that is committed for explicit organization,
- **Public cloud:** it's openly available to public users to register and use the infrastructure in accordance to their utility, and
- **Hybrid cloud:** It's an arrangement of private cloud that can extend to use resources in public clouds. Among all these, the most vulnerable deployment models are public models because they are available for public users to host their services and they may be malicious users.

The cloud service delivery models, as in figure, include:

- **Infrastructure-as-a-service (IaaS):** where cloud providers deliver computation resources, storage and network as an internet-based services. This service model is based on the virtualization technology. The most familiar IaaS provider is Amazon EC2.
- **Platform-as-a-service (PaaS):** where cloud providers deliver platforms, tools and other business services that gives the ability to customers to develop their own applications, and they can also manage the applications by themselves, removing the need of installing any platforms or support tools on their devices. The PaaS model may be hosted on top of IaaS model or on top of the cloud infrastructures directly. The most known PaaS provider are Google Apps and Microsoft Windows Azure
- **Software-as-a-service (SaaS):** where cloud providers deliver applications hosted on the cloud infrastructure as internet based service for end users, without requiring installing the applications on the customers' computers. This model may be hosted on top of PaaS, IaaS or directly hosted on cloud infrastructure. An example of the SaaS provider is SalesForce.

Characteristics of Cloud Computing

a. Broad network access: Various client platforms like laptops, tablets, mobile phones can be used to access these capabilities that are available over the network.

b. On-demand self-service: Without the human interaction with each service provider a consumer can provision computing capabilities automatically as and when required.

c. Rapid Elasticity: A user can quickly acquire more resources from the cloud by scaling out . They can scale backing by releasing those resources once they are no longer required.

d. Resource pooling: Multiple consumers are served with the providers pooled computing resources using a model, with different virtual and physical resources dynamically assigned and reassigned depending on the demand of consumer.

e. Measured Service: Resources usage is metered using suitable metrics such as monitoring storage usage, CPU hours, bandwidth usage etc.

Cloud Computing has advantages and disadvantages. Disadvantages of cloud computing are security threats for cloud computing customer. Disadvantages are generally about security.

II. CLOUD COMPUTING SERVICE DELIVERY MODELS SECURITY ISSUSES

We will summarize the key security issues / vulnerabilities in each service delivery model. Some of these issues are the responsibility of cloud provider while others are the responsibility of cloud consumer.

A. IaaS Issues

1) VM security: It includes securing the VM operating systems and workloads from common security threats such as malware and viruses. It can be achieved by using traditional or cloud-oriented security solutions. The VM's security is the responsibility of cloud consumers. Each cloud consumer can use their own security controls based on their wants, estimated risk level, and their own security management process.

2) Securing VM images repository: unlike physical servers VMs are still under risk even when they are offline. VM images can be compromised by injecting malicious codes in the VM file or even stole the VM file itself. Secured VM images repository is the responsibilities of the cloud providers. Another issue related to VM templates is that it may preserve the original owner information, which might be used by a new consumer.

3) Virtual network security: sharing of network infrastructure among different tenants within the same server (using vSwitch) or in the physical networks will increase the possibility to exploit vulnerabilities in DNS servers, **DHCP, IP** protocol vulnerabilities, or even the vSwitch software which result in network-based VM attacks.

4) Securing VM boundaries: VMs have virtual boundaries compared with to physical server ones. VMs that co-exist on the same physical server share the same CPU, Memory, I/O, NIC, and others (i.e. there is no physical isolation among VM resources). Securing VM boundaries is the responsibility of the cloud provider.

5) Hypervisor security: a hypervisor is the "virtualizer" that maps from physical resources to virtualized resources and virtualized resources to physical resources. Any negotiation of the hypervisor violates the security of the VMs because all VMs operations become traced unencrypted. One of the responsibilities of cloud providers and the service provider is hypervisor security. The SP is the company that delivers the hypervisor software such as VMware or Xen.

B. PaaS Security Issues

1) SOA related security issues: the PaaS model is based on the Service-oriented Architecture (SOA) model. This leads to inheriting all security issues that exist in the SOA domain such as DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks. Mutual authentication, authorization and WS-Security standards are important to secure the cloud provided services. This security issue is a shared responsibility among cloud providers, service providers and consumers.

2) API Security: PaaS may offer APIs that deliver management functions such as business functions, security functions, application management, etc. Such APIs should be provided with security controls and standards implemented, such as OAuth [9], to enforce consistent authentication and authorization on calls to such APIs. Moreover, there is a need for the isolation of APIs in memory. This issue is under the responsibility of the cloud service provider.

C. SaaS Security Issues

In the SaaS model enforcing and maintaining security is a shared responsibility among the cloud providers and service providers (software vendors). The SaaS model inherits the security issues discussed in the previous two models as it is built on top of both of them including data security management [10] and network security.

1) Web application vulnerability scanning: web applications to be hosted on the cloud infrastructure should be validated and scanned for vulnerabilities using web application scanners [11]. This should be updated with the recently discovered vulnerabilities and attack paths maintained in the National Vulnerability Database (NVD) and the Common Weaknesses Enumeration (CWE) [12]. Web application firewalls should be in place to mitigate existing/discovered vulnerabilities (examining **HTTP** requests and responses for applications specific vulnerabilities).

2) Web application security miss-configuration and breaking: One of an important issue in SaaS is web application security miss-configuration or weaknesses. Security miss-configuration is also very critical with multi-tenancy where each tenant has their own security configurations that may conflict with each other leading to security holes. To manage security in a reliable, dynamic and robust way it is mostly recommended to depend on cloud provider.

III. SECURITY THREATS IN CLOUD COMPUTING

The aim of cloud computing models (CCM) is to reduce operational costs and, to allow IT departments focus on strategic projects instead of being concerned only in keeping their data centres working [7]. With such benefits, CC has become a world trend and an area of strong investments. According to Gartner [2], the financial investment on CC in 2016 will have a Global Compounded Annual Growth Rate (CAGR) of: IaaS: 41%, PaaS: 26.6% and SaaS: 17.4% in 2016 [2]. In this scenario, there is a growing concern in relation to the security of the services provided. In the same Gartner survey, the category Management and Security will have a CAGR of 27.2%. The security policies are present in the Quality of Service term (QoS), specified in the Service Level Agreement (SLA).

Truthfully, many solutions are being proposed in literature. However the resulting problems from Security Threats to Cloud Computing Models (STCCM) are even newer. Those threats compromise the CIA of the resources provided. Currently, we may consider seven different threats:

- Abuse and Nefarious Use of Cloud Computing,
- Insecure Interfaces and APIs,
- Malicious Insiders,
- Shared Technology Issues,
- Data Loss or Leakage,
- Account or Service Hijacking and
- Unknown Risk Profile [3].

One of the reasons why those threats are quite challenging is because in Cloud Computing the computational resources are the result of homogeneous data centres. This characteristic means that there is not an individual and proper management for each data centre, making harder the adoption of an efficient security model that fulfils the specifications of the security policies [4].

A. Abuse and Nefarious Use of Cloud Computing

Cloud service provider provides various types of services including unlimited bandwidth and storage capacity. Free limited trial periods are offered by various cloud service provider that gives an opportunity for hackers to access the cloud immorally, their impact includes launching potential attack points, decoding and cracking of passwords and executing malicious commands. As cloud service providers are targeted for their weak registration systems and limited fraud detection capabilities, Spammers, malicious code authors and other cyber criminals can conduct their activities with relative impunity. For example some cybercriminals use rich content applications such as flash files that enable them to hide their malicious code and utilize users browsers to install malware. The consequence of this Threat helps the growth of plagues such as botnets, from which come problems like Distributed Denial of Service (DDoS), solves of Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), storage of malicious files and botnet networks [3].

This Threat evidences the fact that today it is very easy to any user to take on a cloud computing solution, it is also possible to get a free evaluation time having only a official credit card, which could come from a robbery or fraud. This ends up encouraging the action of malicious people to introduce spam, malwares or even to practice unlawful activities on the cloud [3].

B. Insecure Interfaces and APIs

To access and manage the cloud services cloud users are using software APIs and interfaces. These APIs need to be protected because they play a vital part during provisioning, organization and monitoring of the processes running in a cloud environment. The availability and security of cloud services is reliant upon the security of these APIs so they should include features of verification, access control, encryption and activity monitoring. APIs must be intended to defend against both accidental and malicious attempts to avoid threats. If cloud service provider depends on weak set of APIs, diversity of security issues will be raised related to privacy, integrity, availability and accountability such as malicious or anonymous access, API dependencies, limited monitoring/logging capabilities, inflexible access controls, mysterious access, reusable tokens/passwords and inappropriate authorizations.

C. Malicious Insiders

Insider attacks can be performed by malicious employees at the provider's or user's site. Malicious insider can steal confidential data of cloud. This type of threat can shatter the expectation of cloud users on provider. Cryptographic keys, files and password can be easily obtained by malicious insider. These attacks may involve various types of scam, spoil or stealing of information and misuse of IT resources. Due to lack of transparency in cloud provider's processes and procedures the threat of malicious attacks has increased [2]. It means that a provider may not reveal how employees are granted access and how this access is monitored or how reports as well as policy compliances are analysed. Additionally, users have slight visibility about the hiring practices of their provider that could open the door for an opponent, hackers or other cloud intruders to steal confidential information or to take control over the cloud. The stage of access granted could be helpful for the attackers to collect confidential data or to gain complete control over the cloud services with little or no risk of detection. The financial value as well as brand reputation of an organization can be damage by malicious insider attacks.

D. Shared Technology Issues

Iaas is based on shared infrastructure, which is often not designed to accommodate multi- tenant architecture. Overlooked flaws have allowed guest operating system to gain unauthorized level of control and influence on the platform [8].

E. Data Loss or Leakage

Due to operational failures, untrustworthy data storage and inconsistent use of encryption keys data loss can occur. Deletion or variation of records without a backup of the original content that can take place intentionally or unintentionally is refer to operational failure. Unreliable data storage refers to saving of data on unreliable media that will be unrecoverable if data is lost [4]. The inconsistent use of encryption keys will result into loss and unauthorized accesses of data that will lead to the destruction of confidential and sensitive information. Twitter hack is an example of data loss. Online account of Twitter was accessed by hackers and their numerous sensitive corporate documents were stolen by them. These documents were housed in Google's online web office service i.e. Google Docs. As the security of documents from twitter was not efficient enough so the Google was not the one to be blamed for security break-in. Instead, the entire company data was only one password crack away from discovery [5]. From this it's clear that data loss or leakage can damage one's brand, reputation and cause a loss and users' morale as well as trust. Compromise in one's intellectual property can lead to financial implications as well as legal consequences.

F. Account or Service Hijacking

Unauthorized access gained by attackers to control the users' accounts, such as fraud, phishing and exploitation of software vulnerabilities is called account or service hijacking .For example if an attacker gains access to users' credentials, they can manipulate their data, spy on their activities/transactions, return falsified information and redirect them to illegitimate sites.

Users' account or service instances may become a new base for the attackers who can leverage the cloud service providers' reputation by launching subsequent attacks. Attackers can often access critical areas of deployed cloud computing services with stolen credential, which in result allows them to compromise the integrity and confidentiality and of those services. A usual approach to maintain access control when using web-browsers to access cloud computing systems are authentication and authorization through the use of roles and password protecting. However, to secure sensitive and critical data this method is not sufficient enough.

G. Unknown Risk Profile

Users should be acquainted with software versions, security practices, code updates and invasion attempts. Most often, these functionally are well advertised while the details about compliance of the internal security procedures remain unnoticed. Users must know how and where their data and related logs are stored.

Impact of Threats:

- In 2009,the largest cloud service provider Amazon's suffered from the interruption in the storage service twice in February & July 2009.
- In March 2009, Google doc suffers from the serious leakage of user private information.
- The mailing service provide by the one of the largest web browser Google also appeared a global failure up to 4 hours.

- The cloud computing infrastructure and platform, created by Microsoft's also suffers serious accident up to 21 hrs.
- As administrators misuse leading to loss of 45% user data, cloud service provider Linkups had been forced to close down.
- In April 2011, Sony experienced a data breach in their play Station Network. It is estimated that more than 77 million clients are compromised.
- In June 2011, Citi group disclosed a data breach within their credit card operation, affecting approximately 210,000 or 1% of their customer's account.
- It was announced by the Target Corporation that data from around 40 million credit and debit cards was stolen in December 2013.
- In October 2013, Adobe Systems suffers from their corporate database was hacked & data got leaked .It is estimated about 130 millions client records was stolen.
- In August 2014, nearly 200 photographs of celebrities were posted to the image board website 4chan. An investigation by Apple found that the images were obtained "by a very targeted attack on user names, passwords and security questions".
- In September 2014, Home depot suffered a data breach of 56 million credit card numbers.
- In October 2014, Staples suffered a data violation of 1.16 million customer payment cards.
- In November 2014 and for weeks after, Sony Pictures Entertainment suffered a data breach involving personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of (previously) unreleased Sony films, and other information. The hackers involved claim to have taken over 100 terabytes of data from Sony.
- Anthem, in February 2015 suffered a data breach of nearly 80 million records, including personal information such as names, social security numbers, dates of birth, and other sensitive details.

IV. CONCLUSIONS

The cloud computing model is one of the promising computing models for service providers, cloud providers and cloud consumers. But to best utilize the model we need to block the existing security holes. In this paper the purpose is to tell about various security threats in cloud computing and the impact of those threats in the world . Purpose of this paper is intended to guide for people who is interested in cloud computing and want to take the advantages of the cloud computing services.

ACKNOWLEDGMENT

I take the opportunity to thanks all those, who have contributed to the completion of this work and helped me with valuable suggestions for improvement .

I express my deep gratitude to my guide, Dr Rajesh Pathak (HOD) and Dr. Yatin Aggarwal for their valuable support, help and guidance during the project work and providing me with best facilities and atmosphere for the work and encouragement.

REFERENCES

[1] Wentao Liu,"Research on cloud computing security problem strategy ", IEEE, ISBN 978-1-4577-1415-3112.

[2] Networkworld,"Gartner Cloud Putting Crimp in traditional software,hardware sales",July 2012 , Available from http://www.networkworld.com/news/2012/071312-gartner-cloud-260882.html

[3] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0", March 2010, Avaliable from: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "Above the Clouds: A Berkeley View of Cloud", Electrical Engineering and Computer Sciences, University of California at Berkeley, February 10, 2009.

[5] Security guidance for Critical Areas of Focus In Cloud Computing V3.0,Cloud Security Alliance 2011.

[6] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," 2009, http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf, Accessed April 2010.

[7] Velte et al, "Cloud Computing, A Practical Approach", McGraw-Hill Osborne Media, 1st edition, 2009.

[8] http://ccskguide.org/top-threats -to-cloud-computing.

[9] B. Wang, Huang He, Yuan, Liu Xiao, Xi, Xu Jing, Min, "Open Identity Management Framework for SaaS Ecosystem," in *ICEBE '09*. pp. 512517.

[10] S. Subashini,,Kavitha, V., "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. In Press, Corrected Proof.

[11] F. Elizabeth, Vadim, Okun, "Web Application Scanners: Definitions and Functions," in *HICSS 2007*, pp. 280b-280b.

[12] NIST. October, (2010). *National Vulnerability Database (NVD)*. Available: http://nvd.nist.gov/home.cfm

[13] OWASP. (2010, *The Ten Most Critical Web Application Security Vulnerabilities.* Available: http://www.owasp.org/index.php/OWASP Top Ten Project .

