Security Issues in Cloud Computing

Saba Maria[1], Bara Chandrakala[2], Shaziya Tabassum[3]
[1, 2, 3] CSE Department,
[1, 2, 3] GPCET (affiliated to JNTUA, Anantapur), Kurnool, India

Abstract- *Cloud computing has emerged as one of the fastest growing technologies in the field of Information Technology from the past few years. Cloud computing allows the users to store and access data and computing resources over the Internet. As large volumes of data are generated by individuals and organizations, it has become difficult to store the data, information, programs and run it on their personal computers. It provides many benefits such as simplicity, lower costs, unlimited storage, easy utilization of resources, backup and recovery, less maintenance, quality of service, scalability, flexibility, reliability, quality control, automatic software updates, continuous availability, elasticity, fast deployment. Although there are many benefits of cloud computing services its security becomes a major challenge. This paper first describes the service models and deployment models of cloud computing, then discuss the security issues in cloud service models and lists security threats in cloud.*

Keywords- Privacy, Elasticity, Private Cloud, Public Cloud, Hybrid Cloud, Multi-tenant, Security, Risk.

I. INTRODUCTION

The introduction of Internet has led to the emergence of various technologies. Cloud computing is one of such tremendous technologies. Rather than accessing from the local hard drive Cloud computing allow the users to store and access computing resources and data over the Internet. According to the US National Institute of Standards and Technology (NIST), cloud computing is a model enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. The two main characteristics of cloud computing are Elasticity and Multi-Tenancy. Elasticity provides the flexibility to the customer to scale up and scale down the resources automatically based on their requirements. Multitenancy is a software architecture where multiple customers are served by a single instance of the software application. Although there are many benefits provided by the cloud computing there are many threats that cause immense loss to users. Most of the users are unaware of where their data is stored and how the cloud service provider manages the data.

II. RELATED WORK

A. Cloud Computing Service Models

There are three service models in cloud computing as shown in fig 1.

1) Software as a service (SaaS): Software as a service provides an alternate way of accessing software where it allows users to subscribe to the software application and access it online rather than purchasing and installing it on their personal computer. Users do not manage the underlying cloud infrastructure, storage, operating system, network. Some of the examples of SaaS are Google Apps, Office 365, Netflix, Salesforce.
2) Platform as a service (PaaS): Platform as a service provide a developing environment to the developers to develop and deploy their own applications using programming languages, libraries, and tools. Users have control only on the configuration settings for the deployed applications but not on the underlying cloud infrastructure, storage, operating system, network. Some of the examples of PaaS are AWS, Google App Engine, Windows Azure, Apache Stratos.
3) Infrastructure as a service(IaaS): Infrastructure as a service provides an infrastructure to the users such as operating systems, networking, security and servers to deploy and run arbitrary software.Platform virtualization, dynamic scaling, and automated administrative tasks are the characteristics of IaaS. Some of the examples of IaaS are Amazon EC2, Google Compute Engine, Windows Azure, Rackspace.

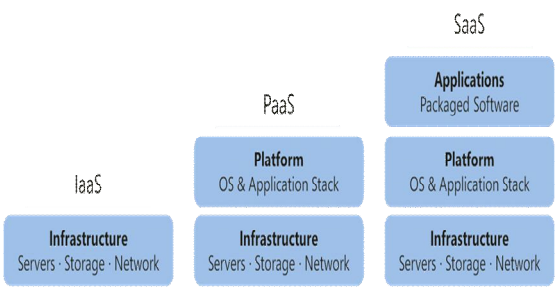

Figure1. Cloud Service models [2]

B. Cloud Computing Deployment Models

Three are three deployment models in cloud computing as shown in fig 2.

1) Public Cloud: Public cloud is a computing model which is provisioned for open use by the general public, in which users can register and use available infrastructure and storage. It can be managed, operated and owned by the academic, business or government organization. Public cloud facilitates services either free or on the basis of the "pay as you go" model. It is located on the premises of the cloud provider.
2) Private Cloud: Private cloud is a computing model where IT services are provisioned for dedicated use by a single organization. It can be managed, operated and owned by the single organization or third party. Private clouds are used when public clouds become inadequate or inappropriate to provide the level of service availability or uptime needed by the organization. It is located on or off premises of cloud provider.
3) Community cloud: Community cloud refers to computing model in which cloud infrastructure is shared among various organizations that have a common interest such as mission, security policy, and requirements. It is located either on premises or off premises of cloud provider.
4) Hybrid Cloud: A hybrid cloud is used to provide distinct functions within the same organization by integrating both public and private cloud services.Benefits of multiple deployment models are offered by the hybrid cloud.To enhance the efficiency of an organization hybrid cloud allows to use public clouds for non-sensitive operations and private cloud only when they require it.

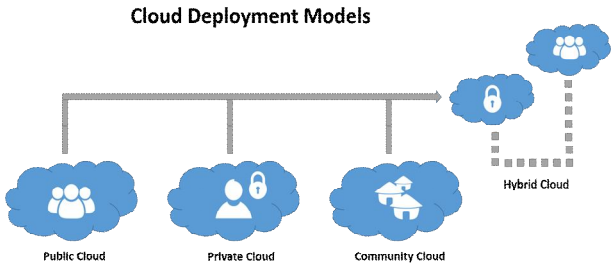

Figure 2. Cloud Deployment models [3]

III. SECURITY ISSUES IN CLOUD SERVICE MODELS

A. Issues in SaaS

As users are concerned about who gets access to their data as they are giving their information and data to the service providers. They have the fear of deletion or corruption of sensitive data by unauthorized. So every user has to review the policies, procedures, level of access and Terms of Agreement before signing. The users don't have total control over their data. For example, if data is corrupted or something has happened to the user data then the user has to contact the service provider and wait for his response which may cause loss to the user. web applications to be hosted on the cloud infrastructure should be validated and scanned for vulnerabilities using web application scanners [4]. Such scanners should be up to date with the recently discovered vulnerabilities and attack paths maintained in the National Vulnerability Database (NVD) and the Common Weaknesses Enumeration (CWE) [5].

B. Issues in PaaS

The private information of the users should be protected before sending to the cloud.Before sending it to the cloud service provider how can the private information of the user is automatically encrypted? Most of the cloud services of the user can be accessed using REST Web Services interfaces.API keys which are similar to passwords can be used to access these services.It is very important to safeguard these keys. Encryption can be performed on these keys to protect them. As platform as a service is based on Service Oriented Architecture model. Therefore, the issues such as Injection attacks, Replay attacks, DOS attacks and man in the middle attack are all inherited. In order to secure the cloud services authentication, authorization, security standards are very important.

C. Issues in IaaS

Vulnerabilities are increased by sharing the same network infrastructure between different users within the same server. Network and internet connectivity threats such as Man In The Middle attack, port scanning, IP spoofing, DNS security. Monitoring VMs includes control actions and VMs resource modification. Any authorized user or the system admin who has control over backend can misuse this. The host can monitor the network traffic of its hosted VMs as all network packets going to or coming from VM will pass through the host. There is a chance of exploiting some features by the attackers in a virtual machine such as shared clip board which allows data to be transferred between VMs and the host to exchange data between cooperating malicious programs in VMs [6].

IV. SECURITY THREATS IN CLOUD COMPUTING

A. Data Breaches

Cloud users might store confidential and important data in the cloud. Cloud service providers become a target for attackers to hack the data stored by them.Data breach attacks involve disclosure of information that is not intended for the public such as financial information, business secrets, intellectual property and personal health information.Data breach is a top security risk in cloud computing.

B. Data Loss

Apart from malicious attacks there could be lot more reasons for data loss in the cloud such as natural disasters like earthquakes, deletion of data by cloud service provider, shut down of the server[7].Some examples of data loss faced by top companies are Google which suffered data loss when it's power grid faced lightning and Amazon that deleted it's own customers data in 2011 [9].

C. Insecure APIs

Application Program Interfaces(APIs) are considered as threats in cloud computing.This is because APIs not only provide flexibility for users to customize the cloud services but also authenticate and provide encryption.As the underlying infrastructure of APIs grow so do it's security threats[9].APIs provide an interface to develop programs that allow users to integrate their applications with other software applications.

D. Account Hijacking

In account hijacking, attackers hijack users account and try to access users credentials, modify the data, intercept the user's transactions and return false results[8]. Thus attackers access cloud computing services of the users and due to that confidentiality, availability, and integrity of services is lost.

E. Denial of Service

In Dos attacks, hackers intend to flood networks, servers, and systems with traffic and prevent the users from accessing services [10]. As cloud services become unavailable to users they might not get what they need in time.

F. System Vulnerabilities

Multitenancy creates a new attacking surface as systems from various organizations and users are brought together and are given access to shared resource pool and memory.In system vulnerability, viruses and bugs are induced into the target system in order to get over the system, steal confidential data and disrupt services.

G. Malicious Insiders

Employees inside the organization might be a big threat.They may be hackers or partner with hackers whose intention is to steal or tamper the data. By using authorized access to organization cloud services, employees might misuse and try to access other employees accounts and confidential information.

H. Malware Injection

Malware injection, malicious code is injected into the cloud services. Attackers try to eavesdrop and steal the data once cloud services begin execution with the injected malware.

V. CONCLUSION

It is beyond doubt that cloud computing has brought a lot of benefits and is becoming more popular. Many enterprises have adopted cloud computing services into their business. Although cloud computing provides a large number of advantages to the users, its security becomes a major challenge. In this paper, we have discussed security issues in cloud service models and threats in cloud computing.

REFERENCES

[1] Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I and Zaharia M 2010 A view of cloud computing, Communications of the ACM Magazine, 53 4 50-58

[2] Cloud computing service models retrieved from https://www.tclouds-project.eu/popular-cloud-computing-services-the-paas-platform-as-a-service/

[3] Cloud computing deployment models retrieved from https://www.uniprint.net/en/7-types-cloud-computing-structures/

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

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

[6] J. Kirch, "Virtual machine security guidelines," 2007. [Online]. Available: http://www.cisecurity.org/tools2/vm/CIS\ VM\ Benchmark\ v1.0.pdf

[7] Khurana S and Verma A G 2013 Comparisons of cloud computing service model: SaaS, PaaS, IaaS International Journal of Electronics & Communication Technology (IJECT) 4 3 29-32

[8] Kiblin T 2011 How to use cloud computing for disaster recovery Retrieved from http://www.crn.com/blogs-op-ed/channel-voices/230700011/how-to-use-cloud-computingfor-disaster-recovery.htm

[9] The top 10 security concerns for cloud basedservices: https://www.incapsula.com/blog/top-10-cloud-security-concerns.html

[10] Kuyoro S O, Ibikunie F and Awodele O 2011 Cloud computing security issues and challenges International Journal of Computer Networks (IJCN) 3 5 247-255