International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 01,January-2015

Cloud Computing Security Threats

Swati Gupta
M.TechScholar,Department of Computer Science,
Geetanjali Institute of Technical Studies (RTU),
Udaipur, India

Mrs. Sarika Khandelwal
Associate Professor, Department of Computer Science
Geetanjali Institute of Technical Studies (RTU),
Udaipur, India

***Abstract*- Today's era is completely dependent on computers. Cloud Computing is the most important technology which is diffusing in the sky of IT. It covers number of advantages like resource sharing; provide large servers for data storage on pay per use basis. But some users still have an impression that saving their confidential data on cloud will no longer remain confidential due to security issues. This paper will concentrate on the basic aspect and the nine security threats related to cloud computing.**

Keywords- cloud computing, security threats, issues, data breaches, data loss.

I. INTRODUCTION

Most people think that the terminology cloud computing is related to some environment or weather conditions. But actually cloud is a metaphor used for internet. It is a vast storage space with number of other resources which are shared by the users. It is an Internet-based computing, whereby shared resources, software and information, are provided to computers and other devices on-demand, like the electric grid. This technology was established in the year 1960, initially used by telecommunication companies. Until 1990 it offers point to point data circuits and then offered virtual private networks. Later, to provide more network bandwidth cloud was introduced for both servers and infrastructures. In 2007 Google, IBM and many remarkable universities and companies adopted it. And in 2008 Gartner highlighted its characteristics for customers as well service providers.

II. CLOUD COMPUTING

There are more than 20 definitions of cloud computing that focus on certain aspects of this technology [1]. According to National Institute of Standard and Technology cloud is defined as "Cloud computing is a model for convenient, on-demand network access to shared pool of configurable computing resources (eg. Networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." The cloud model consists of five essential characteristics, three service models, and four deployment models [2].

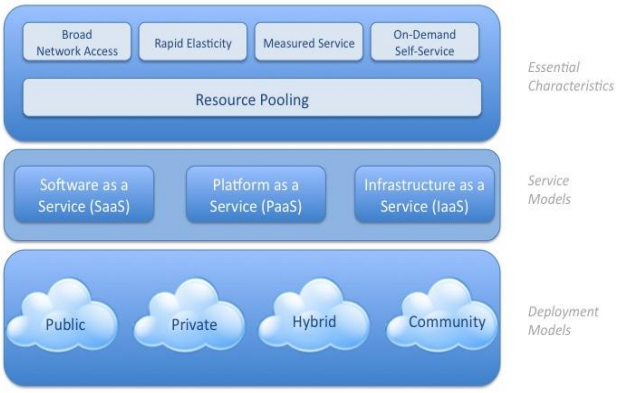


Fig. 1 NIST model of Cloud Computing

Essential Characteristics-

- *On-demand Self Service*- Cloud provides various computing capabilities to the consumers. A consumer can utilize computing resources like servers, network storage, as needed automatically without any human interaction.
- *Broad Network Access*- The network provides extensive capabilities that can be accessed by thin or thick clients following the standard mechanism.
- *Resource Pooling*- The service provider have a reservoir of resources for the consumers. It can serve multiple consumers using multi-tenant model. The various physical and virtual resources are dynamically allocated to the consumers according to the demand. At lower level of abstraction the consumers have no control or knowledge over the exact location of the resources (location independency) but may be able to specify location at higher level.
- *Rapid Elasticity*- Capabilities can be rapidly and elastically provisioned to scale out and rapidly released to scale in. the capabilities available for provisioning appears to be unlimited to the consumers. The consumers can purchase or release in any quantity at any time.
- *Measured Services*- Cloud provides proper measuring of services and resources. Resource utilization is monitored, controlled and reported to provide transparency for both consumer and service provider.

Service Models-

- *Software-as-a-Service*-SaaS provision commercially available software to the consumers. The main advantage of SaaS is that the consumers need not to worry about the purchase and licensing of software and neither there is any version compatibility issue. "The SaaS adoption in India is growing rapidly because it offers quicker time to value with none of the management or cost overheads

associated with it." says Steve McWhirter, senior vice president, enterprise sales, Asia Pacific, salesforce [3].

- *Platform-as-a-Service*-PaaS provides computing platform over the web. It provide services like application runtime, storage, and integration. In this model, the servers, networks and storage are provided by the service providers.
- *Infrastructure-as-a-Service*- IaaS is a complete IT infrastructure consumed as a service. Each user or tenant accesses a portion of resources to create and use their own infrastructure as needed.

Deployment Models-

- *Private Cloud*-In private cloud, the customers have complete control over the resources and pooled infrastructure. It is entirely owned and managed by a single organization.
- *Public Cloud*- In this model the resources and infrastructure are entirely provided by a third party. Customers can access web applications and services over the internet.
- *Hybrid Cloud*- It is the combination of private and public cloud, i.e., the pooled services and resources may be created by joining and federating private cloud with third party resources.
- *Community Cloud*- Some different organizations have same policy and protocols to follow. They use community cloud as deployment model. It further decreases the IT operational cost as it is shared by a larger group.

III.TOP THREATS

TABLE I. Security Threats in Cloud Computing

Threats	Effect
1. Data Breaches	The consumers lost the encryption key; the data will be lost as well.
2. Data Loss	Data Loss will occur due to less security, accidental or physical crisis.
3. Account or Service Hijacking	It includes attacks like phishing, fraud and exploitation of software.
4. Insecure Interfaces & APIs	The interfaces or APIs used to interact with the service providers are prone to risks by attackers.
5. Denial of Service	The attackers prevent the consumers to access their data and services.
6. Malicious Insider	The attackers get through the security wall and access all the sensitive data.
7. Abuse of Cloud Services	Services provision by cloud providers are misused by the attackers
8. Insufficient Due Diligence	Many organizations adopt cloud without complete knowledge of CSP which brings unknown level of risks.
9. Shared Technology Vulnerabilities	In multi-tenant model, individual customers do not impact other tenants.

Cloud computing technology is expected to change the face of computing. But issues like security, scalability, and the requirement of specific customer based customization still remain an issue. The CSA (Cloud Security Alliance) conducted a survey in 2013 and reported nine major security threats of cloud computing. According to the industry experts, these are ranked as the greatest vulnerabilities within cloud computing. Below are the nine critical threats to cloud security (ranked in order of severity) [4].

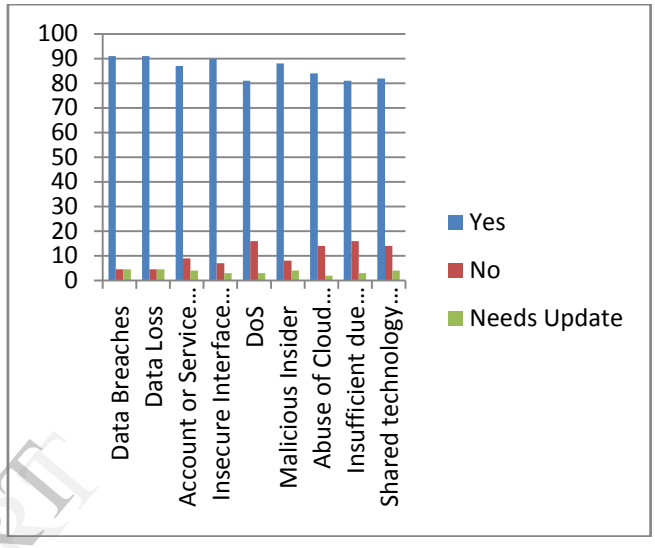
1. *Data Breaches*- The CIOs of every organization has the hallucination of losing their sensitive internal data to their competitors. In November 2012, researchers from the University of North Carolina, the University of Wisconsin and RSA Corporation released a paper describing the fact that if multiple virtual machines are running on a single physical server, than it may be possible to extract the private cryptographic keys used on one virtual machine by sitting on other virtual machine using side channel timing information [4]. In a multi-tenant environment, if a flaw exists in a single tenant's application cloud allow an intruder to access the application of all the clients present in the environment. The impact of data breaches can be reduced by encrypting the data, but if you lose your encryption key, your data will be lost automatically. Multiple copies of data are prepared to reduce the impact of data loss but it will increase your exposure to data breaches.
2. *Data Loss*- For cloud consumers, data loss is one of the most concerning issue. A person lost all his personal files due to lack of data security by the service provider. Of course, data stored in the cloud can be lost due to other reasons also. An accidental or physical crisis like fire and earthquake are also responsible for the loss of data. Furthermore, if a customer upload its data to the cloud after encrypting it and loses the encryption key due to any reason, the data will be lost as well.
3. *Account or Service Traffic Hijacking*-Account or Service hijacking includes attacks like phishing, fraud, and exploitation of software. This security threat arises due to loss of credentials. If the attackers gain access to your credentials and passwords, they can easily get access to your confidential data and accounting information. Also they can manipulate or delete your data, return falsified information, and redirect your client to some illegitimate site. To avoid this, the organizations or individuals should protect their passwords and credentials from being shared between users and services. Also proper authentication technique should be used.
4. *Insecure Interfaces and APIs*- Sometimes customers have to interact with the service providers. For this the providers expose a set of software interfaces or APIs. Management, controlling are done using these interfaces. The security of these APIs is very important. Authentication and encryption is used to make them secure. Also they must be designed to protect against both accidental and malicious attackers.
5. *Denial of Service*-DoS attack won't let the users of cloud services to access their data or applications. The attacker (or attackers as is the case in Distributed Denial of Service (DDoS) attack) creates a system slowdown by consuming system resources such processor power, memory, disk space, bandwidth. This creates confusion

among the users and they get annoyed over the late response for their requests. DoS attack leaves the users into an unending loop in which they are not able to do anything except to sit and wait.

6. *Malicious Insiders*- CERN defines an insider threat as such:[5]
   "A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."
   A malicious insider can have access to all confidential and sensitive data if the security is not properly managed. The systems which are entirely dependent on service providers are more prone to malicious attackers. Even if the data is uploaded after encryption and the encryption keys are not kept with the user, the data is still vulnerable to malicious insider attack.
7. *Abuse of Cloud Services*-Cloud service provides computing power to all the enterprises whether they are small or big. The organizations need not to purchase and maintain thousands of servers, but cloud computingservice providers rent them thousands of servers which are more affordable. But not all organizations use this power as a boon. For an attacker to estimate the encryption keys will take years with a single server. But with the help of thousands of servers it will become easy to estimate the keys within minutes. This threat is more serious issue for cloud providers than cloud consumers.
8. *Insufficient Due Diligence*-Cloud computing is one of the most hyped IT innovations. Many organizations being pushed to the cloud without a complete knowledge of Cloud Service Provider (CSP) environment. Due to this organizations are taking on unknown level of risk. By adopting cloud technologies without proper understanding will leave the organization with number of issues. The base line for any organization to adopt this new technology is that they must have capable resources and perform extensive internal and CSP due diligence to understand the risks associated with the new technology adoption.
9. *Shared Technology Vulnerabilities*- Cloud service provider provision sharing of infrastructure, platform, and software. In some cases, the underlying components (GPUs, CPU caches etc.) were not designed to offer strong isolation capabilities for multi-tenant deployment. Cloud providers should have an in-depth defense strategy. On the shared infrastructure it should be ensured that individual customers do not impact other tenants. Proper environment monitoring and checking should be done by the providers. Strong authentication methods, scanning, and configuration audits should be recommended.

The survey conducted by CSA reported the percentage result about the relevance of the threat.
Is the Threat still relevant?

The industry experts gave their opinion about the question asked in the survey and accordingly a graph is prepared. [4]



CONCLUSION

By reading this paper, it should be clear that security threats related to cloud computing cannot be taken for granted. Proper measures should be kept in mind to reduce the impact of these notorious nine. The security of data should be done by fastidious authentication and encryption.

REFERENCES

1. J. Geelan, "Twenty one experts define cloud computing. Virtualization," Electronic Magazine, http://virtualization.sys-con.com/node/612375.
2. National Institute of Standard and Technology csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc, 2009
3. Dataquest, The Business of Infotech, Vol XXIX No. 10/ May31, 2011, A Cybermedia Publication
4. https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/
5. http://www.cert.org/insider-threat/