A Survey on Security Threats for Cloud Computing & How to Overcome these Challenges

Saroja.V¹, Umamaheswari.S.K²
¹Department of Information Technology, INDIA
²Department of Computer Science Engineering, INDIA

ABSTRACT
Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. Cloud Computing allows firms to outsource their entire information technology (IT) process, allowing them to concentrate more on their core business to enhance their productivity and innovation in offering services to customers. It allows businesses to cut down heavy cost through optimized and efficient computing incurred over IT infrastructure without losing focus on customer needs. However, to a certain limit adopting Cloud computing has struggled to grow among many established and growing organizations due to several security and privacy related issues. Though the cloud computing has its advantages many IT companies have expresses concern about critical security issues which threatens them such as data security, unauthorized access of network and use of infected application. Due to the use of internet and vital remote servers to maintain the data and applications, the cloud computing environment becomes open for the attackers to attack on the user data and communication services. This paper provides review of major security threats and vulnerabilities affecting Cloud Systems and the possible solutions available to such threats.

Keywords— Cloud computing, Data security, Network security, Security Threats

I. INTRODUCTION

Cloud Computing is an on demand service style. At present, it makes everything simple and flexible. But Cloud architecture is complex and is not easy to solve any problem in short. There are three types of clouds is done, such as public, private and hybrid. cloud providers offered three types of Services like Platform as a Service (Peas), Software as a Service (Seas) and Infrastructure as a Service (IaaS). Cloud computing [1] comprises of 2 components—the front end and the back end. The front end includes client’s devices and applications that are required to access cloud. And the back end refers to the cloud itself. The whole cloud is administered by a central server that is used to monitor client’s demands. Cloud Computing is a computing model that enables sharing of resources on-demand with cost effectiveness and location independent. In Cloud systems the customers need not to buy any resources in their own instead they can use the resources from the cloud and they can pay for the resource as per the usage. Cloud computing is a technology that offers many advantages, in that the main drivers of cloud computing is the following

- One can access applications as utilities, over the Internet.
- Manipulate and configure the application online at any time.
- It does not require to install a specific piece of software to access or manipulate cloud application.
- Cloud Computing offers online development and deployment tools, programming runtime environment through

CLOUD COMPUTING SERVICE MODELS

A) Software as a Service (SaaS)
SAAS refers to Software as a Service in this a system with operating systems, hardware & network provided or we can say a pre developed system. In SaaS the software applications such as CRM, ERP and some other online applications to manage the organizations are offered as a service. The additional hardware and software’s that are required to support the pre made application can be offered by the cloud provider itself. It clears the idea that on customer side there is no need of investment for the extra things either the service we occupy.

B) Platform as a Service (PaaS)
Here the platforms or environment needed to develop the applications are provided as a service. The organizations that need a particular environment can buy it
from the cloud infrastructure for developing their applications which will run on the provider’s infrastructure and release the environment when the work completed. In PAAS the operating system, hardware & network are provided and customer/ user install or develop its own software.

C) Infrastructure as a Service (IaaS)

IaaS refers to Infrastructure as a Service in this customer has the knowledge about all the stuff. IaaS is the foundation of cloud services. This type of service provides storage space, processing power and managing the organizations Database On-Demand of the particular company.

Figure1. Cloud Models

Now after services the well known concept Virtualization came. Basically virtualization is a concept of operating system. It came from word “Virtual” which means “Not Actual” or “Imaginary”. So in cloud computing virtualization is the emulation of one of more workstations/servers with in a single physical computer. So by using virtualization the use of hardware resources is increased, cost of resources and management is reduced, business flexibility is improved & security also improved. So by using cloud services it is also valuable or useful that the sensitive information of user remain trustworthy or secured but there are many possible attacks like man in middle attack, denial of service attack etc. So we have to minimize these types of attacks.

TYPES OF CLOUDS

A) Public Cloud

A public cloud can be accessed by any subscriber with an internet connection which own and operated by a service provider who hosts the cloud infrastructure with an access control mechanism. All customers share the same resource pool of the cloud provider with limited security and availability of the resources on demand.

B) Private Cloud

Private cloud is cloud infrastructure delivered to a single organization. The main advantage of private cloud is the protection of the data of user’s because they are restricted into the organization data center. It is not shared with other organizations, whether managed by own or by a third-party cloud providers, and it can be hosted internally or externally.

C) Hybrid Cloud

Hybrid Clouds are a combination of two or more cloud methods of resource pooling. The Hybrid cloud environment is independent in it but commonly connected through a standard interface.

D) Community

A community cloud is shared among several organizations and that is operated, managed and secured commonly by the group of organizations or a third party service provider.

Our main aim is to discuss most of the security threats and trying to discuss some overcoming process. In chapter 2 data protection in cloud is given, after that in Chapter 3 explained some security threats, chapter 4 discussed seven major security vulnerabilities to cloud, chapter 5 discussed solution for security issues, finally chapter 6 provides conclusion for the paper.

II. DATA PROTECTION IN CLOUD

Security of data in cloud is a challenge and is of supreme importance as many flaws and concerns are yet to be identified. Data protection is a crucial security issue for most of the enterprises [7]. The management of the data and services [4] may not be fully trust worthy and the enterprises do not have any control on the data, since the data centers are remotely located. Moreover, data are stored in a multi tenant environment. The common security concerns are:

1. Securing data in transit and at rest,
2. Secure software interfaces,
3. User access control, and
4. Data separation.

Since, data in cloud computing is placed in the hands of third parties, ensuring the data security both at rest (data residing on storage media), as well as, in transit is of great importance. Given the large number of issues concerning data security, many organizations need clear answers regarding data security before migrating to the cloud. The users’ data confidentiality and integrity are maintained by providing data security which is an important quality of service in cloud computing. Data security in the cloud includes the following [5] Data security in network, host and application levels has become a vital part of cloud storage. The data in cloud can be in any of the forms as shown in figure 1[6].

Figure2. Data Forms in Cloud
III. SECURITY THREATS

A Secure cloud is always a trustworthy source of resources or information’s so securing the cloud is a main aspect of the cloud providers who are in charge for the cloud area. Cloud computing security means that securing data from the malicious persons, providing high performance to users, using high quality encryption standards which protect data from the hackers etc. The main problems cloud computing faces are securing confidentiality and integrity of data in terms data security. The Cloud Security Alliance has put together a list of the nine most prevalent and serious security threats in cloud computing. The security threats are as follows:

A. DATA THREATS

1) Data Breaches:

Data breach is defined as the leakage of sensitive customer or organization data to unauthorized user. Data breach from organization can have a huge impact on its business regarding finance, trust and loss of customers. This may happen accidentally due to flaws in infrastructure, application designing, operational issues, insufficiency of authentication, authorization, and audit controls [2]. An example of data breach is cross VM side channel attack introduced by Y. Zhang et al. that extracts cryptographic keys of other VMs on the same system and can access their data.

2) Data Loss or Leakage:

Data loss is the second most important issue related to cloud security. Like data breach, data loss is a sensitive matter for any organization and can have a devastating effect on its business. Data loss mostly occurs due to malicious attackers, data deletion, data corruption, loss of data encryption key, faults in storage system, or natural disasters. 44 percent of cloud service providers have faced brute force attacks in 2013 that resulted in data loss and data leakage.

B. NETWORK THREATS

1) Account or Service Hijacking:

Account hijacking involves the stealing of user credentials to get an access to his account, data or other computing services. These stolen credentials can be used to access and compromise cloud services. The network attacks including phishing, fraud, Cross Site Scripting (XSS), botnets, and software vulnerabilities such as buffer overflow result in account or service hijacking. This can lead to the compromise of user privacy as the attacker can eavesdrop on all his operations, modify data, and redirect his network traffic. In 2009 a legitimate service was purchased from Amazon’s EC2, and compromised to act as Zeus botnet [3].

2) Denial of Service:

Denial of Service (DOS) attacks are done to prevent the legitimate users from accessing cloud network, storage, data, and other services. DOS attacks have been on rise in cloud computing in past 5 years and 81 percent customers consider it as a significant threat in cloud [1]. They are usually done by compromising a service that can be used to consume most cloud resources such as computation power, memory, and network bandwidth. This causes a delay in cloud operations, and sometimes cloud is unable to respond to other users and services.

C. SECURITY THREATS INHERITED FROM NETWORK CONCEPT

Network plays an important role in deciding how efficiently the cloud services operate and communicate with user. The most critical network threats in Cloud are listed below:-

1) SQL Injection Attacks:

In this type of attack a malicious code is inserted into a standard SQL code. Thus the attacker gain unauthorized access to a database and are able to access sensitive data.

2) Man in the Middle Attacks:

In this type of attack, an entity tries to intrude in an ongoing conversation between a sender and a client to inject false information and to have knowledge of the important data transferred between them.

3) Security Concerns with the Hypervisor:

Cloud Computing rests mainly on the concept of virtualization. In a virtualized world, hypervisor is defined as a controller popularly known as virtual machine manager (VMM) that allows multiple operating systems to be run on a system at a time. Since multiple operating systems would be running on a single hardware platform, it is not possible to keep track of all such systems and hence maintaining the security of the operating systems is difficult.

4) Distributed Denial of Services Attacks:

Distributed Denial of Services Attacks (DDoS) attack is a form of DoS attacks in which multiple network sources are used by the attacker to send a large number of requests to the cloud for consuming its resources.
Application Programming Interface (API) is a set of protocols and standards that define the communication between software applications through internet. Cloud APIs are used at all the infrastructure, platform and software service levels to communicate with other services. Infrastructure as a Service (IaaS) APIs are used to access and manage infrastructure resources including network and VMs, Platform as a Service (PaaS) APIs provide access to the cloud services such as storage and Software as a Service (SaaS) APIs connect software applications with the cloud infrastructure.

2) Malicious Insiders:

A malicious insider is someone who is an employee in the cloud organization, or a business partner with an access to cloud network, applications, services, or data, and misuses his access to do unprivileged activities. Cloud administrators are responsible for managing, governing, and maintaining the complete environment. They have access to most data and resources, and might end up using their access to leak that data. Other categories of malicious insiders involve hobbyist hackers who are administrators that want to get unauthorized sensitive information just for fun, and corporate espionage that involves stealing secret information of business for corporate purposes that might be sponsored by national governments.

3) Abuse and Nefarious use of Cloud Services:

The term abuse of cloud services refers to the misuse of cloud services by the consumers. It is mostly used to describe the actions of cloud users that are illegal, unethical, or violate their contract with the service provider. Abusing of cloud services was considered to be the most critical cloud threat in 2010 [2], and different measures were taken to prevent it. However, 84 percent of cloud users still consider it as a relevant threat [1]. Over the years, different attacks have been launched through cloud by the malicious users. For example, Amazon’s EC2 services were used as a command and control servers to launch Zeus botnet in 2009 [6]. Famous cloud services such as Twitter, Google and Facebook as a command and control servers for launching Trojans and botnets.

4) Insufficient Due Diligence:

The term due diligence refers to individuals or customers having the complete information for assessments of risks associate with a business prior to using its services. Cloud computing offers exciting opportunities of unlimited computing resources, and fast access due which number of businesses shift to cloud without assessing the risks associated with it.

5) Shared Technology Issues:

Cloud computing offers the provisioning of services by sharing of infrastructure, platform and software. However, different components such as CPUs, and GPUs may not offer cloud security requirements such as perfect isolation. Moreover, some applications may be designed without using trusted computing practices due to which threats of shared technology arise that can be exploited in multiple ways. In recent years, shared technology vulnerabilities have been used by attackers to launch attacks on cloud. One such attack is gaining access to the hypervisor to run malicious code, get unauthorized access to the cloud resources, VMs, and customer’s data.

E. SECURITY THREATS RELATED TO THE LOCATION OF THE CLOUD:

1) Multi-location of the Private Data:

In Cloud Computing the private data is/are placed in someone else’s computer. There many things can go wrong. Firstly, the Cloud service provider may go out of business. Secondly, the cloud service provider may decide to hold the data as hostage if there is a dispute. Thirdly, it is rather important for a company to understand in which country its data will be hosted.

2) Data Combinations:

The cloud Computing client needs to ensure that its private data is stored separately from others or not. If they are combined with those of other clients’ data then it is much more dangerous.

3) Data Location:

It might be rather difficult or even impossible for the cloud service provider to assure the locations where the client’s data will be stored.

4) Data Transfer Across the Borders:

Knowing where the cloud service provider will host the data is a prerequisite to know how to transfer data across the country borders, which makes the law to be applied even more complicated and consequently resulting in the private information to be more vulnerable from attack.

IV. SEVEN MAJOR VULNERABILITIES TO CLOUD

A. Session Riding and Hijacking

This vulnerability is related to web applications weaknesses which allow the hackers to perform malicious activities such as session hijacking by using a valid session key gain the unauthorized access into the computer system of the authorized users. On the other hand the session riding refers the act of tricking the user open an email or to visit a harmful website which deletes the user information by sending commands to a web application.

B. Reliability and Availability of Service

When considering this issue cloud computing is not perfect because when building more and more services on top of the cloud infrastructure many internet services and applications may stop working. The paper gives the example of an event in 2008 when Amazon’s Web Service cloud storage infrastructure went down for several hours. This caused data loss and access issues.

C. Insecure Cryptography

For all cryptographic algorithms there is a novel method identified by the attackers to break the
cryptography which results in insecurity. It is very common to identify flaws in the cryptographic algorithms which turn a very strong encryption into a weak encryption. The Virtual machines used on the cloud do not have enough sources of entropy and are therefore susceptible to attacks.

D. Data Protection and Portability

This vulnerability is based on the protection of data such that if the client doesn’t want to continue the service or if the agreement between the CSP and the client was terminated then what happens to the sensitive data of the client. On the other hand in terms of portability if the provider get out of the business then what will happen to the data of the client and the services which provided by the provider.

E. Virtual Machine Escape

In this type of vulnerability the attacker directly interact with the host operating system by breaking the isolation layer which separate the VM’s from the host OS. Through this there is an increase in the attack surface for the attacker.

F. Vendor Lock-in

The Lock-in will make the client dependent on the vendor for services. Though the providers not capable of providing good standards of services the client will not switch to another provider because of the principles and policies established before the agreement.

G. Internet Dependency

Cloud Computing is mostly dependent on the internet because all the application interfaces used to connect to the cloud will work only when the internet connection is available. All the services accessed through the web browsers by the users. The question on the dependency is that whether the internet is reliable for the users who have use the cloud for 24 hours such as the Health care industry.

V. SOLUTIONS FOR SECURITY ISSUES

A. Data Security

1) Protection from Data Breaches:

Some measures that must be taken to avoid data breaches in cloud are to implement proper isolation among VMs to prevent information leakage, implement proper access controls to prevent unauthorized access, and to make a risk assessment of the cloud environment to know the storage of sensitive data and its transmission between various services and networks. Considerable amount of research has been carried out for the protection of data in cloud storage. Cloud Proof [4] is system that can be built on top of existing cloud storages like Amazon S3 and Azure blob to ensure data integrity and confidentiality using encryption. To secure data in cloud storage attributed based encryption can be used to encrypt data with a specific access control policy before storage. Therefore, only the users with access attributes and keys can access the data [5]. Another technique to protect data in cloud involves issuing scalable and fine grained data access control [6]. In this scheme, access policies are defined based on the data attributes. This is achieved by combining techniques of attribute based encryption, proxy re-encryption, and lazy re-encryption.

2) Protection from Data Loss:

To prevent data loss in cloud different security measures can be adopted. One of the most important measures is maintaining backup of all data in cloud which can be accessed in case of data loss. Different data loss prevention (DLP) mechanisms have been proposed in research and academics for the prevention of data loss in network, processing, and storage. R Chow et al. proposed the usage of Trusted Computing to provide data security. A trusted server can monitor the functions performed on data by cloud server and provide the complete audit report to data owner. In this way, the data owner can be sure that the data access policies have not been violated [7]. Tomoyoshi T. et al. proposed a system to protect moving data of a company inside a USB even if it is lost.

B. Network Security

1) Protection from Account or Service Hijacking:

Account or service hijacking can be avoided by adopting different security features on cloud network. These include employing intrusion detection systems (IDS) in cloud to monitor network traffic and nodes for detecting malicious activities. An IDS system for cloud was designed by combining system level virtualization and virtual machine monitor (responsible for managing VMs) techniques.

2) Protection from Denial of Service:

To avoid DOS attacks it is important to identify and implement all the basic security requirements of cloud network, applications, databases, and other services. Applications should be tested after designing to verify that they have no loop holes that can be exploited by the attackers. The DDOS attacks can be prevented by having extra network bandwidth, using IDS that verify network requests before reaching cloud server, and maintaining a backup of IP pools for urgent cases.

C. Security Threats inherited from Network Concept

In order to avoid Security Threats inherited from Network Concept are as given below:

1) SQL Injection Attacks:

A proxy based architecture is used towards preventing SQL injection attacks.

2) Man in the Middle Attacks:

A few might be considered in order to avoid this threats are: software as a service, separate endpoint and server security process, evaluating virtualization at the end point have been done to tackle with this kind of attack in cloud computing.

3) Security Concerns with the Hypervisor:
Security concerns with the hypervisor can be avoided is to develop advanced cloud protection system by monitoring the activities of the guest VMs (virtual machines) and inter-communication among the various infrastructure components.

4) Distributed Denial of Service Attacks:

The use of IDS in the virtual machine is used to protect the cloud from DDOS attacks. Another method commonly used to guard against DDOS is to have intrusion detection system on all physical machines.

D. Cloud Environment Security

1) Protection from Insecure Interfaces and APIs:

To protect the cloud from insecure API threats it is important for the developers to design these APIs by following the principles of trusted computing. Cloud providers must also ensure that all the APIs implemented in cloud are designed securely, and check them before deployment for possible flaws. Strong authentication mechanisms and access controls must also be implemented to secure data and services from insecure interfaces and APIs.

2) Protection from Malicious Insiders:

The protection from these threats can be achieved by limiting the hardware and infrastructure access only to the authorized personnel. The service provider must implement strong access control, and segregation of duties in the management layer to restrict administrator access to only his authorized data and software.

3) Protection from Abuse of Cloud Services:

The implementation of strict initial registration and validation processes can help in identifying malicious consumers. The policies for the protection of important assets of organization must also be made part of the service level agreement (SLA) between user and service provider. Packets and all the updated security devices in network should be installed.

4) Protection from Insufficient Due Diligence:

It is important for organizations to fully understand the scope of risks associated with cloud before shifting their business and critical assets such as data to it. The service providers must disclose the applicable logs, infrastructure such as firewall to consumers to take measures for securing their applications and data [7]. Moreover, the provider must setup requirements for implementing cloud applications, and services using industry standards. Cloud provider should also perform risk assessment using qualitative and quantitative methods after certain intervals to check the storage, flow, and processing of data.

5) Protection from Shared Technology Vulnerabilities:

In cloud architecture, hypervisor is responsible for mediating interactions of virtual machines and the physical hardware. Therefore, hypervisor must be secured to ensure proper functioning of other virtualization components, and implementing isolation between VMs. Moreover, to avoid shared technology threats in cloud a strategy must be developed and implemented for all the service models that include infrastructure, platform, software, and user security. The baseline requirements for all cloud components must be created, and employed in design of cloud architecture.

VI. CONCLUSION

Cloud Computing is one of the most significant shifts in information and technology. However, there are different Security issues associated with it. In order to obtain user confidence, security should be considered as an important part of cloud. In this paper we discuss about various security threats and impact of these threats on cloud user and provider. We have also provide some effective counter measures to avoid or to handle security threats in cloud computing. In this paper, the basic concepts of security threats are discussed & several ways to overcome or handle these security threats in cloud computing. This paper focused on security issues in cloud computing service model architecture Finally, Cloud Computing business model still have some security issues.

REFERENCES