SECURITY ISSUES OF VARIOUS LAYERS OF LARGE SCALE DISTRIBUTED DATABASE

Dr. Manish Jivtode
Head and Assistant Professor,
Department of Computer Science,
Janata Mahavidyalaya, Chandrapur - 442401 (Maharashtra)

***Abstract*:**
Cloud computing is viewed as one of the most promising technologies in computing today. This is a new concept of large-scale distributed computing. It provides an open platform for every user on a pay-per-use basis. Cloud computing provides a number of interfaces and APIs to interact with the services provided to users. With the development of web services distributed applications, Security of data is another important subject in various layers of distributed computing. In this study, the security of data that can be used during the access of the distributed environment over various layers will be described.

Keywords: Cloud computing services, Distributed database, Cloud models, Security services and Layered protocols, Privacy issues.

I. INTRODUCTION

Web service is a kind of online application technology very suitable for implementing Cloud Computing System. The structure of Web service is designed in Client-Server format. It provides the scalable IT resources such as applications and services, as well as infrastructure [1].

Cloud Computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing works with two models, one is Delivery model and other is Deployment model [2] [3].

A. Delivery Model

Cloud computing services can be delivered to users in many ways. These include –

a) **Software as a service (SaaS)**
This service provides the consumer with the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices, through a thin client interface, such as a web browser (e.g. web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user -specific application configuration settings.

b) **Platform as a service (PaaS)**
This service provides the consumer with the capability to deploy onto the cloud infrastructure, consumer-created or acquired applications, produced using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

c) Infrastructure as a service (IaaS)
This service provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources, and allows the consumer to deploy and run arbitrary software, which can include operating systems and applications. The consumer has control over operating systems, storage, deployed applications, and possibly limited control of select networking components.

d) Communication as a service (CaaS)
This service includes communications can contain voice over IP, Communicate center applications, voice conference and more. It is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS).

e) Monitoring as a service (MaaS)

This is an outsourced service that provides companies visibility into business critical platforms.

B. Deployment Model

Cloud computing provides two basic models-

a) Public cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

b) Private cloud

The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise.

c) Hybrid cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology, that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

d) Community cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise. Deployment model can be summarized by the following table-

Deployment model	Managed by	Infrastructure owned by	Infrastructure located at	Accessible and Consumed by
Public	Third Party provider	Third party provider	Off-premise	Un-trusted
Private	Organization	Organization	On-premise Off-premise	Trusted
Hybrid	Both organization and third party provider	Both organization and third party provider	On-premise Off-premise	Trusted or Un-trusted
Community	Third party provider	Third party provider	On-premise	Un-trusted or Trusted

Table 1: Various deployment models

II. WEB SERVICES SECURITY AND PRIVACY ISSUES

There is a number of security issues associated with cloud computing but these issues fall into two broad categories – Security issues faced by cloud providers (organizations providing software, platform or infrastructure as a service via cloud) and security issues faced by their customers [4]. The cloud computing technology has the following issues-

a) Privacy

Data are stored in a server its ease of access makes raise the issue of data privacy over the cloud environment.

b) Security

As cloud computing is achieving popularity it raises questions on security issues. The data are transferred through the internet which makes the users worried about security as their details will be stored over in the computing environment.

c) Abuse

Hackers may purchase the service with take identity and use the service for hacking and cracking purposes.

In most cases, the provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customers must ensure that the provider has taken the proper security to protect their information. There are security and privacy about cloud computing are given as follows –

i) **Identity management**
In identity management, to control access to information and compute resources. Cloud providers either integrated the customer's identity management system into their own infrastructure, using federation or provide an identity management solution.

ii) **Physical and Personal security**
Physical machine are adequately secure and access to these machines as well as all relevant customers' data is not restricted but that access is documented.

iii) **Availability**
Cloud providers assure customers that they will have regular and predictable access to their data and applications.

iv) **Application security**
Applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires application security measures be in place in the production environment.

v) **Confidently and Privacy**
All critical data are masked and that only authorized users have access to data in its entirety. Digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

III. FOCUS ON SECURITY ISSUES OF LARGE SCALE DISTRIBUTED DATABASE

The main aspect describing the achievement of any new computing technology is the height of security it provides whether the data located in the cloud is protected at that level that it can avoid any sort of security issue [5]. So it must say that Security and privacy are the key challenges in the cloud computing. Here are some security issues, we have presented in this paper.

1. **Data confidentiality issue**
Confidentiality is a set of rules or an agreement that bounds access or location restriction on certain types of information so in cloud data reside publically so Confidentiality refers to, customers data and computation task are to be kept confidential from both cloud provider and other customers who is using the service.
   a. Situation 1. The first situation where user's information may be disclosed when service provider knows where the user's private information resides in the cloud systems.
   b. Situation 2. The second situation where user's information may be disclosed when service provider has the authority to access and gather user's private information in the cloud systems.
   c. Situation 3.The third situation where user's information may be disclosed when service provider can figure out the meaning of user's information in the cloud systems.

   These are the following situation due to, service provider can collect or get access users information or data, if the service provider must know the place of the data in the cloud computing and have the authority to access users data. As we know that the current cloud computing consists of three layers Software layer, Platform layer, Infrastructure layer. Software layer provider the user interface for the user to use the services running on the cloud infrastructure. The platform layer provides the platform such as operation environment for software to run with the help of provided system resources. And the infrastructure layer provides the hardware resources for computing, storage and network. Although as the each service provider has its own software, platform and infrastructure layer with this when user uses the cloud application provided by service provider, it is mandatory for the user to use the platform as well as infrastructure provided by the service provider and therefore service provider is aware of, where the users data is placed and the full accessibility to the data.

2. **Data availability issue**
At remote location which is owned by others, data owner may face the problem of system failure of the service provider. And if cloud stops working, data will not be available as the data depends on single service provider. Threats to data availability are flooding attacks causes deny of service and Direct /Indirect (DOS) attack. Cloud computing is to provide on-demand service of different levels. If a certain service is no longer available or the quality of service cannot meet the Service Level Agreement (SLA), customers may lose faith in the cloud system.

3. **Data integrity issue**
The data integrity proofs the validity, consistency and regularity of the data. It is the perfect method of writing of the data in a secure way the persistent data storage which can be reclaim or retrieved in

the same layout as it was stored later. Therefore cloud storage is becoming popular for the outsourcing of day-to-day management of data .So integrity monitoring of the data in the cloud is also very important to escape all possibilities of data corruption and data crash. The cloud provider should provide surety to the user that integrity of their data is maintained in the cloud.

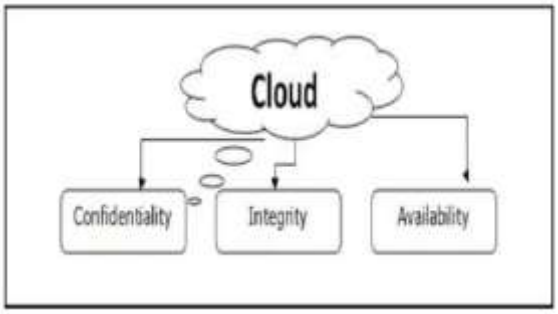

Figure 1 – Basic Security Threats

4. **Data security issue**
   When data storage in the cloud computing or on premise application deployment model, the sensitive data of every enterprise continues to reside within the enterprise boundary and is focus to its physical, logical and personnel security and access control guidelines. Though in Software-as-a-Service model or public cloud the enterprise data is stored outside the enterprise boundary, by the CSP. So as a result, the CSP must agree to implement additional security checks to ensure data security and need to prevent breaches because of security vulnerabilities in the application or through malicious employees. These all above concern issues require to use a strong encryption techniques for the protection of the data because the some traditional encryption which have been used since, are not as powerful as we need. The data protection needs to be implemented in order to secure data from the following uncertainties.
5. **Trust issue**
   Trust is also a major issue in cloud computing. Trust revolve around assurance and confidence that people, data, objects, information will perform or behave in projected way. Trust can be in between, human to human, machine to machine, human to machine or machine to human. Therefore in cloud computing when any user store their data on cloud storage, they must have trust to the cloud provider so that they don't scare to put their data on cloud, likewise we use Gmail server, yahoo server because we trust our provider. Therefore cloud provider must have to come forward to tackle with the trust issue and build trust with the users so that more and more people will be able to take advantage of cloud computing without having any doubt.
6. **Data locality issue**
   In the data storage model of cloud computing environment the user the applications provided by the service provider and process their data but in this scenario the user does not have any knowledge about where their data is being stored, in many situations this can be a legal issue.

IV. MAJOR SECURITY CHALLENGES AND THREATS

Cloud computing was a new concept of providing dramatically scalable and virtualized resources, bandwidth, software and hardware on demand to consumers. As provides the sharing of data and resources so there are various security threats at various layers while implementing cloud computing. Some of them are given below-

1. **Application Layer Security Threats**
   Application security is the first level security. The application can only be accessed by providing some kind of credentials. The application security can be divided in four part 1.Identity based access 2. Role based access 3. Key based access 4. Claim based access [7][8].
   a) **Interface and APIs**
      Cloud computing provides number of interfaces and APIs to interact with the services provided to the users. These interfaces and APIs demands authorization and authentication before their usage. Organization and third parties build upon these interfaces to value-added services to their customers. This introduces the complexity of the new layered API. It also increases risk.

b) Cloud service user access

Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are reused, which amplifies the impact of such attacks.

2. Transport Layer Security Treats

This is a protocol that ensures privacy between communicating applications and their users on the Internet. TLS is the successor to the Secure Sockets Layers. The Transport Layer Security is layered on top of the Transport Layer such as TCP. The protocol is composed of two layers: the TLS record layer and the TLS handshake layer. Transport layer suffer various security problems such as –

a) Data Leakage

The loss of encryption key or privileged access code will bring serious problems to the cloud service users. Accordingly to lack of cryptography information such as encryption keys, authentication codes and access privileges will heavily lead sensitive damages on data loss and unexpected leakage to outside.

b) Loss of reliability

Data protection includes access to data for the confidently as well as its integrity. If the cloud service user trust is not in the central of cloud security, it is a major differentiator for a cloud service provider.

3. Virtual Layer Security Threats

Hackers and Security researchers have shown that these capabilities of virtualization can be exploited to create new and more robust forms of malware that are hard to detect and can evade current security technologies. There are following security branches of virtual layers.

a) vSwitch attacks

This is vulnerable to a wide rage of layer-2 attacks like a physical switch. These attacks include vSwitch configurations, VLANs and trust zones, and ARP tables.

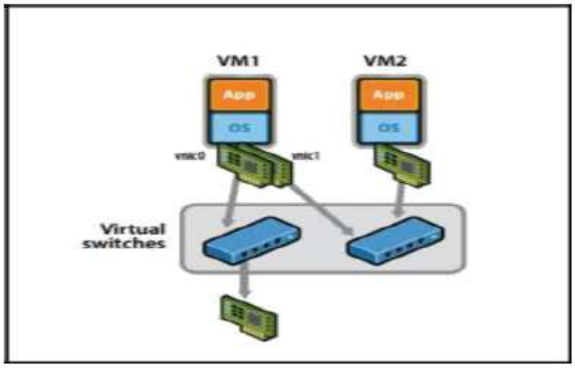

Figure 2 – Virtual Switches with uplink port or with no uplink port [9]

b) Virtual Machine Attacks

Cloud servers contain tens of VMs; These VMs may be active or offline. Active VMs are valuable to all traditional attacks that can affect physical servers. The VMs share the same hardware and software resources e.g. memory, device, drivers, storage [10]. In a single server and sharing the same resources increases the attack surface and the risk of VM to VM. When VM becomes offline, it is still available as VM image files that are susceptible to malware infections and patching. Various security threats at various layers as given table –

Layer	Security issue
Application Layer	Insure cloud service for user access
	Insecure interface and APIs
Transport Layer	Data Leakage
	Loss of reliability
Virtual Layer	vSwitch attack
	VM attack

Table 2 – Security threats at various layers

With the analysis of the widely used cloud computing technology Distributed File System, we will get the data security needs of cloud computing. Distributed database is used in large-scale cloud computing in typical distributed file system architecture, its design goal is to run on commercial hardware, and the advantages of open source, it has been applied in the basis of cloud facilities. It is very similar to the existing distributed file system, such as GFS (Google File System) [11]. They have the same objectives, performance, availability and stability. The master is called Name node, which manages the file system name space and controls access to the client. Other slave nodes is called Data node, Data node controls access to his client. In this storage system, a file is cut into small pieces of paper, Name node maps the file blocks to Data nodes above. The file system still support the creation, delete, open, close, read, write and other operations on files.

Data security needs of cloud computing can be divided into the following points: The client authentication requirements in login: The vast majority of cloud computing through a browser client, such as IE, and the user's identity as a cloud computing applications demand for the primary needs[12]. The existence of a single point of failure in Name node: if name node is attacked or failure, there will be disastrous consequences on the system. So the effectiveness of Name node in cloud computing and its efficiency is key to the success of data protection. The rapid recovery of data blocks and r/w rights control: Data node is a data storage node, there is the possibility of failure and cannot guarantee the availability of data. In addition to the above three requirements, the other, such as access control, file encryption, such as demand for cloud computing model for data security issues must be taken into account. All the data security technique is built on confidentiality, integrity and availability of these three basic principles. Confidentiality refers to the so-called hidden the actual data or information, especially in the military and other sensitive areas, the confidentiality of data on the more stringent requirements. For cloud computing, the data are stored in "data center", the security and confidentiality of user data is even more important. The so-called integrity of data in any state is not subject to the need to guarantee unauthorized deletion, modification or damage. The availability of data means that users can have the expectations of the use of data by the use of capacity. Large Scale Distributed Database Security Model

Database model of cloud computing can be described in math as follows-

DF = C (Name Node)
Kf = f * DF
C ( ): the visit of nodes
DF: the distributed file f
Kf: the state of data distribution
F is the file and can be described as
f = { F(1),F(2),…….F(n)}, means f is the set of n file blocks F(i) ∩ F(j) = €, i≠j; j<=1,2,3….n

To enhance the data security of cloud computing, we provide a Cloud Computing Data Security Mode called C2DSM.It can be
Described as follows:
D'f = CA (namenode)
D'f = M. D'f
Kf = E(f) Df
Df is not order, Df can convert to D*f (l- i) matrix i>=1; Kf become L – i length vector, that make confliction to the definition of the model.

V. CONCLUSION

Security is an active area of research and experiment. As the development of cloud computing, security issue has become a top priority. To address these issues requires getting confidence from user for cloud applications and services. Managing and providing secure environment is attracting much attention. This paper discusses the cloud computing environment with the safety issues through analyzing a cloud computing framework and also provides a study about various security risks at different layers. This study will help to manage a secure connection at various layers. This focus on the analysis of the solution in the cloud environment. Finally it conclude a cloud computing model for data security.

REFERENCES

[1] Top Threats to Cloud Computing, Version 1.0, CSA 2013
[2] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, and Sagata Sanyal published, "A survey on Security Issues in Cloud Computing in Cornell University, May 2013.
[3] Kangchan Lee published,"Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications Vo. 6, No. 4, October, 2012.
[4] Secure, Reliable and compliant: How the cloud can make archiving profitable for the channel, An Osterman Research white paper, July 2011.
[5] Amani S. Ibrahim, James Hamlyn-Harris and John Grundy, published,"Emerging Challenges of Virtual Infrastructure
[6] Security and Security privacy Issues in Cloud Computing Jaydip Sen Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA
[7] Jean-Daniel Cryans, Criteria to Compare Cloud Computing with Current Database Technology 2008
[8] Christopher Moretti,All-Pairs: An Abstraction for DataIntensive Cloud Computing IEEE 2008
[9] Huan Liu, Dan Orban, GridBatch: Cloud Computing for Large-Scale Data-Intensive Batch Applications IEEE DOI 10.1109/CCGRID.2008.30
[10] Mladen A. Vouk Cloud Computing – Issues, Research and Implementations Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246
[11] Bob Gourley, Cloud Computing and Net Centric Operations ' Department of Defense Information Management and Information Technology Strategic Plan 2008-2009.
[12] Cloud Computing Security:making Virtual Machines Cloud-Ready, www.cloudreadysecurity.com 2008.