EXPERIMENT NO.7

DATA STORAGE SECURITY IN PRIVATE CLOUD.

AIM: A Study of Data Storage Security Issues in Cloud Computing.

THEORY:

Cloud computing is the combination of many pre-existing technologies that have matured at different rates and contexts. The purpose of cloud computing is to allow all users to take benefit from all these technologies. Many organizations are moving towards cloud because it allows the users to store their data on clouds and can access at any time and anywhere. Data breaching is a possible way in a cloud environment, since data from various users and business organizations lie together in the cloud. By uploading the data to the cloud, the data owners transfer the control of their data to a third person that may raise security problems. Cloud users place their confidential or sensitive data, it includes personal health records, emails and government sensitive files.

Cloud Storage: In cloud computing cloud storage is the primary user. Cloud storage as a storage of the data online in the cloud. Cloud computing does not provide control over the stored data in cloud data centers. The cloud service providers have control over the data, they can perform any malicious tasks such as copy, destroying, modifying, etc. Distributed data centers include a cloud storage system, which typically uses cloud-computing technologies and offers some kind of interface for storing and accessing data. When storing data on the cloud, then the data is stored in a particular place with a specific name.

There are four main types of cloud storage:

Personal Cloud Storage: It is also called mobile cloud storage. In personal cloud storage individual data is stored in the cloud, and he may access the data from anywhere.

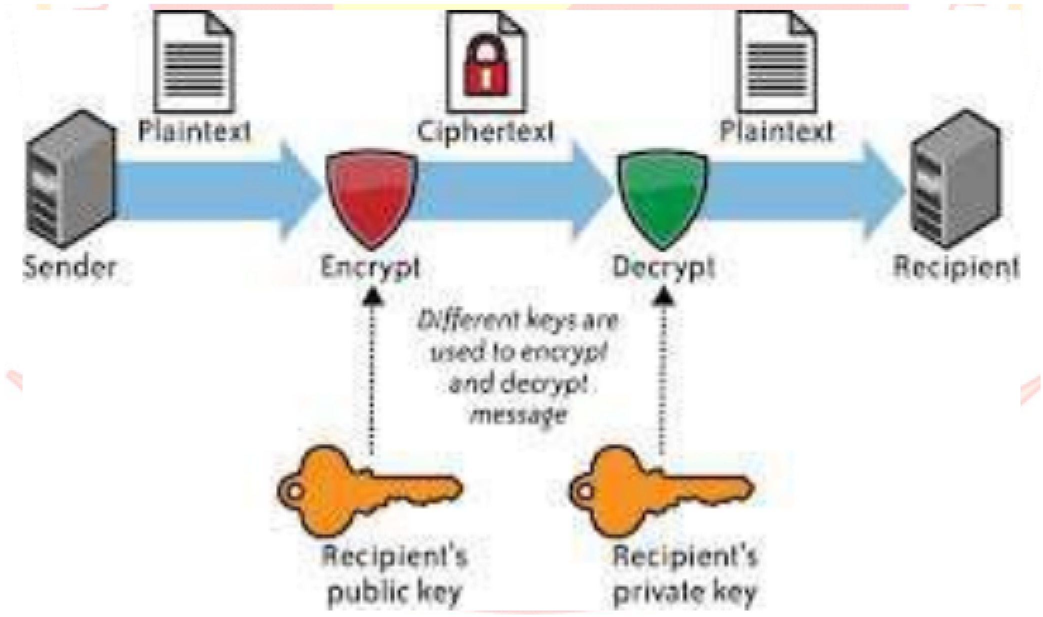
Public Cloud Storage: The enterprise and storage service provider are separate and they do not have any cloud resources stored in the enterprise's data centre. Public cloud storage fully manages the cloud storage provider.

Private Cloud Storage: It is the enterprise and cloud storage provider integrated in the enterprise's data centre. In this storage, the storage provider has infrastructure in the enterprise's data centre that is typically managed by the storage provider. Private cloud storage helps resolve the potential for security as well as performance.

Hybrid cloud storage: It is a combination of public and private cloud storage, where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

Encrypted Data Storage for Cloud: Data in the cloud is placed anywhere, it is important that the data can be encrypted. We are using the secure co-processor as part of the cloud infrastructure to enable efficient encrypted storage of sensitive data. The secure co-processor is tamper resistant, one could be tempted to run the entire sensitive data storage. Pushing the entire data storage functionality into a secure co-processor is not feasible due to many reasons. Another issue is that the software running on the SCP must be totally trusted and verified. This security requirement implies that the software running on the SCP should be kept as simple as possible. We can encrypt the sensitive data sets using random private keys and to alleviate the risk of key disclosure. V.

Security and Privacy Issues in Data Storage: Cloud Computing allows the users to store their data on the storage location maintained by a third party. Once the data is uploaded into the cloud the user loses its control over the data and the data can be tampered by the attackers. The attacker may be an internal (CSP) or external.



DATA SECURITY AND STORAGE

The protection of information arises from the following challenges:The security and privacy issues related to data storage are confidentiality, integrity and availability.

A.Confidentiality: The major dispute in cloud computing is confidentiality. Data confidentiality means accessing the data only by authorized users and is strongly related to authentication. In another way confidentiality means keeping users' data secret in the cloud systems. As we are storing the data on a remote server and transferring the control over the data to the provider here arises the questions such as:

For ensuring confidentiality, cryptographic encryption algorithms and strong authentication mechanisms can be used. Encryption is the process of converting the data into a form called ciphertext that can be understood only by the authorized users. Blowfish is a fat and simple encryption algorithm.

B. Integrity

Another serious problem faced by cloud computing is integrity. Integrity of data means to make sure that the data has not been changed by an unauthorized person or in an unauthorized way. It is a method for ensuring that the data is real, accurate and safeguarded from unauthorized users. As cloud computing supports resource sharing, there is a possibility of data being corrupted by unauthorized users. Digital Signatures can be used for preserving the integrity of data. The simple way for providing integrity is using Message Authentication Code (MAC).

C. Availability

Availability refers to being available and accessible to authorized users on demand. The aim of availability in cloud computing systems is to ensure that its users can use them at any place and at any time.

Contractual and Legal issues:

After moving to a cloud computing environment, there are many issues in geographic regulatory law, performance assurance, contract enforcements, etc. The issues come under the legalities, Service Level Agreements and data location in data centers.

Service level agreements:

The Service Level Agreement (SLA) can be described as a protocol, it specifies a set of conditions and terms among user and Cloud service provider. The SLA should specify the following: Actions that CSP will take when a data breach happens, remedial actions and performance level at minimum level.

Legal issues:

The legal issues arise because of the presence of CSP resources in geographically conflicting various legal jurisdictions. If the user is migrated from one geographical to another, an issue will occur because of different legal jurisdictions. For a movement data is distributed over various data centers, those are owned by CSP that have different laws and security guidelines. This scenario may take into the serious issue in cloud computing.

Data backup:

The data backup is important when accidental and/or intentional disasters. The CSP has to perform regular backups of stored data to ensure the data availability. In fact, the backup data should be kept with security guidelines to prevent malicious activities such as tampering and unauthorized access.

CONCLUSION:

Cloud computing enables users to store their data in remote storage locations. But In cloud computing data security is a major threat. Due to this many organizations are not willing to move into a cloud environment. To overcome this, confidentiality, integrity, availability should be encapsulated in a CSP‘s Service-Level Agreement (SLA) to its customers. Effective auditing mechanisms also can be used for providing data integrity