**Episteme: an online interdisciplinary, multidisciplinary & multi-cultural journal**
**Bharat College of Arts and Commerce, Badlapur, MMR, India**
**Volume 8, Issue 2** **September 2019**

# *A STUDY OF DATA STORAGE SECURITY ISSUES IN CLOUD COMPUTING*

**By Ankita Awsarmal**

**Abstract**

Cloud Computing is defined as an environment in which users can share their resources with others in pay per use model. The resources are stored centrally and can access from anywhere. Cloud computing provides on demand services to its clients. Data storage is among one of the primary services provided by cloud computing. Cloud service provider hosts the data of data owner on their server and user can access their data from these servers. As data, owners and servers are different identities, the paradigm of data storage brings up many security challenges. An independent mechanism is required to make sure that data is correctly hosted in to the cloud storage server. In this paper, we will discuss the different techniques that are used for secure data storage on cloud.

**Keywords**

Cloud computing, Data storage, Cloud storage server, Confidentiality, Encryption, Integrity, Privacy, and Security.

**Objective**

Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Microsoft etc. There are some security issues creeping in while using services over the cloud. This research paper presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure.

**Introduction**

The National Institute of Standard and Technology's (NIST) defined cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. The NIST has listed five main characteristics of cloud computing as:

- On-demand self-service: Resources are available to users based on their demand.
- Broad network access: The services are rendered over the network and the users can access it if having an internet connection.
- Resource pooling: Resources from vendors are pooled to serve multiple users.
- Rapid elasticity: Users can access the resources whenever needed and also they can release the resources when they no longer required.
- Measured service: Users have to pay only for the time they are using the resources.

The delivery models are:

- Infrastructure as a Service (IaaS): The IaaS model offers the infrastructure to run the applications.
- Platform as a Service (PaaS): The PaaS model enables the application developer with a development environment and also offer the services provided by vendor.
- Software as a Service (SaaS): In SaaS model, the users can use the software for rent instead of purchasing it.

Cloud computing is the combination of many preexisting technologies that have matured at different rates and in different contexts. The goal of cloud computing is to allow users to take

benefit from all these technologies. Many organizations are moving into cloud because it allows the users to store their data on clouds and can access at anytime from anywhere. Data breaching is possible in cloud environment, since data from various users and business organizations lie together in cloud. By sending the data to the cloud, the data owners transfer the control of their data to a third person that may raise security problems. Sometimes the Cloud Service Provider (CSP) itself will use/corrupt the data illegally.

Security and privacy stands as major obstacle on cloud computing i.e. preserving confidentiality, integrity and availability of data. A simple solution is to encrypt the data before uploading it onto the cloud. This approach ensures that the data are not visible to external users and cloud administrators but has the limitation that plain text based searching algorithm are not applicable. In this paper, the security flaws in data storage and the mechanisms to overcome it.

**Cloud Storage:**

Cloud storage is one of the primary use of cloud computing. We can define cloud storage as storage of the data online in the cloud. A cloud storage system is considered as a distributed data centers, which typically use cloud-computing technologies and offers some kind of interface for storing and accessing data. When storing data on cloud, it appears as if the data is stored in a particular place with specific name. There are four main types of cloud storage:

**1) Personal Cloud Storage:**

It is also known as mobile cloud storage. In this type storage, individual's data is stored in the cloud, and he/she may access the data from anywhere.

**2) Private Cloud Storage:**

In Private Cloud Storage the enterprise and cloud storage provider are integrated in the enterprise's data centre. In private cloud 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 and performance concerns while still offering the advantages of cloud storage.

**3) 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.

**Threats in Cloud Computing**

There are certain aspects associated with Cloud Computing as a result of which many organizations are still not confident about moving into the cloud. The Computer Security Alliance Group has listed the threats that may occur in cloud computing. They are:

- Abuse of cloud computing.
- Insecure Interfaces and API's.
- Malicious Insiders.
- Shared Technology Issues.
- Data Loss and Leakage.
- Account or Service Hijacking.
- Unknown Risk Profile.
- Hardware Failure.
- Natural Disasters.
- Closure of Cloud Service.
- Cloud-related Malware.
- Inadequate Infrastructure Design and Planning.

Among these data loss and leakage was ranked as the second most common threat. Data loss and leakage occurs due to lack of security and privacy in both storage and transmission. To reduce this risk, the data security aspects taken into account are:

- Data-in-transit refers to the data during transmission either from data owner to cloud provider or from cloud provider to owner.
- Data-at-rest: Data-at-rest refers to the data in the storage.
- Data lineage: Data lineage specifies what happened to data from its source through distinct applications and its use for auditors. Data lineage is difficult for public clouds.

- Data provenance: Data provenance is not just proving the integrity of data, but the more specific history of the data i.e., who created, modified and deleted the data in the cloud.
- Data remanence: Data remanence refers to the data left behind after deletion.

This paper highlights the issues related to data storage. Data Storage refers to storing the data on a remote sever hosted by the CSP. The benefits of data storage in cloud are:

- Provides unlimited storage space for storing user's data.
- User can access the data at anytime from anywhere using an internet connection in more than one machine.
- No need to buy the storage device for storing the data.

The main constraint in data storage was absence of security and privacy which arises due to loss of control over the data. The basic requirements for secure data storage are:

- The data on the cloud must be confidential and CSP should not be able to compromise it at any cost.
- Data access must be given to the intended user only.
- The data owner must have full control over the authorization of data.

**Literature Review**

1) Data storage issues solutions

The SecCloud is presented by Wei et al. it provides a storage security protocol for cloud customer's data and it not only secures the stored data but also provides security on computational data. The SecCloud protocol uses encryption for storing data in secure mode. The multiplicative groups and cyclic additive pairing is used for key generation for cloud customers, CSP, and other business partners or trusted third party. The encrypted data along with the verifiable signature is sent to cloud data center along with session key. The Diffie-Hellman algorithm is used for generation of session key for both bilinear groups. By receiving encrypted data the cloud decrypts the data, verifies the digital signature and stores the original data in specified location in cloud. The SecCloud verifies whether data is stored at specified location or not. The Merkle hash tree is used for computation security in SecCloud protocol. The verifying

agency will verify the computational results that are building by using Merkle hash tree. The File Assured Deletion (FADE) protocol provides a key management with data integrity and privacy.

2) Identity management and Access control solutions

The authors proposed Simple Privacy preserving Identity Management for Cloud Environments (SPICE) for identity management systems. The SPICE ensures group signature for providing the unidentified authentication, access control, accountability, unlink ability, and user centric authorization. The SPICE provides above mentioned properties with only a single registration. After user registration with trusted third party they obtain unique credentials for all the services provided by CSP. By using the credentials, user generates authentication certificate. Different CSPs expecting variety attributes for authentication and user has to generate their required form of authentication certificate with same credentials.

**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. Unauthorized access is also a common practice due to weak access control. The protection of information arises the following challenges:

- Access control: Are there appropriate controls over access of information when stored in the cloud?
- Structured versus unstructured: How is the data are stored? Whether it supports data access in a very fast manner?
- Integrity/availability/confidentiality: How are data integrity, availability and confidentiality maintained in the cloud?
- Encryption: Several laws and regulations require that certain types of information should be stored only when encrypted. Is this requirement supported by the CSP?

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 cipher text that can be understood only by the authorized users. Encryption is an efficient technique for protecting the data but have the obstacle that data will be lost once the encryption key is stealed algorithms. 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).Message Authentication Code is a cryptographic checksum calculated using hash functions and is send along with the data for checking the integrity. Auditing mechanisms can also be used for preserving integrity. In private auditing the integrity of data is checked by the data owner using algorithms.

**C. Availability:**

It 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.

**Research Methodology**

The complexity of the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques are needed to be radically tweaked to be able to work with the clouds architecture.

**Conclusion**

Cloud computing enables users to store their data in remote storage location. But data security is the major threat in cloud computing. Due to this many organizations are not willing to move into cloud environment. To overcome this, confidentiality, integrity, availability should been capsulated in a CSP's Service- Level Agreement (SLA) to its customers. Otherwise ensure that any sensitive information is not put into a public cloud and if any it is to be stored in encrypted form. Effective auditing mechanisms also can be used for providing data integrity.

**References**

[1] V.Nirmala, R.K.Sivanandhan, Dr.R.Shanmuga Lakshmi, "Data Confidentiality and Integrity Verification usingUser Authenticator scheme in cloud", Proceedings of 2013 International Conference on Green High Performance Computing (ICGHPC 2013). March 14-15, 2013, India.

[2] Arjun Kumar, Byung Gook Lee, HoonJae Lee, Anu Kumari, "Secure Storage and Access of Data in Cloud Computing", 2012 International Conference on ICT Convergence (ICTC), 15-17 Oct. 2012.

[3] M.R.Tribhuwan, V.A.Bhuyar, Shabana Pirzade, "Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management", 2010 International Conference on Advances in Recent Technologies in Communication and Computing.

[4] Mr. Prashant Rewagad, Ms.Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", 2013 International Conference on Communication Systems and Network Technologies.

[5] Uma Somani, Kanika Lakhani, Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel, Volume 3, Issue 1, January-February-2018 | www.ijsrcseit.com | UGC Approved Journal [ Journal No : 64718 ] 1745 Distributed and Grid Computing (PDGC - 2010).

[6] M. AlZain, E. Pardede, B. Soh, and J. Thom, "Cloud computing security: From single to multi-clouds," in System Science (HICSS), 2012 45th Hawaii International Conference on, Jan 2012, pp. 5490–5499.

[7] M. Sookhak, H. Talebian, E. Ahmed, A. Gani, and M. K. Khan, "A review on remote data auditing in single cloud server: Taxonomy and open issues," Journal of Network and Computer Applications, vol. 43, pp. 121–141, 2014.

[8] E. Aguiar, Y. Zhang, and M. Blanton, "An overview of issues and recent developments in cloud computing and storage security," in High Performance Cloud Auditing and Applications. Springer, 2014, pp. 3–33.

[9] I. Gul, M. Islam et al., "Cloud computing security auditing," in Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on. IEEE, 2011, pp. 143–148.

**Bio**

Ankita Awsarmal is working as an Assistant Professor at Bharat College of Arts & Commerce. The author can be reached at ankitaawsarmal@gmail.com.