# Review on Secure Auditing, Preserving and Integrity of Data Using TPA on Cloud Storage

Sayali Vichare[1], Rupesh Shinde[1], Pooja Patil[1], Pankaj Pawar[1], Prof. Swati Gajbhiye[1]

*Department of Information Technology*[1]

*Shah &Anchor Kutchhi Engineering College, Mumbai-India*

**Abstract** —User should use the data storage without any loss as it is stored locally. Auditing process is important process to ensure integrity, user are not that skilful to maintain integrity of data and they are not aware about risk and security action. Hence so to perform user can depend on TPA (third party authentication), which will check integrity and privacy on cloud data which is stored locally.TPA audit the integrity and provides appropriate result to user. Results contain modified, deleted and uploaded information of files. User has to make sure that privacy is preserved from TPA with minimal consumption of cloud resources while auditing process. In this paper we propose a system that will provide integrity to locally stored data without downloading files avoiding additional resources and vulnerability. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

***Keywords***- *cloud computing, integrity, privacy, cryptography, privacy preservation.*

*****

## I. INTRODUCTION

Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network.

Cloud computing exhibits the following key characteristics:

a) Agility for organizations may be improved, as cloud computing may increase users' flexibility with re-provisioning, adding, or expanding technological infrastructure resources.

b) Cost reductions are claimed by cloud providers. A public-cloud delivery model converts capital expenditures (e.g., buying servers) to operational expenditure. This purportedly lowers barriers to entry, as infrastructure is typically provided by a third party and need not be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is "fine-grained", with usage-based billing options. As well, less in-house IT skills are required for implementation of projects that use cloud computing. The e-FISCAL project's state-of-the-art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

c) Device and location independence enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect to it from anywhere.[43]

d) Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places (e.g., different work locations, while travelling, etc.

e) Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

f) Utilisation and efficiency improvements for systems that are often only 10–20% utilised.

g) Performance is monitored by IT experts from the service provider, and consistent and loosely coupled architectures are constructed using web services as the system interface.

h) Productivity may be increased when multiple users can work on the same data simultaneously, rather than

waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer.

i) Reliability improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

j) Scalability and elasticity via dynamic ("on demand") provisioning of resources on a fine-grained, self-service basis in near real-time (Note, the VM startup time varies by VM type, location, OS and cloud providers), without users having to engineer for peak loads. This gives the ability to scale up when the usage need increases or down if resources are not being used.

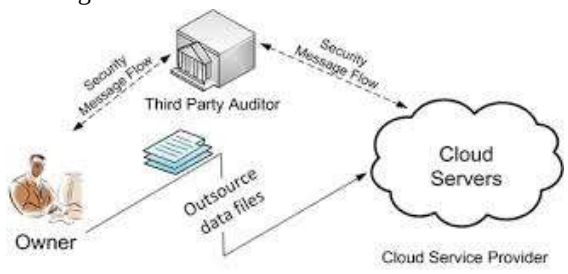


Fig:- Network architecture for cloud data storage

## II. SECURITY IN CLOUD COMPUTING

Cloud computing faces various security threats for several reasons:

a) Loss of control - the user's loss the control of data in the cloud environment and hence the usual cryptographic techniques cannot be directly applied for the purpose of data security. To ensure continuous and long term data security of the various kinds of data stored in the cloud, the problem of integrity and correctness of stored data in cloud becomes more challenging.

b) Integrity of data – The stored data need to be frequently updated. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. However, such important area remains to be fully explored in the literature.

In cloud computing, many users and even the resources join or leave the cloud at random. There should be a trustworthy relationship among the users, resources and the cloud. Establishing the trustful relationship is a challenge because of the different security policies of the users and the resources in the cloud. In fact, there will be a Service Level Agreement between the cloud participants to maintain the confidentiality of their data. The traditional way to ensure security of data during transmission and storage is to compress the data and encrypt it. Unencrypted data of the client cannot be stored in the cloud because the cloud provider will have access to the data and hence the confidentiality of the data will be lost. Also, a malicious cloud provider can modify the client's data and hence, the integrity of the data will be lost. An encrypted file system is used to encrypt the user's data, manage and create keys which are used for data encryption and decryption. The encryption and decryption of files is transparent to the user and the application. The dependable and secure computing includes not only security and confidentiality, but also reliability, availability, safety and integrity. Considering these facts, we propose a new way that is conducive to improve the secure and dependable computing in cloud. Cloud computing provides Internet-based services to customers and business and also provides significant cost effective IT resources as cost on demand IT based on the actual usage of the customer. The cloud computing technology helps companies with much more efficient computing by centralizing resources, but at the risk of data privacy. The diversity of users multiplies the associated risk. Identity management (IDM) is one of the key components in cloud privacy and security. This can improve security and user satisfaction and help reduce some of the problems associated with cloud computing. The identity management can be deployed by a centralized component processing authentication and authorization requests. [1]

The foremost issues in cloud data security include data privacy, data protection, data availability, data location, and secure transmission. Threats, data loss, service disruption, outside malicious attacks, and multi tenancy issues are the security challenges included in the cloud. Data integrity in the cloud system means preserving the integrity of stored information. The data should not be lost or modified by unauthorized users.

Data auditing is introduced in Cloud computing to deal with secure data storage. Auditing is a process of verification of user data which can be carried out either by the user himself (data owner) or by a TPA. It helps to maintain the integrity of data stored on the cloud. The verifier's role are categorized into two: first one is private audit ability, in which only user or data owner is allowed to check the integrity of the stored data. No other person has the authority to question the server regarding the data. But it tends to increases verification overhead of the user. Second is public auditability, which allows anyone, not just the client, to challenge the server and performs data verification check with the help of TPA. The TPA is an entity which is used so that it can act on behalf of the client. It has all the necessary expertise, capabilities, knowledge and professional skills which are required to handle the work of integrity verification and it also reduces the overhead of the client. It is necessary that TPA should efficiently audit the cloud data storage without requesting for the local copy of data. It should have zero knowledge about the data stored in the cloud server. It should not introduce any

additional on-line burden to the cloud user . The three network entities viz. the client, cloud server and TPA are present in the cloud environment. The client stores data on the storage server provided by the cloud service provider (CSP). TPA keeps a check on client's data by periodically verifying integrity of data on-demand and notifies client if any variation or fault is found in client's data. [2]

## III. RELATED WORK

Cloud computing faces many problems on integrity and privacy of user's data stored in the cloud. Hence it requires some secure and efficient methods which can ensure the integrity and privacy of data stored in the cloud.

Mr. Satishkumar R proposed Encryption and Proxy encryption algorithm to protect the privacy and integrity of outsourced in cloud Environment. Secure privacy preserving public auditing cloud storage using DES encryption techniques. Cloud data security is an important aspect for the client while using cloud services. The third party is used to resolve any kind of conflicts between service provider and client [3].

Mrs. Shingare Vidya Marshal, utilize the Public Provable Data Possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at untrusted server; can be used to realize audit services.With random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. To support efficient Handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users [5].

Wang et al. [6] has proposed a privacy preserving public auditing protocol which makes use of an independent TPA to audit the data. It utilizes the public key based homomorphic linear authenticator (HLA) with random masking techniques. But this protocol is vulnerable to existential forgeries known as message attack from a malicious cloud server and an outside attacker. To overcome this problem, Wang et al. [4] proposed a new improved scheme which is more secure than the protocol proposed in [6]. It is a public auditing scheme with TPA, which performs data auditing on behalf of users. It uses HLA which is constructed from Boneh-Lynn-Shacham short signature referred as BLS signatures. It also uses random masking for data hiding. For the sake of data binding, this new scheme involves computationally intensive pairing operation thus making it inefficient to use. This proposed scheme has been implemented practically on Amazon EC2 instance which demonstrates the fast performance of the design on both the cloud and the auditor side.

## IV. EXISTING SYSTEM

Cloud Computing is a promising area providing computing and other services to the cloud users. It provides the users with many advantages primarily increasing or decreasing the number of resources according to user's requirements. As the saying goes, "Every Coin Has Two Sides", Cloud Computing also has its own share of problems and challenges. Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity

The cloud computing suffers from the following drawbacks:

DATA SECURITY AND PRIVACY: - Data is stored in the cloud shared by multiple tenants. The data location is mobile, that is, it can move from one location to another. The cloud users may not be aware of the data location or about the access log of their data. The confidential information is stored away from its owner, which increases its vulnerability. This raises serious questions about the security of user's data. Since many people are managing the cloud at the same time, the privacy of cloud data cannot be guaranteed. Any number of people can eavesdrop over the data.

IDENTITY AND ACCESS MANAGEMENT: - Data in the cloud is stored at multiple locations, that is, the location of data in the cloud is mobile. The cloud user may or may not be aware of his data's location. The cloud being multi-tenant in nature, the cloud user may have to logon using different user credentials for different providers. This poses potential threat to data as any individual may fake as the original owner in case the credentials are lost/leaked outside the system. A cloud needs to have a strong and sturdy identity and access management system in place so as to attract more transfers to the cloud. [7]

## V. PROPOSED SYSTEM

The proposed system will be developed to verify the correctness of cloud data by TPA, periodically or on demand without retrieving the entire data or without introducing additional online burden to the cloud users and cloud servers. It will assure that no data content is leaked to TPA during the auditing process. It maintains storage correctness of data, integrity and confidentiality of stored data.

In the proposed scheme, to perform the task of data auditing a TPA is been used for this purpose. TPA performs data auditing either periodically or on demand by the client. On receiving the auditing request from user or data owner, the TPA starts its auditing process. TPA will store the signature which has been generated by data owner. The TPA follows the same process performed by data owner such as generating hash for encrypted blocks of data files, concatenating them and generating signature on it. Later it compares the two signatures in verification process. If it matches then it means the integrity of data is maintained and otherwise not maintained. This

means that data is not been tampered or changed. The result for the same is provided to the data owner by the TPA.

## VI. CONCLUSION

In this paper, an essential and efficient secure auditing system is been proposed. Auditing preserving and integrating data is successfully achieved using a TPA (Third Party Auditor).It therefore results in auditing without retrieving the copied data through which privacy is preserved. TPA is used to verify the data integrity requested by the client but it only checks whether the stored data is tampered or not and informs it to the user. We have tried to overcome the limitations of the existing auditing scheme. An attempt is made to make cloud data more secure for the clients using cloud services.

## REFERENCES

[1] Susmita J A Nair1 , Anitha K L2 , Rosita F Kamala3,"Trusted Third Party Authentication in Cloud Computing" ,Vol. 2 Issue 11, November – 2013, International Journal of Engineering Research & Technology (IJERT)

[2] Swapnali Morea , Sangita Chaudharib," Third Party Public Auditing scheme for Cloud Storage", 7th International Conference on Communication, Computing and Virtualization 2016

[3] Mr. Satishkumar R, "Secure Privacy Preserving Public Auditing for Cloud Storage" ISSN: 2319-8753, Volume-3, Special Issue 1, January 2014.

[4] Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy Preserving Public Auditing for Secure Cloud Storage. *http://eprint.iacr.org/2009/579.pdf*

[5] Mrs. Shingare Vidya Marshal, "Secure Audit Service by Using TPA for Data Integrity in Cloud System" ISSN: 2278-3075, Volume-3, Issue-4, pp. 50, September 2013.

[6] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing.

[7] Parul Chachra," A Survey of the Existing Security Issues in Cloud Computing", Vol. 5 (2)