International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 8, Issue 3, May 2021 |

Privacy Preserving System For Shared Data in the Cloud Environment by Using Public Auditing Scheme: A Review

Sudhakar H. Yerme

Department of CSE, HVPM College of Engineering & Technology, Amravati, Maharashtra, India

ABSTRACT: In cloud data can be store in large scale and which can be shared as well it means that a single database can be controlled or access by single or multiple users at same instance. The data can be accessed by user or group of user as well. The data owner plays an important role in these things that is owner will decide the access of data to TPA. In such system for TPA it's necessary to maintain the security and integrity of data.So that system is going to perform the privacy preserving on to the all data which is shared in group or with TPA for auditing .this will help to maintain data integrity for auditor and security over shared data.

KEYWORDS: Cloud Storage, TPA, Privacy Preserving, Public Auditing, Integrity

I. INTRODUCTION

Cloud computing is a type of internet based computing that provides shared computer processing resources and data to computers and other devices on demand, and provide the storage space to the users to store their data such as documents, images, also can retrieve data whenever they want. there is no surety about security of the data.

Cloud Service Providers (CSP) provide the services to the users and also manage an enterprise infrastructure class that offers a scalable, reliable and secure environment to the users, and requires a very low marginal cost to the sharing nature of resources. It is regular process for users to use cloud storage services to share data with others user. Current system believes that sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage. A unique problem introduced during the process of public auditing for shared data in the cloud is how to preserve identity privacy from the TPA, because the identities of signers on shared data may indicate that a particular user in the group or a special block in shared data is a higher valuable target than others. For example, Ramesh and Krishna work together as a group and share a file in the cloud. The shared file is divided into a number of small blocks, which are independently signed by users. Once a block in this shared file is modified by a user, this user needs to sign the new block using her public/private key pair. The TPA needs to know the identity of the signer on each block in this shared file, so that it is able to audit the integrity of the whole file based on requests from Ramesh orKrishna

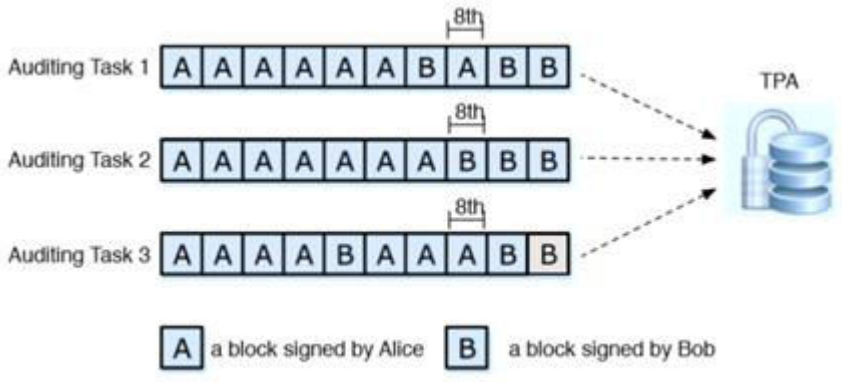

Fig.1. Ramesh and Krishna share a file in the cloud

As shown in Fig. 1, after performing several auditing tasks, some private and sensitive information may reveal to the TPA. On one hand, most of the blocks in shared file are signed by Ramesh, which may indicate that Ramesh is a important role in this group, such as a group leader. On the other hand, the 8-th block is frequently modified by different users. It means this block may contain high value data, such as a final bid in an auction, that Ramesh and Krishna need to discuss and change it several times [1]. Cloud Computing refers to both the applications delivered as

| ISSN: 2395-7852 | www.ijarasem.com | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 8, Issue 3, May 2021 |

services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. In general we heard about the public and private cloud. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public [2].

The authenticity of data can be emerged as a critical issue while storing data on the untrusted servers. The data can move from peer-to-peer storage systems, network file system, web-service object stores, and database systems. These kinds of systems prevents storage servers from mixed kind of representation and modifying data by analysing and providing authenticity to check when accessing the data [3]. The archival storage requires many guarantees about the authenticity of data during the process of storage. During the process of accessing the data it is insufficient to detect and modify the data. Due to the storage, the server retains tremendous amount of data, in which little can be accessed [4]. Since cloud service providers (CSP) are separateadministrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, 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 [5]. We formalize the related notion of ring signature schemes. These are simplified group signature schemes which have only users and no managers(we call such signatures "ring signatures" instead of "group signatures" since rings are geometric regions with uniform periphery and no center). Group signatures are useful when the members want to cooperate, while ring signatures are useful when the members do not want to cooperate. [6].

1.1. Motivation

Cloud computing is a computing model in which resources are provided to the users based on their demand. In cloud computing resources are provided by the cloud service provider known as CSP. Cloud has a number of users which daily uploading the data, user can also share the data with other users. So cloud needs a proper way of maintenance and security. TPA plays a role for maintain and analyzing the cloud properly, so it has motivated as proposed system can try to provide the privacy to all the documents and data and keep it secure from the unauthorized users, also maintain the data integrity in cloud. Proposed system is going to provide security to the data and user can share secured data with team members who are authenticated to access that data.

1.2. Objectives

Current dissertation is dedicated to achieve some of the following objectives.

- To achieve data privacy over the shared cloud environment to maintain confidentiality of user sensitive data.
- To identify &analyze the corrupted block of data in cloud via TPA.
- To implement secured data sharing by using ring signature.
- To build a secure mechanism for accessing shared data from the cloud.
- To implement public auditing scheme for shared data in the cloud, to maintain the integrity of data
-

II. RELATED WORK

Cloud computing is becoming powerful network architecture to perform large- scale and complex computing. Cloud computing is the delivery of computing as a service rather than a product. The idea of providing a centralized computing service dates back to the 1960s, In 1966, Canadian engineer Douglass Parkhill published his book The Challenge of the Computer Utility, in which he describes the idea of computing as a public utility sharing mechanism effectively utilized computing resources and provided acceptable performance to users; however, mainframes were difficult to scale and provision up because of increasingly high hardware costs. Accordingly, users didn't have full control over the performance of mainframe applications because it depended on how many users utilized the mainframe at a given moment. As such, with the introduction of personal computers users loved the idea of having full control of their computing resources, even though these resources are not as effectively utilized [7]. Consider Public auditability in their defined "provable data possession" (PDP) model for ensuring possession of data files on untrusted storages. Their scheme utilizes the RSA based homomorphic linear authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file. However, the public auditability in their scheme demands the linear combination of sampled blocks exposed to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the auditor. [5].

| ISSN: 2395-7852 | www.ijarasem.com | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 8, Issue 3, May 2021 |

2.3 Pitfalls of Existing System

Sr. No.	Paper Title	Authors	Year Of publishing	Methods Used	Limitations
1	Privacy-Preserving Public Auditing for Secure Cloud Storage[5]	Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou,	2013	public auditability	do not consider the privacy protection of users' data against external auditors. Indeed, they may potentially reveal user data information to the auditors.[5]
2	Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud [1]	Boyang Wang, Baochun Li, , and Hui Li,	2014	Homomorphic authenticable signatures, not homomorphic signatures.	Signature schemes do not support blockless verification. Without blockless verification, the TPA has to download the whole data file to verify the correctness of shared data, which takes long verification times.[1]
3	Dynamic Audit Services for Outsourced Storages in Clouds [10]	Devi Parvathy Mohan, K.J.Jagdish	2014	fragment structure, random sampling, and index-hash table (IHT)	It must requires external TPA monitoring. Not Secure [7]
4	Provable data possession for securing the data from untrusted server [3]	S.Karthikeyan , J.praveen And Author Mrs. Sumathy	2015	Provable Data Possession (PDP)	The provable data possession is not capable for the source authentication technique. PDP is restricted form of the memory checking.

III. PROPOSED SYSTEM

The proposed system implementing various auto signature generation techniques over each and every file uploaded or share document by user with privacy preserving over cloud. In this TPA is able to maintain the auditing on the shared data and also check for data integrity without any information about user by using above techniques we can efficiently achieve followings.

(1) Public Auditing: The third party auditor is able to verify the integrity of shared data for a group of users without retrieving the entire data.

(2) Correctness: The third party auditor is able to correctly detect whether there is any corrupted block in shared data.

(3) Enforceability: Only a user in the group can generate valid verification information on shared data.

(4) Identity Privacy: During auditing, the TPA cannot distinguish the identity of the signer on each block in shared data.

| ISSN: 2395-7852 | www.ijarasem.com | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 8, Issue 3, May 2021 |

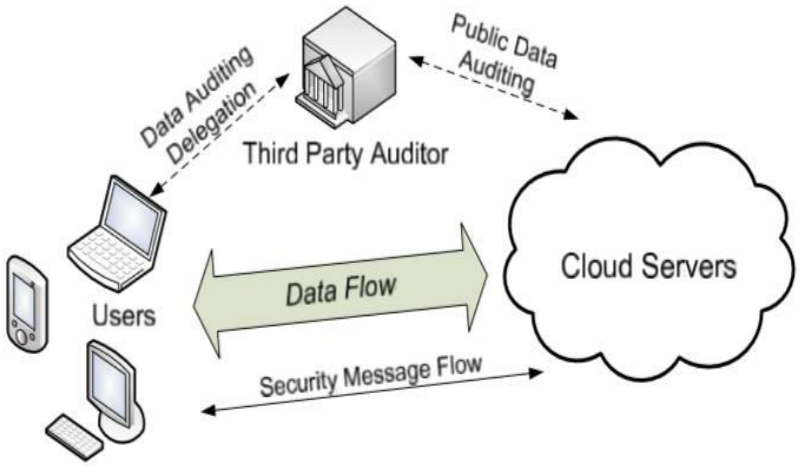

Fig.2. The architecture of cloud data storage system Model [8]

3.1 Plan & Module:

Proposed system has some modules which are as given below:

- **Data Owner:** it is the user which is going to store their data on to the cloud and can share with the group members and access whenever its required.
- **TPA:** TPA (Third Party Auditor) is used to perform the public auditing on cloud based data and check the integrity and confidentiality of the user's data without accessing the entire file of data and generate auditing report for the data owner to know which group member access her file.
- **Cloud:** As we all know cloud is used to store the data in the same way we are going to not only store the data onto the cloud but also preserve the privacy of user's data by using privacy preserving system and user can access that data with specific authentication.

Flow Diagram:

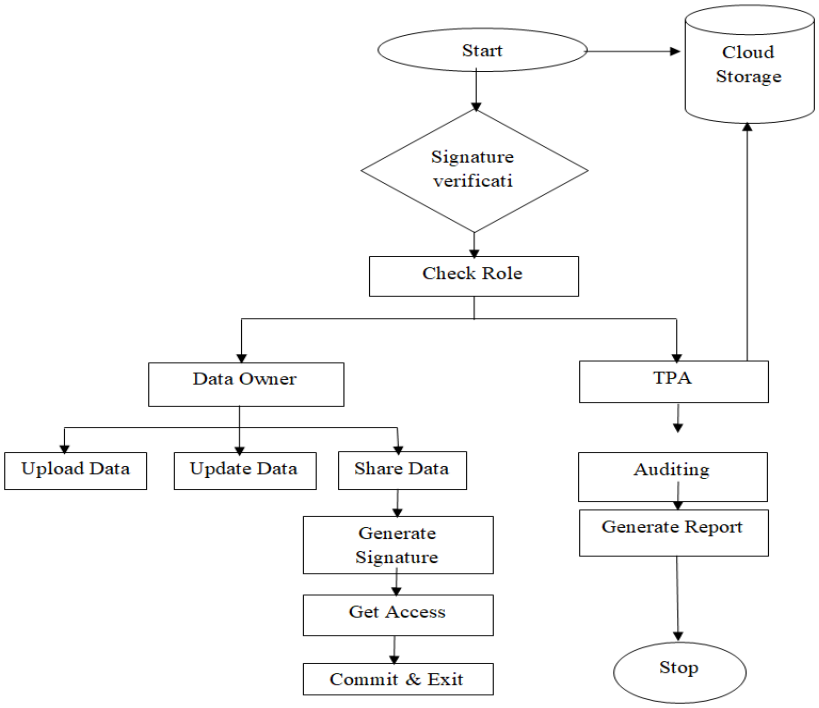

Fig.3. Flow diagram represents working of project

Stepwise working of the Proposed System:

- Data owner login the system with his generated signature and upload the documents on the cloud.

| ISSN: 2395-7852 | www.ijarasem.com | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 8, Issue 3, May 2021 |

- Data owner can also modify the data after uploading the document and can share with other users or group members if he wants to share the data.
- Provide security to the documents with the user signature and documents signature.
- Update signature to the cloud server and by using TPA maintain the privacy of all documents.
- TPA can access only the document information like size, no uses time, modification done by the user if any, last update etc, not the data.
- User can access the document if and only if he has the valid verified signature provided by the data owner.
- Maintain the data integrity and apply privacy preserving on the cloud storage.

Advantages of Proposed System:

- Unauthorized user can't get access to the data
- Authorized user can easily modify, upload, and share their data
- TPA Perform auditing without retrieving the entire copy of data
- It does not reveal the users confidential information
- TPA maintain the data integrity over the cloud

IV.CONCLUSION

Conclusion & Future Scope

Cloud computing provide the storage space and the related services to the user by its own CSP (cloud service provider) and day by day it grows fast and every organization use cloud to store data and access whenever it required, so the cloud is best to manage our data at the remote system.

Future Scope:

In future we can use the cloud storage for storing our data and no need to worry about security issues. As the world grows technically day by day we require more security for the data and in future we can deploy this system for many organizations and maintain privacy of all confidential documents.

REFERENCES

[1] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, "*Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud*", Ieee 5th International Conference On Cloud Computing Year 2014.

[2] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia, "*Above the Clouds: A View of Cloud Computing*".

[3] S.Karthikeyan , J.praveen And Mrs Sumathy, "*Provable data possession for securing the data from untrusted server*", Int. Journal of Engineering Research and Applications, Vol. 5, Issue 3, (Part -2) March 2015.Giuseppe Ateniese, Randal Burns,Reza Curtmola,Joseph Herring, Lea Kissner, Zachary Peterson,Dawn Song, "*Provable Data Possession at Untrusted Stores*", CCS'07, October 29–November 2, 2007, Alexandria, Virginia, USA. Copyright 2007 ACM.

[4] Giuseppe Ateniese, Randal Burns,Reza Curtmola,Joseph Herring, Lea Kissner, Zachary Peterson,Dawn Song, "*Provable Data Possession at Untrusted Stores*", CCS'07, October 29–November 2, 2007, Alexandria, Virginia, USA. Copyright 2007 ACM.

[5] Cong Wang, Sherman S.-M. Chow, Qian Wang,Kui Ren,and Wenjing Lou,"*Privacy-Preserving Public Auditing for Secure Cloud Storage*".

[6] Ronald L. Rivest, Adi Shamir, and Yael Tauman, "*How to Leak a Secret*".

[7] Devi Parvathy Mohan, K.J.Jagdish, "*Dynamic Audit Services for Outsourced Storages in Clouds*", International Journal of scientific research and management(IJSRM), Volume 2, Issue6, 2014.

[8] Swapnil More,Sangita Chaudhari, "Third Party Public Auditing Scheme for Cloud Storage", Procedia Computer Science7 79 (2016) 69-76.

[9] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "*Privacy-Preserving Public Auditing for Secure Cloud Storage*", A preliminary version [1] of this paper was presented at the 29th IEEE Conference on Computer Communications (INFOCOM'10).

[10] Rampal Singh, Sawan Kumar, Shani Kumar Agrahari, "*Ensuring Data Storage Security in Cloud Computing*", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 3 March 2013.

[11] Kedar Jayesh Rasal, Dr. S.V.Gumaste, Sandip A. Kahate, "Survey on Privacy Preserving Public Auditing Techniques for Shared Data in the Cloud", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 4, Issue 3, May 2015.