Public Auditability Services for Outsourced Storages in Clouds using Third Party Auditor

Lavanya B C
PG Student: Dept of CS&E
Acharya Institute of Technology
Bangalore, India

P V Kumar
Professor: Dept of CS&E
Acharya Institute of Technology
Bangalore, India

Ravikumar G K
Principle Consultant
Wipro Technology
Bangalore, India

Abstract— Outsourcing the data on the cloud relieves burden of the client for maintenance and storage management by offering a scalable, location independent platform and comparably low cost. To enable public auditability for the outsourced storages in cloud, the data owner resorts to a Third Party Auditor for checking the integrity of the data on the cloud. TPA checks for the integrity of the data without demanding the local copy of data, and provides no online burden to the Data Owner. An efficient Interactive Proof of Retrievability Scheme is used for providing Public Audit Services for checking the integrity for the outsourced data in the cloud.

Keywords— Public Auditability, Audit Service, Cloud Storage, TPA, IPOR;

I. INTRODUCTION

A. Introduction to Cloud Computing and Third Party Auditor (TPA)

Cloud: cloud is a large-scale of distributed computing paradigm that is driven by economies of scale, in which a pool of virtualized, dynamically-scalable, abstracted, managed computing power, storage, platforms and services are delivered on demand to end user's over the Internet [1].

Cloud Computing: Cloud computing can be defined as the use of computing resources (Software and Hardware) that are delivered as a service over a network (typically over the Internet).
Cloud computing is one of the platform for providing On-Demand network access to a shared pool of configurable computing resources (e.g., storage, servers ,networks, services and applications) that can be rapidly provisioned and released with minimal service provider interaction or management effort [1].

*Third Party Auditor (TPA) for Public Auditing***:** Auditing can be defined as periodically verifying the integrity of the outsourced data by the Trusted Third Party. Public Auditing can be achieved using Third Party Auditor (TPA).Third Party Auditor (TPA) is a kind of Auditor (Verifier).There are two types of Auditability namely:

*1) Public Auditability***:** In this scheme, to ensure data integrity for the outsourced data, the TPA or the Trusted Person is involved for the verification of the data.TPA is a Third Party between the Data Owner (DO) and the Cloud Service Provider (CSP).Here the end user's are not responsible for verifying the integrity of the outsourced data. Public Auditing scheme allows anyone, not only the Data Owner (DO) or the client, for verifying the integrity of the outsourced data. To reduce the risk of storage management of the data of the Data Owner, TPA is mainly used for Auditing the clients data.TPA removes the involvement of the client by Auditing that whether the data which is stored in the cloud server are intact, which is very much important in achieving the economies of scale for cloud computing.
The periodic audit report helps the data owner's (DO) to effectively evaluate the risk's of the outsourced data in the cloud server and it is also useful to the Cloud Service Provider (CSP) to enhance their cloud based service platforms [2].TPA thus helps the Data Owner's (DO) to make sure that their data which is stored on the cloud server are safe and less burden to the Data Owner (DO) and the management of the data will be easy.

*2) Private Auditability***:** In this scheme, the end user is completely responsible for verifying the integrity of their data. Here there is no involvement of the Third Party Auditor (TPA) for verifying the integrity of the outsourced data.
The main disadvantage of Private Auditability scheme is that, first the end user's have to download the entire file for checking the integrity of the outsourced data. But if the data or the file which is stored on the cloud server is huge, then it takes too long time to download the entire file. Another disadvantage of this approach is that periodic verification to detect the errors at regular intervals of time is not supported.

B. Security Issues in Outsourcing the Data

The important security issues for outsourcing the data on the cloud are:

- *Data Integrity Verification at Un-Trusted Servers:* The attacker's by using the cloud's IP Address may modify the content of the data. The Cloud Service Provider (CSP) for the benefit of data possession he may behave unfaithfully towards the end user's. As a result the end user's will lose faith on the Cloud Service Provider (CSP) [3].

- *Data Accessed by Un-Authorised User's:*
  By encrypting the data before outsourcing to the remote server's the confidentiality feature is guaranteed by the Data Owner (DO).Provable Data Possession (PDP) technique is used for verifying the integrity of the outsourced data to validate the effectiveness of data which is stored at the remote sites [3].

- *Location Independent Services:*
  One of the important characteristics of cloud computing is that, the ability to provide the services to the client's irrespective of the location of the Cloud Service Provider (CSP) [3].

- *Infrastructure and Security:*
  To avoid the potential security threats the infrastructure used for providing the services should be secured appropriately [3].

- *Data Recovery or Backup:*
  The users must consider the security as well as bandwidth issues for achieving data recovery in cloud [3].

II. EXISTING SYSTEM AND ITS LIMITATIONS

Traditional cryptographic technologies for data availability and integrity ,based on signature schemes and hash functions cannot work on the outsourced data without a local copy of the data [4], [5], [6].Further it is not a good solution for data validation by downloading them due to the expensive communication cost especially for large-sized files. Also, the ability to audit the intactness of the data in a cloud environment can be expensive and infeasible for the cloud users. Therefore it is very important to adopt public auditability for cloud storage service (CSS), so that the data owner's may request to a Third Party Auditor (TPA), who has expertise knowledge that a common user does not have for periodically auditing the outsourced data.

Xie et al. [7] proposed an efficient method on content comparability for the outsourced database, but it was not suitable for irregular data. Wang et al. [8] also proposed a similar architecture for public audit services. For example, in this scheme, an outsourced file is split into n blocks, and for each block a verification tag was generated. To maintain security in this scheme, the length of the block must be equal to the size of the cryptosystem, i.e., 160 bits which are 20 bytes. This means that 1M byte file is split into 50,000 blocks and 50,000 tags [9] were generated, and the number of tags increases as the number of blocks was increased. Therefore, it is not efficient to build an audit system based on this scheme. To address this problem fragment structure is introduced, to improve the system performance and to reduce the extra storage.

Another main problem is the security issue of dynamic data operations for public audit services. In clouds, providing dynamic scalability is one of the core design principles. This means that the outsourced data may not only be accessed by the client's, but also dynamically updated by them through the block operations such as insertion, deletion, and modification. But these operations introduces security issues in most of the existing schemes, e.g., the forgery of the verification meta data generated by the data owner's and the leakage of the user's secret key.

To implement public auditability, Provable Data Possession (PDP) [10] and Proof Of Retrievability (POR) [11] are proposed.PDP and POR approaches are based on Probabilistic Proof technique for the storage provider to prove the client's data to remain intact. These PDP/POR schemes work on a publicly verifiable way, so that anyone can use the verification protocol to prove the availability of the outsourced data. Hence these schemes help to accommodate the requirements from public auditability. POR/PDP schemes evolved around an un-trusted storage, provides a publicly accessible remote interface to check the large amount of data.

III. PROPOSED SYSTEM AND ITS ADVANTAGES

Audit system architecture for outsourced data in clouds is as shown in Fig.1 [12].In this architecture the data storage service involves four modules:

- *Data Owner (DO)*: Data Owner contains large amounts of data to be stored in the cloud server.

- *Cloud Service Provider (CSP)*: CSP provides data storage service and has enough computation resources and storage space.

- *Third Party Auditor (TPA*): TPA is responsible to manage or monitor the outsourced data under the delegation of data owner. The TPA is independent and reliable through the following audit functions:
  - TPA should perform regular checks on the availability and integrity of the outsourced data at appropriate intervals.
  - TPA should be able to maintain, organize, and manage the outsourced data instead of data owners.
  - TPA should support dynamic data operations such as insertion, deletion and modifications for authorized applications.
  - TPA should be able to take the evidences for disputes about the inconsistency of data in terms of authentic records for all data operations [12].

- *Authorized Applications (AA)*: Only the Authorised Applications have the rights to access and manipulate the stored data. Finally, application users can enjoy various cloud application services via these authorized applications.

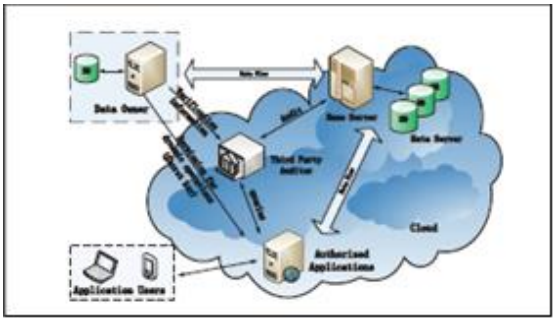

Fig. 1 Audit System Architecture

The use case diagram [13] shown in Fig.2, explains the functionality of the Audit services by TPA for the data integrity in cloud system, in which TPA verifies the data as an agent of the Data Owner (DO).

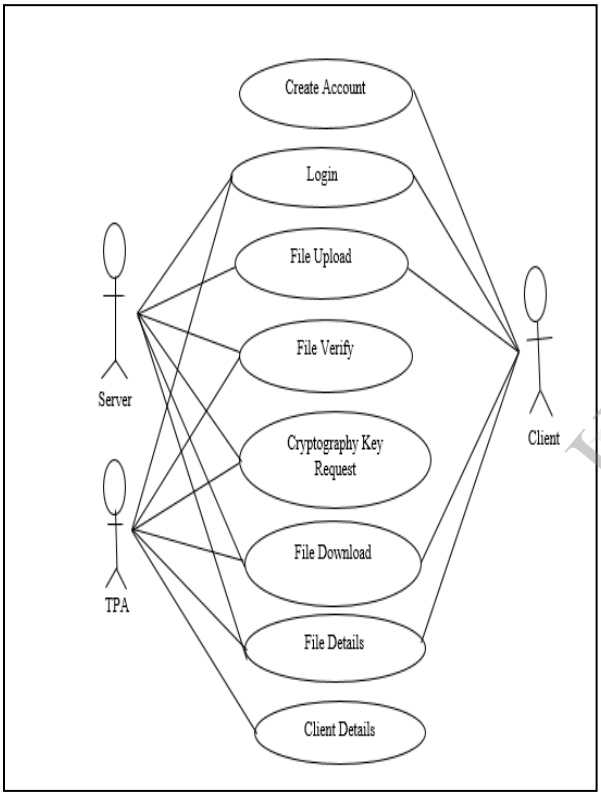

Fig. 2 Use Case Diagram of Public Audit Service by using TPA for Data Integrity in Cloud System

A. *Advantages of the Proposed System*

1) Public Auditability: Public Auditability allows the Third Party Auditor (TPA) to verify the correctness of cloud data on demand under the delegation of data owner without retrieving a copy of the whole data or introducing additional on-line burden to cloud services [12].

2) Dynamic Operations: Dynamic data operations such as insertion, deletion, and modifications are performed by the Authorised Applications by receiving the secret key from the Data Owner (DO), upon receiving the request from the Data Owner [12].

3) Timely Detection: To detect data errors or losses in the outsourced storage, as well as anomalous behaviours of data operations in a timely manner [12].

4) Effective Forensic: To make the TPA to perform strict auditing and supervision for outsourced data, and to report effective evidences for anomalies [12].

5) Lightweight: To allow the TPA to perform auditing tasks with lower communication cost, minimum storage and less computation overhead [12].

IV. DESIRABLE PROPERTIES FOR PUBLIC AUDITING

To enable Public Audit for cloud data storage is the main objective of this paper. Therefore, the entire Audit service architecture design should not only be cryptographically strong, but also it should be more practical from a systematic point of view. To satisfy the design principles some of the desirable properties for public auditing are listed below [14]:

1) Minimize Auditing Overhead: First and foremost, the overhead imposed by the auditing process on the cloud server should not outweigh its benefits. Such overhead includes both the bandwidth cost for data transfer and the I/O cost for data access. Any online burden on a data owner should be also being as low as possible. The data owner should just enjoy the cloud storage service after the audit delegation process. The data owner should be worry free after storing the data on to the cloud server, since the auditing process will be done by the Third Party Auditor (TPA).

2) Protect Data Privacy: One of the important aspects of a Service Level Agreement (SLA) is to provide data privacy protection for the outsourced data on the cloud. Therefore, the implementation of a public auditing protocol should help in achieving the owner's data privacy. That is, TPA should be able to audit outsourced data without retrieving a local copy of the data.

3) Support Data Dynamics: Since the Cloud Storage Service (CSS) is not just a data warehouse, the Authorized Applications (AA) should perform dynamic data operations such as insertion, deletion and modifications. The audit protocol design should include this important feature of data dynamics in Cloud Computing.

4) *Support Batch Auditing*: When multiple auditing tasks are received from different data owner's delegations, TPA must be able to handle such delegations in a fast yet cost-effective manner. This feature enables the scalability of a public Auditing service even with a multiple number of data owners.

V. INTERACTIVE AUDIT PROTOCOL (IPOR) FOR PUBLIC AUDITING

An efficient Interactive Proof of Retrievability (IPOR) Scheme is used for providing Public Audit Services for

checking the integrity for the outsourced data in the cloud. In this scheme, every client holds the secret key *sk*, which may be used for generating the tags of many files [12].IPOR is a public Auditing scheme for cloud storage which can be defined through three algorithms: KeyGen, TagGen, and Proof which works as follows:

1) KeyGen (1λ): When given a security parameter λ as an input, this randomized algorithm generates public verification parameters and cloud users public/private key pair (pk, sk).

2) TagGen (sk, F): This randomized algorithm takes users secret key sk and data file F as inputs, and produces the authentication tags t, which contains the information on the file being stored and additional secret information encrypted under the secret key sk. The file F and tag t will be stored in the cloud server.

3) Proof (CSP, TPA): It is a 3-move protocol between the Prover (CSP) and Verifier (TPA): Commitment, Challenge and Response which is as shown in Fig. 3 [12].

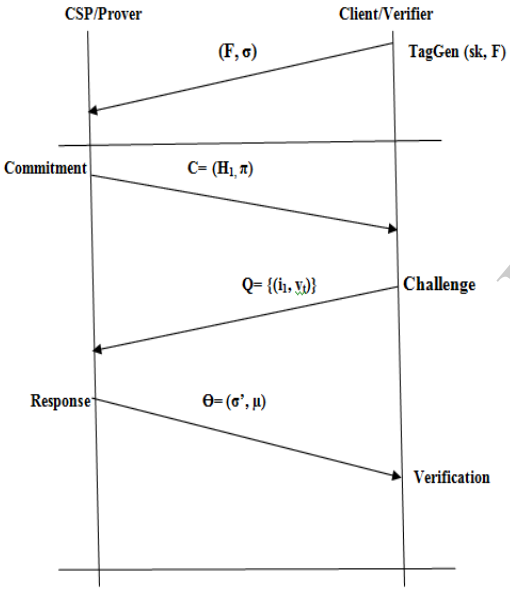

Fig. 3 Three Move Operations of IPOR Protocol

This scheme is constructed based on the standard model of Interactive Proof System which can ensure the confidentiality of secret data i.e. Zero-Knowledge Property and an undecidability of invalid Tags i.e., Soundness Property. Zero-Knowledge Property prevents the leakage of the verified data and Soundness Property prevents the Fraud users.

VI. PERFORMANCE EVALUATION

To reduce the workload on the cloud server, TPA issues a random sampling challenge at regular intervals of time to detect the misbehaviors of the cloud service provider (CSP).To detect the errors in a timely manner the detection probability P is a very important parameter.The detection probability [12] is:

$$P = 1 - \left(n - \frac{e}{n}\right)t = 1 - (1 - \rho b)t$$

Hence the number of queried blocks is:

$$t = \frac{\log(1 - P)}{\log(1 - \rho b)}$$

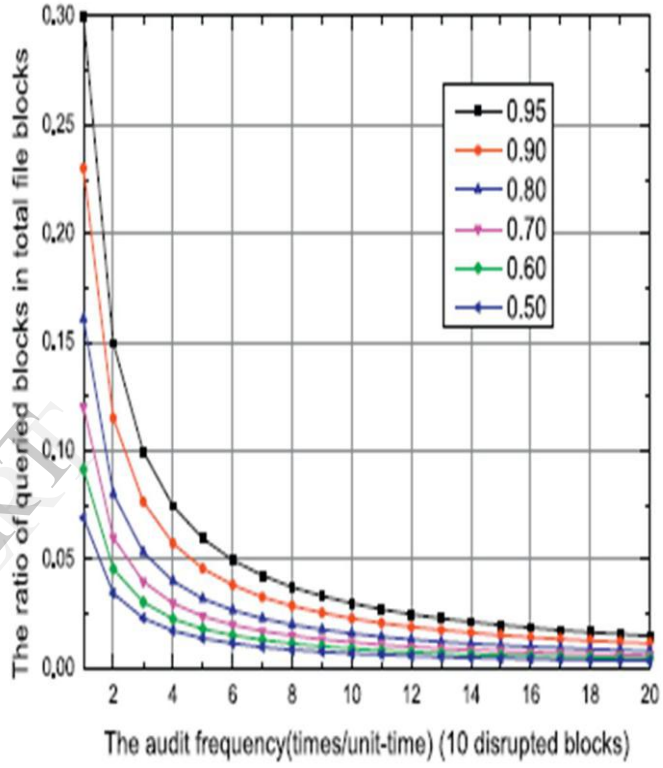

Fig. 4 Ratio of Queried Blocks in Total File Blocks Under Different Audit Frequency [12]

VII. CONCLUSION

In Private Auditing Scheme the end user is completely responsible for verifying the integrity of the outsourced data on the cloud server. Here the end user's have to download the entire content of the data from the cloud server and then they have to check for the integrity of the data. But if the content of the data which is stored on the cloud server if it is too large then it takes very long time to download the data from the cloud server. To overcome this problem public Auditing scheme is used.

In public Auditing the end user is not responsible for verifying the integrity of the data which is stored on the cloud. Instead Third Party Auditor (TPA) is used for checking the correctness of the data. Third Party Auditor (TPA) is a trusted third party between the Data Owner and Cloud Service Provider (CSP) is employed for providing Public Audit services for the outsourced data on the cloud. In Public Auditing, Third Party Auditor (TPA) verifies the integrity of

the outsourced data on the cloud under the delegation of the Data Owner (DO) so that the data owner burden is reduced. Public Auditing supports dynamic data operations such as insertion, deletion and modification and it also supports timely anomaly detection by issuing a random sampling challenge by the TPA. Public Auditing scheme checks for the integrity of the outsourced data without downloading the raw data from the cloud server.

An Interactive Audit Protocol known as Interactive Proof of Retrievability (IPOR) is used for performing public Audition. It is a protocol which is introduced between the TPA and CSP. It is a 3 move protocol i.e., Commitment, Challenge and Response. IPOR scheme not only supports complete privacy protection and dynamic data operations, but also enables significant savings in communication and computation cost, as well as high detection probability of disrupted blocks.

REFERENCES

[1] Y. Tharam Dillon, Chen Wu and Elizabeth Chang,"Cloud Computing Issues and challenges", 24th *IEEE International Conference on Advanced Information Networking and Applications*, 2010

[2] G.Ateniese et al.,-Provable Data Possession at Untrusted Stores, *proc*.ACM CCS=07, Oct.2007.PP.598-609.

[3] Rakhi Bharadwaj, and Vikas Maral, "Dynamic Data Storage Auditing Services in Cloud Computing", *International Journal of Engineering and Advanced Technology (IJEAT)*, ISSN2249-8958, Volume-2, Issue-4, April-2013.

[4] H.-C. Hsiao, Y.-H.Lin, A.Studer, K.-H.Wang, H.Kikuchi A.Perrig, H.-M.Sun, and B.-Y.Yang**,**"A Study of User-Friendly hash comparison schemes", in *ACSAC*, 2009, PP.105-114.

[5] A.R.Yumerefendi and J.S.Chase, "Strong Accountability for Network Storage", in *FAST.USENIX*, 2007, PP.77-92.

[6] Y.Zhu, H.Wang, Z.Hu,G.-J.Ahn, H.Hu, and S.S.Yau, "Efficient Provable Data Possession for Hybrid Clouds", in *Proceedings of the 17th ACM Conference on Computer and Communication Security*, New York, NY, USA: ACM, 2010, PP.756-758.

[7] M.Xie, H.Wang, J.Yin, and X.Meng, "Integrating Auditing of Outsourced Data", in VLDB, 2007, PP.782-793.

[8] C.Wang, Q.Wang, K.Ren, and W.Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", INFOCOM, 2010 *Proceedings IEEE*, 14-19 2010, PP.14-22, 2009.

[9] H.Shacham and B.Waters, "Compact Proofs of Retrievability", in Advances in Cryptography ASIACRYPT 2008, ser.Lecture Notes in Computer Science, J.Pieprzyk, Ed., Vol.5350.Springer, 2008, PP.90-107.

[10] G.Ateniese, R.C.Burns, R.Curtmola, J.Herring, L.Kissner, Z.N.J.Peterson, and D.X.Song, "Provable Data Possession", in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, 2007, PP.598-609.

[11] A. Jules and B.S.K.Jr., "Pors: Proofs of Retrievability for Large Files", *in Proceedings of the 2007 ACM Conference on Computer and Communication Security*, CCS 2007, 2007, PP.598-609.

[12] Yan Zhu, Gail-Joon Ahn, "Dynamic Audit Services for Outsourced Storages in Clouds*",IEEE Transactions on Services Computing and Cloud Computing*, Volume:6,Issue:2,Issue Date: April-June 2013.

[13] Shingare Vidya Marshal, "Secure Audit Services by using TPA for Data Integrity in Cloud System", *International Journal of Innovative Technology and Exploring Engineering (IJITEE)"*, ISSN: 2278-3075, Volume-3, Issue-4, and September 2013.

[14] Cong Wang and Kui Ren, "Towards Publicly Auditable Secure Cloud Data Storage Services", *IEEE Transactions*, July-August 2010.