A Novel Approach for Public Data with Proficient User Revocation in the Cloud

Guguloth Vinoda
PG Scholar,
Department of CSE,
Brilliant Institute of Engineering and Technology, Hayathnagar.

P.Lakshmi
Assistant Professor,
Department of CSE,
Brilliant Institute of Engineering and Technology, Hayathnagar.

Adapa Gopi
HOD,
Department of CSE,
Brilliant Institute of Engineering and Technology, Hayathnagar.

Abstract:

In today’s computing world, cloud computing is one of the biggest innovations that utilize advanced computational power and improve data sharing and data storing capabilities. The main challenge in cloud computing was issues of data integrity, data privacy, and data accessibility by unauthorized users. TTA (Trusted Third Party) is used to store and share data in cloud computing. Modification and sharing of data are quite simple as a group. To verify integrity of the Publicdata, members in the group need to compute signatures on all Publicdata blocks. Different blocks in Publicdata are generally signed by different users due to data modifications performed by different users. User revocation is one of the biggest security threats in data sharing in groups.

During user revocation, Publicdata block signed by revoked user needs to be downloaded and re-signed by existing users. This task is very inefficient because of the large size of Publicdata blocks on cloud. PANDA Plus is the new public auditing mechanism for maintaining the integrity of Publicdata with proficient user revocation in the cloud. This mechanism is based on proxy re-signatures concept, which allows the cloud to re-sign blocks on behalf of existing users during user revocation, so that downloading of Publicdata blocks is not required. PANDA Plus is the public auditor which audits the integrity of Publicdata without retrieving the entire data from the cloud. It also monitors batch to verify multiple auditing tasks simultaneously.

Keywords:

Cloud computing, Data integrity, Public auditing, User revocation

I. INTRODUCTION:

[A] Cloud Computing:

Cloud computing is nothing but Internet-based computing which made revolution in today’s world. It is the biggest innovation that uses advanced computational power and improves data sharing and data storing capabilities. Cloud is a large group of interconnected computers, which is a major change in how we store information and run applications. Cloud computing is a Publicpool of configurable computing resources, on-demand network access and provisioned by the service provider[1]. The advantage of cloud is cost savings. The prime disadvantage is security. The cloud computing security contains a set of policies, technology & controls deployed to protect data, application & the associated infrastructure of cloud computing. Some security and privacy issues that need to be considered. The only thing was the cloud computing lacks regarding the issues of data integrity, data privacy, and data accessed by unauthorized members.

[B] Data Integrity:

Integrity is nothing but consistency. It is a major factor that affects the performance of the cloud. Data integrity contains protocols for writing of the data in a reliable manner to the persistent data storages which can be retrieved in the same format without any changes later. Maintaining integrity of Publicdata is quite difficult task. Numbers of mechanisms have been proposed [2]-[15] to protect integrity of data. Concept of attaching Signature to each block of data is used in these mechanisms. Data Integrity is most important of all the security issues in cloud data storages as it ensures completeness of data as well as that the data is correct, accessible, consistent and of high quality.
Data model consists of three types of integrity constraints:

- Entity integrity
- Referential integrity
- Domain integrity

**[C] Public Data Auditing in Cloud:**

On cloud, we can store data as a group and share it or modify it within a group. In cloud data storage contains two entities as cloud user (group members) and cloud service provider/cloud server. A cloud user is a person who stores large amounts of data on a cloud server managed by the cloud service provider. A cloud service provider will provide services to cloud users. The major issue in cloud data storage is to obtain correctness and integrity of data stored on the cloud.

Cloud Service Provider (CSP) has to provide some form of mechanism through which a user will get the confirmation that cloud data is secure or is stored as it is. No data loss or modification is done by unauthenticated members. To achieve security in data auditing concept is coming into picture. This can be achieved in two ways as without trusted third party or with trusted third party. Trusted third party based on who does the verification. In cloud computing architecture data is stored centrally and managing this centralised data and providing security to it is very difficult. TPA (Third Party Auditor) is used in this situation. The reliability is increased as data is handled by TPA but data integrity is not achieved. TPA uses encryption to encrypt the contents of the file. It checks data integrity but there is threat of TPA itself leaking user’s data.

Researchers of [3] specify a way to achieve storage correctness without Trusted Third Party (TTP). They achieve this by using secure key management, flexible access right management, and light-weight integrity verification process for checking an unauthorised change in the original data without requesting a local copy of the data.

**II. LITERATURE REVIEW:**

**[A] Techniques used in Public Auditing on Cloud:**

There are some different techniques which are used in different auditing mechanisms. This section introduces some of these techniques like MAC, HLA etc. which are used for different purposes like data authentication, data integrity in auditing schemes on cloud.

1. **MAC Based Solution:**

   This technique is used for data authentication. In this mechanism, users upload data blocks with MAC and the Cloud provider provides secret key SK to TPA. Here, TPA’s task is to retrieve data blocks randomly and MAC uses SK to check correctness of data. Limitations of this technique are: Online burden to users due to limited use (i.e., bounded usage) and stateful verification. Complexity in communication and computation is high as TPA states are difficult to maintain. Users need to recompute MAC and re-publish it on CS. This technique only supports static data.

2. **HLA Based Solution:**

   This technique performs auditing without retrieving data blocks. HLA is nothing but unforgettable verification meta-data that should be authenticated. It checks integrity of data block by authenticating it in linear combination of individual blocks. This technique allows proficient data auditing and consumes only constant bandwidth, but its time-consuming as it uses linear combinations for authentication.

3. **Using Virtual Machine:**

   Abhishek Mohta proposed Virtual machines concept which is useful in case of Software as a Service (SaaS) model of the cloud computing.
In this mechanism as shown in Fig when user request CSP for service CSP authenticate the client and provide a virtual machine by means of Software as a service. Virtual Machine (VM) uses RSA algorithm for cryptography, where client encrypt and de-crypt the file. A SHA-512 algorithm is also used for making the message digest and check the integrity of data. This also helps in avoiding unauthorised access and providing privacy and consistency. Limitation to this technique is it is useful only for SaaS model.

Fig. 2 Architecture of Cloud Data Storage Service using Virtual Machine.

4. Using EAP:

As mentioned by S. Marium Extensible authentication protocol (EAP) can also use through three ways hand shake with RSA. Using EAP they proposed identity based signature for hierarchical architecture. They provide an authentication protocol for cloud computing (APCC) [4]. As compare to SSL authentication protocol APCC is more lightweight and proficient. It also used Challenge – hand shake authentication protocol (CHAP) for authentication.

The steps are as follows:

1)When Client request for any service to cloud service provider, SPA send a CHAP request / challenge to the client.

2)The Client sends CHAP response/ challenges which is calculated by using a hash function to SPA

3)SPA checks the challenge value with its own calculated value. If they are matched then SPA sends CHAP success message to the client.

5. Using Automatic Protocol Blocker:

Balkrishna proposed proficient Automatic Protocol Blocker technique for error correction which checks data storage correctness [4]. Kiran Kumar proposed automatic protocol blocker to avoid unauthorized access [5]. When an unauthorized user access user data, a small application runs which monitors user inputs, it matches the user input, if it is matched then it allow user to access the data otherwise it will block protocol automatically. It contains five algorithms as keygen, SinGen, GenProof, VerifyProof, Protocol Verifier. Protocol Verifier is used by CS. It contains three phases as Setup, Audit and Pblock.

6. Random Masking Technique:

Jachak K. B. proposed privacy preserving Third party auditing without data encryption. It uses a linear combination of sampled block in the server’s response is masked with randomly generated by a pseudo random function (PRF) [7].

[B] Different Public auditing mechanisms on Cloud:

This section consist different mechanisms, different system proposed by authors which are used for auditing in cloud computing.

1. Compact Proofs of Retrievability Hovav Shacham and Brent Watersy[9] proposed proof-of-retrievability system. In this system, data storage center must prove to a verifier that he is actually storing all of a client’s data. They have proposed two homomorphic authenticators the first, based on PRFs, gives a proof-of-retrievability scheme secure in the standard model. The second, based on BLS signatures [8], gives a proof-of-retrievability scheme with public variability secure in the random oracle model. Frameworks explained by them allow to argue about the systems unforgeability, extractability, and retrievability with these three parts based respectively on cryptographic, combinatorial, and coding-theoretical techniques.

2. Provable Data Possession at Untrusted Stores Giuseppe Ateniese et all introduce a model which based on provable data possession (PDP)[10].
This is used for verifying that server is processing the original data without retrieving it. In this model probabilistic proof of possession is generated by sampling random sets of blocks from the server. This helps to reduce I/O cost.

As shown in Fig. 3 client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. DP model for remote data checking supports large data sets in widely-distributed storage systems. A key component of this mechanism is the homomorphic verifiable tags.

3. Privacy Preserving Public Auditing Cong Wang Proposed Privacy Preserving Public Auditing technique [11]. In this technique public auditing allows TPA along with user to check the integrity of the outsourced data stored on a cloud & Privacy Preserving allows TPA to do auditing without requesting data. Here TPA can audit the data by maintaining cloud data privacy. They have used the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the proficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also prevent the users from fear of the outsourced data leakage.

This mechanism is based on 4 algorithms:

**Keygen:** It is a key generation algorithm for setup the scheme.

**Singen:** It is used by the user to generate verification metadata which may consist of digital signature.

**GenProof:** It is used by CS to generate a proof of data storage correctness.

**VerifyProof:** Used by TPA to audit the proofs

4. LT Codes-based Secure and Reliable Cloud Storage Service Ning Cao et al. explore the problem of secure and reliable cloud storage with the efficiency consideration of both data repair and data retrieval, and design a LT codes-based cloud storage service (LTCS) [12]. LTCS provides proficient data retrieval for data users by utilizing the fast Belief Propagation decoding algorithm, and releases the data owner from the burden of being online by enabling public data integrity check and employing exact repair. LTCS is much faster data retrieval than the erasure codes-based solutions. It introduces less storage cost, much faster data retrieval, and comparable communication cost comparing to network coding-based storage services.

5. Oruta: Privacy-Preserving Public Auditing for Public-Data in the Cloud Boyang Wang et al. propose Oruta, the first privacy preserving public auditing mechanism for Publicdata in the cloud in [13]. They have used ring signatures to construct homomorphic authenticators, so the TPA is able to audit the integrity of Publicdata, without retrieving the entire data. They have used HARS and its properties for constructing Oruta.

**III. CONCLUSIONS:**

Cloud computing is world’s biggest innovation which uses advanced computational power and improves data sharing and data storing capabilities. It increases the ease of usage by giving access through any kind of internet connection. As every coin has two sides it also has some drawbacks. Privacy security is a main issue for cloud storage. To ensure that the risks of privacy have been mitigated a variety of techniques that may be used in order to achieve privacy.

This paper showcase some privacy techniques and different methods for overcoming the issues in privacy on untrusted data stores in cloud computing. There are still some approaches which are not covered in this paper. This paper categorizes the methodologies in the literature as encryption based methods, access control based mechanisms, query integrity/keyword search schemes, and auditability schemes.
Even though there are many techniques in the literature for considering the concerns in privacy, no approach is highly developed to give a privacy-preserving storage that overcomes all the other privacy concerns. Thus to handle all these privacy concerns, we need to develop privacy-preserving framework which handle all the worries in privacy security and strengthen cloud storage services.

REFERENCES


