International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Summary on Deduplicatable Dynamic Proof of Storage for Multi-User Environments

Megha T P[1], Poornima B G[2]

[1]*Student, Dept. of CSE, Vidyavardhaka college, Karnataka, India*
[2]*Associate Professor, Dept. of CSE, Vidyavardhaka college, Karnataka, India*

Abstract - *The most prevalent cloud benefit is information stockpiling. To save the security of record, documents are frequently put away in cloud in an encoded shape. Dynamic Proof of Storage (PoS) is a valuable cryptographic crude which empowers client to check respectability of record. There are numerous dynamic PoS plots in single client situations. The issue of multiuser condition as been overcome in this paper. A reasonable multi-client distributed storage framework needs the safe customer side cross-client deduplication procedure, which enables a client to skirt the transferring procedure and acquire the responsibility for records specifically, when different proprietors of similar documents have transferred them to the cloud server. In this paper, the idea of deduplicatable dynamic confirmation of capacity is presented and propose a proficient development called DeyPoS, to accomplish dynamic PoS and secure cross-client deduplication.*

Key Words: **Cloud Storage, deduplication, dynamic proof of storage, Multiuser, Cross-user.**

1. INTRODUCTION

Information is a gathering of huge informational collections. Storage outsourcing is winding up increasingly appealing to both industry and the scholarly world because of the benefits of minimal effort, high openness, and simple sharing. One of the storage outsourcing shapes is cloud storage which picks up wide consideration as of from years.

Data integrity is a standout amongst the most essential properties when a client outsources its records to distributed storage. Clients ought to be persuaded that the documents put away in the server are not altered. Conventional procedures for securing information uprightness, for example, message confirmation codes (MACs) and computerized marks, expect clients to download the greater part of the documents from the cloud server for check, which brings about a substantial correspondence cost . These strategies are not appropriate for distributed storage administrations where clients may check the uprightness much of the time, for example, consistently . Along these lines, analysts presented Proof of Storage (PoS) for checking the integrity without downloading documents from the cloud server.

In any case, dynamic PoS stays to be enhanced in a multi-client condition, because of the necessity of cross-client deduplication on the customer side. This shows clients can avoid the transferring procedure and acquire the responsibility for quickly, as long as the transferred records as of now exist in the cloud server. This method can decrease storage room for the cloud server, and spare transmission transfer speed for clients.

1.1 Existing System

- In most of the existing dynamic PoSs, a label utilized for trustworthiness confirmation is produced by the secret key of the uploader. Hence, different proprietors who have the responsibility for files however have not transferred it because of the cross-client deduplication on the customer side, can't produce another label when they refresh the file. In this circumstance, the dynamic PoSs would fail.
- Halevi *et al.* introduced the concept of proof of ownership, as a solution of cross-user deduplication on the client-side.
- Pietro et al. proposed another proof of ownership scheme for improving the efficiency.
- Xu *et al.* proposed scheme as client side deduplication for encrypted data.

Disadvantages:

- ✓ Multi-user environment is not supported by existing POSs.
- ✓ Due to problem of private tag generation and structure diversity, existing system cannot be extended to dynamic PoS.
- ✓ Schemes cannot support deduplication due to private tag generation and structure diversity.

1.2 Proposed System

- Homomorphic Authenticated Tree (HAT) is designed, to reduce the communication cost in both the deduplication phase and the proof of storage phase with similar computation cost.
- HAT can support cross-user deduplication, dynamic operations integrity verification, and with good consistency.
- Deduplicatable dynamic Proof of Storage (deduplicatable dynamic PoS) is proposed, solves

the private tag generation and structure diversity challenges.

- Deduplicatable dynamic PoS called Dey-PoS is proposed, which supports unlimited number of update operations and verification.

Advantages:

- ✓ It is an efficient authenticated structure.
- ✓ DeyPoS provides security in the random oracle model.
- ✓ The hypothetical and test comes about demonstrate that DeyPoS execution is productive.
- ✓ Performs better when the file size and the number of the challenged blocks are large.

2. RELATED WORK

1. Cryptographic cloud storage

S. Kamara et.al [1] proposed "Cryptographic cloud storage". They considered the problem of building a secure cloud storage service on top of a public cloud infrastructure, where service provider is not trusted completely by the customer. They described several architectures that combine recent and non-standard cryptographic primitives in order to achieve goal. This new economic and computing model is commonly referred to as cloud computing. This includes various types of services such as: infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS).

2. A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data

Z. Xia et.al [2] proposed "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data". More data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. Sensitive data should be encrypted before outsourcing for privacy requirements. A secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents.

3. Secure and efficient proof of storage with deduplication

Q. Zheng et.al [3] proposed "Secure and efficient proof of storage with deduplication". For the success of cloud storage both security and efficiency are critical. Proof of Data Possession (PDP) and Proof of Retrievability (POR) was proposed for detecting that the data stored in the cloud. The notion of Proof of Ownership (POW) was proposed to alleviate the cloud server from storing multiple copies of the same data.

4. Proofs of ownership and retrievability in cloud storage

R. Du et.al [4] proposed "Proofs of ownership and retrievability in cloud storage". Deduplication is a basic requirement for cloud storage as it saves storage space of cloud servers. As clients are not trusted from the perspective of the server, the concept of Proofs of Ownership (PoWs) has been proposed in client-side deduplication. On the other hand, the clients cannot completely trust the server either, thus clients have to know whether their files are stored integrally in the cloud. Most of the existing system focuses on only one-way validation. Proofs of Ownership and Retrievability (PoOR) is introduced in this paper. Clients can prove to the server their ownership of files and verify the retrievability of the files without uploading or downloading them.

3. SYSTEM DESIGN

3.1 SYSTEM MODEL

There are five phases in system:

- Pre-process
- Upload
- Deduplication
- Update
- Proof of storage.

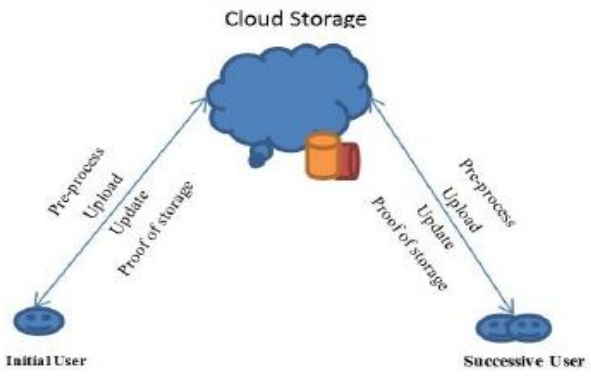

Fig -1: System Architecture

Fig – 1 represents the system model of deduplicatable dynamic Pos.

In the pre-process phase, users tries to upload their files. The cloud server decides whether these files should be uploaded. If the upload process is granted, go into the upload phase; otherwise, go into the deduplication phase.

In the upload phase, the files to be uploaded that are not existed in the cloud server. The users encodes the local files and upload them to the cloud server.

In the deduplication phase, the files to be uploaded alreadyexists in the cloud server. The subsequent users possess the files locally and the cloud server stores the

authenticated structures of the files. Subsequent users need to convince the cloud server that they own the files without uploading them to the cloud server.

In the update phase, users may modify, insert, or delete some blocks of the files.

In the proof of storage phase, users only possess a small constant size metadata locally and they want to check whether the files are faithfully stored in the cloud server without downloading them.

3.2 USE CASE DIAGRAM

There are three modules in the system:

- Owner Module
- Proxy Module
- User Module

Owner Module

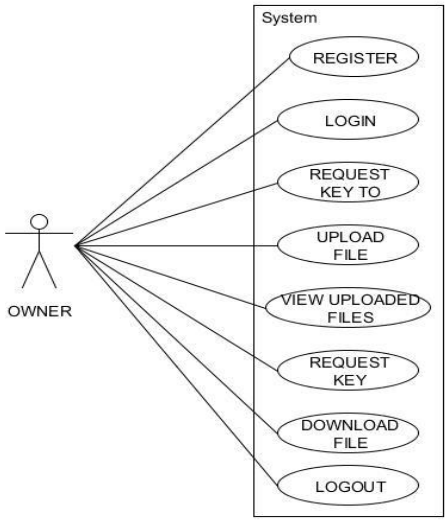

Fig -2: Use case diagram of owner module

Fig – 2 shows use case diagram of owner module. Owner first registers by giving all details, after that owner logs-in. Owner uploads file by obtaining private key from admin through email. Owner can view all files uploaded by particular owner. Owner downloads files by requesting private key. After all program owner logs-out.

Proxy Module

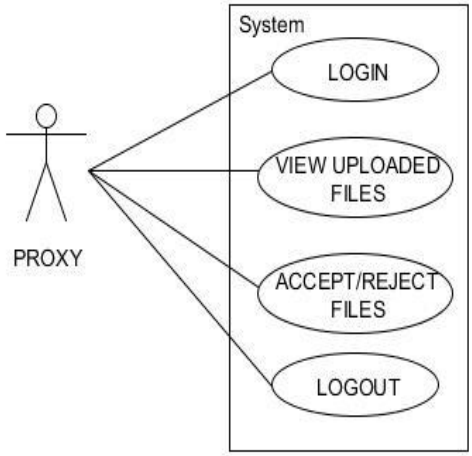

Fig -3: Use case diagram of proxy module

Fig – 3 shows use case diagram of proxy module. Here, proxy can view all uploaded files of owner. Proxy has authority for accepting or rejecting the files uploaded by owner.

User Module

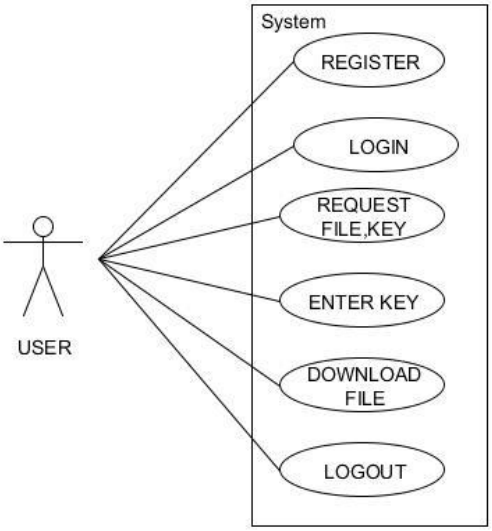

Fig -4: Use case diagram of user module

Fig – 4 shows use case diagram of user module. User first registers by giving all details, after that user logs-in. User requests key for downloading file from owner. User gets key through email.

4. CONCLUSIONS

The comprehensive requirements in multi-user cloud storage systems and the model of deduplicatable dynamic PoS is introduced. HAT is an efficient authenticated structure. Based on this HAT, the first practical deduplicatable dynamic PoS scheme called DeyPoS is proposed. The results shows that DeyPoS implementation is efficient, when the file size are large. Email Notification of private key to data owner to upload and download files.

REFERENCES

[1] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Proc. of FC*, pp. 136–149, 2010.

[2] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340–352, 2016.

[3] Q. Zheng and S. Xu, "Secure and efficient proof of storage with deduplication," in *Proc. of CODASPY*, pp. 1–12, 2012.

[4] R. Du, L. Deng, J. Chen, K. He, and M. Zheng, "Proofs of ownership and retrievability in cloud storage," in *Proc. of TrustCom*, pp. 328–335, 2014.