A Novel Approach for an Enhanced Oruta with Data Freshness

Ridham Kapadiya
Research Scholar
Department of Computer Science
Parul Institute of Technology, Vadodara, Gujarat

Jignesh Prajapati
Assistant Processor
Department Of Computer Science
Parul Institute of Technology, Vadodara, Gujarat

ABSTRACT
Cloud computing has become an emerging service because of the ease of its use. Its vast usage has raised some serious issues. When cloud has become a large storage for the data, the security and integrity have become most serious issues. Users must be concerning with the data stored remotely. Many auditing schemes have been introduced for public auditing which audits data without downloading the whole data. Among them, Oruta is privacy preserving public auditing scheme which uses ring signature that audits data with identity privacy. But Oruta lacks with data freshness, batch auditing and traceability. We have introduced an enhanced scheme which enables data freshness within Oruta. Data freshness is to update data with the latest one.

Keywords
Cloud computing, Shared Data, public auditing, identity, privacy, Data Freshness

1. INTRODUCTION
Cloud computing can be termed as metaphor of an Internet. The reason behind it is the services it provides. The basic meaning of the cloud computing is "Pay as per Use". Cloud computing provides number of services as large storage, online access, remote computing and online software deployment. Cloud services have been defines in three terms

1. Software as-a-service (SAAS)
2. Platform as-a-service (PAAS)
3. Infrastructure as-a-service (IAAS)

Cloud computing has number of benefits like Scalability, Reliability, Reduction in cost, Availability, Data Storage, Online access, Pay Per Use, Device diversity and location independent etc.

Apart from them, cloud computing has several threats as Security , Load balancing, Task scheduling etc. Data stored at remote device faces number of threats like unauthorized access, data loss, data leakage, in secure API, Abuse use of cloud etc.

While cloud provides large storage, there is threat related to integrity. Recently, these mechanisms [5], [6], [7], [8], [9], [10], [11], [12], [13] have been proposed public auditing which can verify the data without retrieving the whole data. The correctness of a client's data can be checked by Provable data possession (PDP), proposed by Ateniese et al. [9], allows a verifier to stored at an untrusted server. [1] describes Oruta which is one of the public auditing scheme. It is privacy preserving auditing scheme which uses third party auditor to verify the integrity of the data. It has bottlenecks like Data freshness, traceability and batch auditing.

This paper includes an enhanced scheme which enables data freshness within Oruta. The rest of the paper is organized as follows. Section II contains system and threat model of privacy preserving public auditing techniques and their design objectives. In section III, an enhanced approach with data freshness is described. Section IV gives the comparative study of all the mechanisms described. Finally, the whole paper is concluded in section V.

2. THE SYSTEM AND THREAT MODEL[1]
System Model[1]

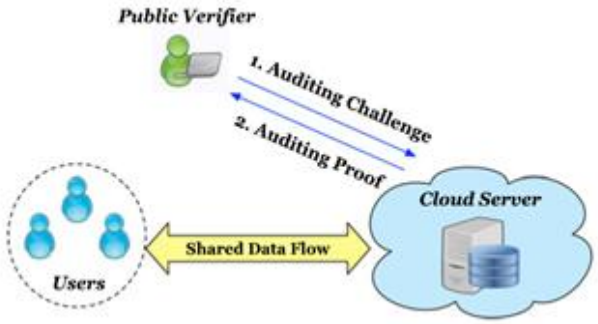

Figure:1 System Model that includes cloud server, a group of users and public verifier[1]

As per shown above in the figuer(1), there are three parts in system model:

1. Cloud Server
2. Public verifier
3. Group of users

Group of users consists two types of user:

1. Data Owner : He/She shares data on cloud server
2. Data User : A number of users which use data that is shared over cloud server.

When a user wants to check the integrity of his data, public verifier sends auditing challenge to cloud server. In response server sends auditing proof. With the use of auditing proof, public verifier checks the integrity.

Threat Model

1. **Integrity Threats**

Two types of threats can be possible:

1. Through an attacker: He may try to corrupt the remotely stored data..
2. Through cloud server provider : Hardware failure and human errors may corrupt data.

2. Security Threats

A public verifier can disclose the identity of the user which may target the particular high-value identity.

Design Objectives

Privacy Preserving mechanisms should achieve following properties:

1. Identity Privacy: A public verifier cannot disclose the identity of user.
2. Correctness: A public verifier should verify the integrity of shared data correctly.
3. Public auditing: The integrity of the shared data must be verified publically without retrieving the entire data from the cloud server.

3. RELATED WORK

In past, most of the data was audited using the traditional MD5 and RSA algorithm, which were auditing the whole data correctly. But for the whole operation, they must have to download the whole data. After that, many mechanisms [4],[5] have been introduced which can audit the data without downloading the whole. This is known as public auditing.

Oruta[1] is one of them which uses public auditing. While Oruta uses public auditing and identity privacy but it has some draw backs.

Oruta fails in achieving data freshness, batch auditing and Treacibility.

After Oruta, Knox[2] has been introduced with treacibility. While Oruta fails in identify the user on some special occasion, Knox has overcome from it using group signature.

In this paper, we are achieving the freshness of the data in Oruta which gives the latest update of the shared data using timestamp.

4. PROPOSED ALGORITHM

Our proposed scheme to achieve data freshness within Oruta is described below:

1. Select the particular shared file to be operated.
2. Select operations from Insert, Update or Delete for selected file.
3. If, file is to be **inserted/updated**, the user will be provided a local copy of the block which will be further updated within the file with new content and updated block identifiers.
4. If, size is to be **deleted,** the block will be removed from the file and the identifiers of the other block will not be affected.
5. When the user will commit the operation, the new timestamp will be updated within the metadata of the object of the file.

Hence, updated timestamp will have the latest possession of the data.

In our mechanism, we have used TimeStamp. When a user will update the block of the data, the object's metadata which is obviously a shared file will be changed, in terms of the value of the TimeStamp. This will lead to freshen up the data in timely manner. After the update of the metadata value, whenever the specific file will be asked, the new updated version will be provided to the user.

5. EXPERIMENTAL RESULTS

We have implemented the whole Oruta within Amazon s3 which is the large storage application provided by Amazon.

Once you share a file within the server, it will be saved and enable to use by other users among the group. As soon as any of the user will update the data, the TimeStamp value within the metadata of the object file will be changed. These all can be seen in the LogFile, as per seen in the figure below.

This will freshen up data according to the time.

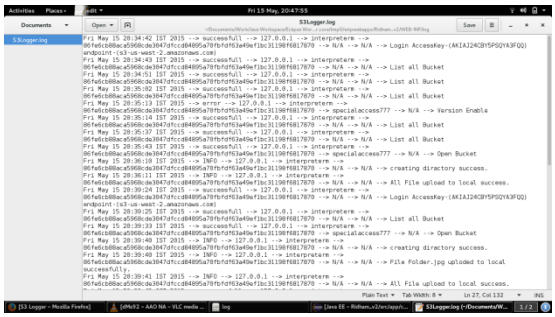

Figure: LogFile in Experimental setup

6. CONCLUSION

In this paper, we have described a detailed description of the system model of Oruta, an enhanced scheme which enables data freshness within Oruta and a comparative analysis of different public auditing mechanism. Data freshness is update with latest data which makes the system more accurate in timely manner. We have achieved data freshness within particular file size by considering it a single block. Data freshness on large size file within blocks can be further extended.

7. REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2012.

[2] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS'12),pp. 507-525, June 2012.

[3] P. Maheswari, B. Sindhumathi, " AFS: Privacy-Preserving Public Auditing With Data Freshness in the Cloud ", IOSR

[4] Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 PP 56-63C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf.

Computer and Comm. Security (CCS ’07), pp. 598-610, 2007.

[6] H. Shacham and B. Waters, “Compact Proofs of Retrievability,” Proc. 14th Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT ’08), pp. 90-107, 2008.

[7] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,“Dynamic Provable Data Possession,” Proc. 16th ACM Conf. Computer and Comm. Security (CCS’09), pp. 213-222, 2009.

[8] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing,” Proc. 14th European Conf. Research in Computer Security (ESORICS’09), pp. 355-370, 2009.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” Proc. 17th Int’l Workshop Quality of Service (IWQoS’09), pp. 1-9, 2009.

[10] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, “Remote Data Checking for Network Coding-Based Distributed Storage Systems,”Proc. ACM Workshop Cloud Computing Security Workshop (CCSW’10), pp. 31-42, 2010.

[11] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau,“Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds,” Proc. ACM Symp. Applied Computing (SAC’11), pp. 1550-1557, 2011.

[12] N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, “LT Codes-Based Secure and Reliable Cloud Storage Service,” Proc. IEEE INFOCOM,2012.

[13] B. Wang, B. Li, and H. Li, “Certificateless Public Auditing for Data Integrity in the Cloud,” Proc. IEEE Conf. Comm. and Network Security (CNS’13), pp. 276-284, 2013.

[14] Ridham Kapadiya, Jignesh Prajapati, "A survey of privacy preserving public auditing techniques for shared data in cloud computing", Proc. IJCA , issue 14, vol 110,2015.