Volume: 2 Issue: X Month of publication: October 2014
DOI:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Enhanced Privacy Preserving with Data Freshness by Accomplishing Traceability over Oruta

R. Rajasaranyakumari[1], S.Velmurugan[2], K.J. Nithya[3]

M.E Scholar, Assistant Professor, M.E Scholar,CSE DEPARTMENT, Veltech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College

Abstract*— Cloud is used not only for storing data, but also the stored data can be shared by multiple users. Due to this the integrity of cloud data is subject to doubt. Several mechanisms have been designed to support public auditing on shared data stored in the cloud. During auditing, the shared data is kept private from public verifiers, who are able to verify shared data integrity using ring signature without downloading or retrieving the entire file. Ring signature is used to compute verification metadata needed to audit the correctness of shared data. With this, the identity of the signer in shared data is kept private from public verifiers. In this paper, we propose a traceability mechanism that improves Data Privacy by achieving traceability and the data freshness(the cloud possess the latest version of shared data) is also proved while still preserving identity privacy.

***Keywords*— traceability, data freshness, public auditing, shared data**

I. INTRODUCTION

Cloud computing platforms provide users scalable data storage services with a low cost than traditional approaches. The integrity of data is subject to doubt due to human errors and hardware or software failures. Therefore, the integrity of cloud data should be verified without any data utilization and without downloading the entire cloud. Traditionally, the data integrity is verified by retrieving the entire data from the cloud and then the correctness of signature is checked. However the efficiency of using this method on cloud data is in doubt [3].

The main reason is that normally the size of cloud data is large. Downloading the entire cloud data to verify data integrity will cost or even waste user’s amounts of computation and communication resources, especially when data have been corrupted in the cloud. Besides many uses of cloud data do not necessarily need users to download the entire cloud data to local devices. It is because cloud providers, such as Amazon, can offer users computation services directly on large-scale data that already existed in the cloud.

Recently, many mechanisms [3], [4] have been proposed to allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing [2]. In these mechanisms, data is divided into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking [3]. A public verifier could be a data user who would like to utilize the owner’s data via the cloud or a third-party auditor (TPA). Moving a step forward, Wang et al. designed an advanced auditing mechanism [2] (named as WWRL in this paper),so that during public auditing on cloud data, the content of private data belonging to a personal user is not disclosed to any public verifiers. That is, there is a leakage of identity privacy.

Failing to preserve identity privacy on shared data during public auditing will reveal significant confidential information to public verifiers. To solve the above privacy issue on shared data, a novel privacy-preserving public auditing mechanism has been proposed. Here Ring signature [9] is exploited to construct homomorphic authenticators, so that a public verifier is able to verify the integrity of shared data without retrieving the entire data, while the identity of the signer on each block in shared data is kept private from the public verifier.

In this paper, to improve Data Privacy on shared data in cloud, we propose Traceability oruta mechanism to achieve traceability. The data freshness (the cloud possesses the latest version of shared data) is also proved while still preserving identity privacy. Achieving data freshness ensures that the retrieved data always reflects the most recent updates and prevents rollback attacks. Achieving data freshness is essential to protect against mis-configuration errors.

	PDP[9]	WWRL[5]	Oruta	Traceability Oruta
Public Auditing	✓	✓	✓	✓
Data Privacy	×	✓	✓	✓
Identity Privacy	×	×	✓	✓
Traceability	×	×	×	✓

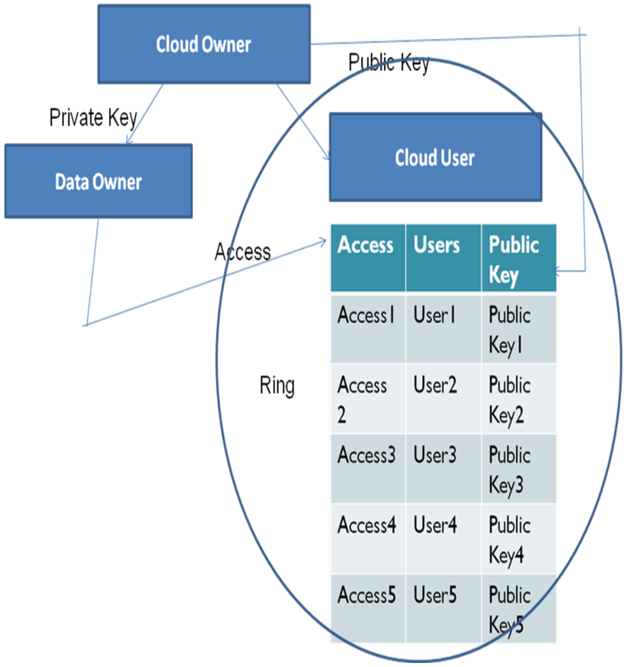
Fig 1. Comparison among Different Mechanisms

II. PROBLEM STATEMENT

The system model in this paper involves cloud owner, Data owner, cloud user or group of users. There are two types of users in a group: the original user and a number of group users. Both the original user and group users are members of the group. Every member of the group is allowed to access and modify shared data. Shared data and its verification metadata (i.e., signatures) are both stored in the cloud server. A public verifier audits the shared data and it checks the integrity of shared data by the ring signature.

As illustrated in fig. 2, when the Data owner stores the data in the cloud, the cloud owner gives the public key to the Data owner and the public key to the cloud user or the group of users. The original user in the group will form a ring signature using his private key and the other group members' public key. Due to this, a public verifier is convinced that a signature is computed using one of group members' private keys, but the verifier is not able to find which one. Due to this, the identity of the signer is preserved from a verifier during auditing. Now there comes a problem when the private key is leaked other than the data owner. This leakage should be tracked.

Our mechanism should be designed to achieve the following properties: (1) **Public Auditing**: A public verifier is able to publicly verify the integrity of shared data without retrieving or downloading the entire data from the cloud. (2) **Correctness**: A public verifier is able to correctly verify shared data integrity. (3) **Traceability:** Tracking the fake user from accessing the data from the cloud. (4) **Identity Privacy**: A public verifier cannot distinguish the identity of the signer on each block in shared data during the process of auditing**. (5) Data freshness**: Data freshness is essential to protect against mis-configuration errors.



Access	Users	Public Key
Access1	User1	Public Key1
Access 2	User2	Public Key2
Access3	User3	Public Key3
Access4	User4	Public Key4
Access5	User5	Public Key5

Fig. 2 our system model includes the cloud owner, data owner and cloud user or group of users

III. ARCHITECTURE DESIGN

In this paper, we are going to propose traceability Oruta to achieve traceability (tracking the fake user).
Data Freshness is also proved by using authenticated file system.

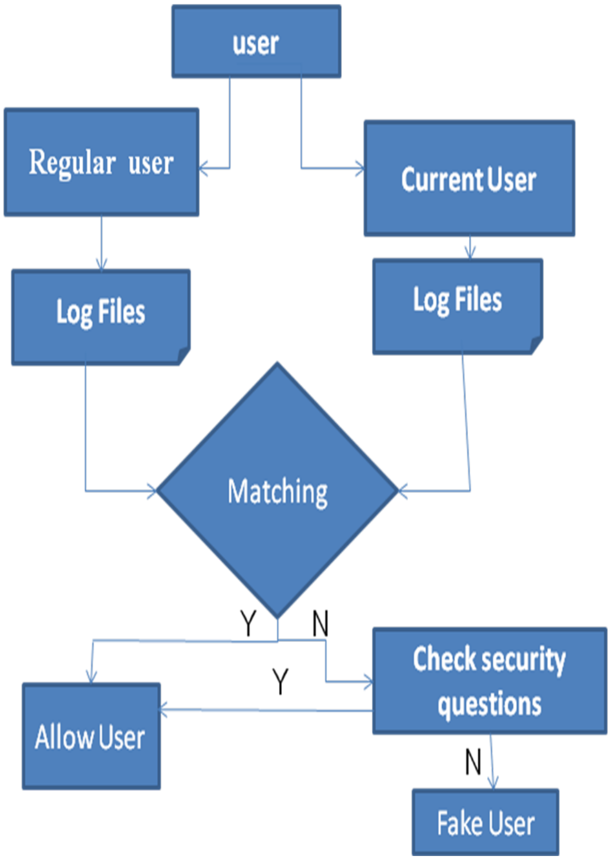


Fig 3. Tracking the fake user

The above figure explains about tracking the fake user. The verifier saves all the attributes and details of the regular user in the log files. The verifier maintains the log files. When the user login; the verifier checks the log files with the existing log files. If the matching is yes, it allow the user and if the matching is no, it checks by asking some security questions. If the answer is correct, then it will allow the user and if the answer is wrong, it is considered as fake user and it blocks that user from accessing the data from the cloud.

IV. RELATED WORK

Provable data possession (PDP) [3], allows a verifier to check the correctness of a data stored at an untrusted server. By utilizing RSA-based homomorphic authenticators and sampling strategies, the verifier is able to publicly audit the integrity of data without retrieving the entire data, which is referred to as public auditing. Unfortunately, this mechanism is only suitable for auditing the integrity of personal data. Proofs of Retrievability(POR), which is also able to check the correctness of data on an untrusted server. The public mechanism proposed by Wang et al. [2] and [6] are able to preserve users' confidential data from a public verifier by using random masking. Compared to previous works [1],[5],[7], this mechanism is able to improve data privacy by using traceability and the data freshness is also proved.

V. CONCLUSION

In this paper, we propose an enhanced Privacy Preserving with Data Freshness by accomplishing traceability over oruta. A new mechanism is adopted to achieve traceability called Traceability Oruta. Due to this, Data Privacy in cloud is improved. We utilize ring signatures, so that a public verifier is able to audit shared data integrity without retrieving the entire data. Data freshness is also proved. Freshness verification should be extremely efficient for existing file system operations and induce minimal latency. To ensure freshness, it is necessary to authenticate not just data blocks, but also their *versions*.

VI. ACKNOWLEDGMENT

I would like to thank my guide Mr.S. Velmurugan for assisting me in this paper work.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy- Preserving Public Auditing for Shared Data in The Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295- 302, 2012.
[2] C. 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.
[3] 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
[4] 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
[5] C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013
[6] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," Proc. IEEE INFOCOM, pp. 2904-2912, 2013
[7] B. Wang, B. Li, and H. Li, "Panda: Public for Shared Data with Efficient User Revocation in the Cloud," IEEE Trans. Services Computing, 20 Dec. 2013, DOI:10.1109/TSC.2013.2295611
[8] 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.
[9] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 552-565, 2001.
[10] A. Juels and B.S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 584-597, 2007