Privacy Preserving Third Party Auditing for Secure Cloud Storage

Swati B. Ghavle
PG Student,
M.B.E.S. College of Engg Ambajogai

B. M. Patil, PhD
PG Department,
M.B.E.S. College of Engg Ambajogai

ABSTRACT
With cloud data services, it is possible to all or common place for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to misconception due to the existence of hardware/software failures and human errors. To allow both data owners and public verifiers several mechanisms have been designed for efficiently auditing cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these previously existing mechanisms will inevitably reveal confidential information, identity & privacy to public verifiers. In this work a novel privacy-preserving mechanism used to supports public auditing on shared data stored in the cloud. In particular, here exploit ring signatures is used which computes verification of metadata on user demand and audit the correctness of shared data.

Keywords
Public auditing, privacy-preserving, shared data, cloud computing, ring signature, data integrity.

1. INTRODUCTION
Cloud services means services made available to users on demand via the Internet from a cloud computing provider's servers. Cloud services are designed to provide easy, scalable access to applications, resources and services and are managed by a cloud services provider. Cloud Platform provides a range of storage services that allow you to maintain easy and quick access to your data. It is timetable for clients to power cloud storage space choices to work together with others in a group. The reliability of data in cloud storage space, however, is liable to instability and examination, as data spared in the cloud can without much of a stretch be missing or harmed because of the unavoidable hardware / software programming issues and individual mistakes. To maintain the popularity such an instances are hide by the cloud server. Therefore, the reliability of cloud information should be verified before any information usage, for example, look for or computation over cloud information.

Previously for verifying information correctness the whole information is recover from the cloud server, and then verify data reliability by verifying the correctness of signatures [7] or hash principles of the entire data. Certainly, this approach has the capacity to effectively check the correctness of cloud information however the execution of utilizing this technique is unreasonable.

As of late, numerous frameworks have been recommended to permit an information proprietor it as well as a public verifier to proficiently perform reliability verifying without downloading the whole information from the cloud, which is generally known as public auditing [4]. In these frameworks, data is divided into number of blocks, where each block is freely signed by the data owner; and a unique mixture of all block rather than the entire data is recovered during integrity checking. Moving forward, Wang et al. developed an auditing procedure, so that during public audit on cloud information, the content of individual information that belong to an individual client is not disclosed to any public verifiers.

Discussing information among several customers is one of the most interesting functions that motivate cloud storage space. Therefore, it is also necessary to create sure the integrity of distributed information in the cloud is correct. Current public audit systems can actually be prolonged to verify distributed information reliability.

In this paper, to fix the above problem on shared data, Oruta a privacy-preserving public auditing procedure is used. More importantly, the ring signatures is implemented to create homomorphic authenticators in Oruta, along with Third Party Auditors (TPA) which is part of a cryptosystem intended to perform data integrity on cloud. So that the verifier is able to check the integrity of distributed information without accessing the entire data, while in shared data the identification of the singer on each block is kept personal from public verifier. Moreover, further increase this procedure to support batch audit, which is capable of doing several audit tasks simultaneously and enhance the performance of verification for several audit projects. And also to improve the privacy in cloud.

The paper is organized as follows. Section 2, presents the Literature survey of the existing systems. Section 3 defines proposed system. In section 4 Result discussion is done, while section 5 conclude the paper. At the end various references used in this paper are mentioned.

1.1 Objectives
Oruta is designed to achieve following properties:

1.1.1 Privacy Preserving
TPA cannot see the user's data content during the auditing process.

1.1.2 Public Auditing
To allow TPA to verify the correctness of cloud data without demanding the copy of whole data.

1.1.3 Batch Auditing
TPA handles multiple users for multiple task during auditing process.

1.1.4 TPA
TPA performs auditing process with minimum communication.

1.1.5 Identity Privacy
The TPA cannot identify the signer of each block when auditing process is going on.

2. LITERATURE REVIEW

2012: B. Wang, B. Li, and H. Li [1] discussed with cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. 2010: C. Wang[4] unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed by 2013: C. Wang [13] to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information-identity privacy-to public verifiers.

2012: K. Ren, C. Wang, and Q. Wang[8] first discussed a number of pressing security challenges in Cloud Computing, including data service outsourcing security and secure computation outsourcing. Then, will focus on data storage security in Cloud Computing. As one of the primitive services, cloud storage allows data owners to outsource their data to cloud for its appealing benefits. However, the fact that owners no longer have physical possession of the outsourced data raises big security concerns on the storage correctness. Hence, enabling secure storage auditing in the cloud environment with new approaches becomes imperative and challenging.

2010: C. Wang, Q. Wang, K. Ren, and W. Lou[4] says **c**loud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. 2007:G. Ateniese[3] said However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. 2012: A Mohta[17], 2012 K Govinda[19] introduces TPA to securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.

2013: B. Wang, M. Li, S.S. Chow, and H. Li[9] addressed the emergence of cloud computing brings users abundant opportunities to utilize the power of cloud to perform computation on data contributed by multiple users. These cloud data should be encrypted under multiple keys due to privacy concerns. However, existing secure computation techniques are either limited to single key or still far from practical, 2013: B. Wang[9] designed two efficient schemes for secure outsourced computation over cloud data encrypted under multiple keys. This schemes employ two non-colluding cloud servers to jointly compute polynomial functions over multiple users' encrypted cloud data without learning the inputs, intermediate or final results, and require only minimal interactions between the two cloud servers but not the users. Authors demonstrate this scheme efficiency experimentally via applications in machine learning. This schemes are also applicable to privacy-preserving data aggregation such as in smart metering.

2010: S. Yu, C. Wang, K. Ren, and W. Lou[21], discussed **c**loud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, 2003:D. Boneh[6] introduce existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved.

2.1 Disadvantages of Existing System:

2.1.1 Failing to preserve identity privacy on shared data during public auditing will reveal significant confidential information to public verifiers.

2.1.2 Protect these confidential information is essential and critical to preserve identity privacy from public verifiers during public auditing.

3. PROPOSED SYSTEM

A public verifiers can publicly verify the integrity of shared data without retrieving the entire data from the cloud. Valid verification metadata (i.e., signatures) is generated by users in the group on shared data. A public verifier cannot distinguish the identity of the signer on each block in shared data during the process of auditing. The original user are initially allowed to create shared data in the cloud, and they shares it with users group. Original user and group users both are members of the group. Every member of the group have access to shared data and also can modify shared data. Shared data and its verification metadata are both stored in the cloud server. A public verifier, such as a third party auditor providing expert data auditing services or a data user outside the group planing to utilize shared data, is able to publicly verify the integrity of shared data stored in the cloud server.

User Login: If the user is an authorized user, he/she can download the file by using file id which has been stored by data owner when it was uploading. When a public verifier wishes to check the integrity of shared data, it first sends an auditing challenge to the cloud server. After receiving the auditing challenge, the Cloud server responds to the public verifier with an auditing proof of the possession of shared data.

If a third party auditor TPA (maintainer of clouds) should register first. This system allows only cloud service providers. After third party auditor gets logged in, He/ She can see how many data owners have uploaded their files into the cloud.

3.1 Cloud Server

3.1.1 Design Objective

This mechanism should be designed to achieve the following properties:

3.1.1.1 Public Auditing: A Third party Auditor (TPA) is able to publicly verify the integrity of shared data without

downloading or retrieving the entire data from the cloud, on behalf of user request.

3.1.1.2 Correctness: A Third Party Auditor can correctly verify correctness shared data integrity.

3.1.1.3 Identity Privacy: A public verifier can't recognize the identity of the signer on each one block in shared data during the auditing process.

3.1.1.4 Unforgeability: Only a user in the group can generate valid verification metadata (i.e., signatures) on shared data. Only users in group have access to shared data.

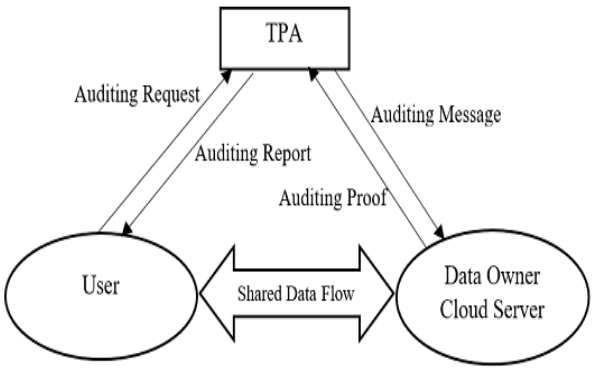

Figure 1: System Architecture

In this scheme three parties are involve: the cloud server, a number of users (group of users) and a public verifier. The unique user and a number of team users are the two kinds of users in the group. The original user originally makes distributed information in the reasoning, and shares it with team customers. Both the unique customer and group users are associates of the team. Every participant of the group is permitted to accessibility and change distributed information. Shared data with its confirmation meta-data (i.e., signatures) are stored at cloud server. When a public verifier desires to examine the reliability of shared information, it first delivers an audit task to the cloud server. After getting the audit task, the cloud server reacts to the community verifier with an auditing evidence of the ownership of distributed information. Then, the community verifier verifies the correctness of the entire data by confirming the correctness of audit evidence. Essentially, the procedure of community audit is a challenge and-response method between a community verifier and the cloud server.

3.2 Group of Users

There are two types of users in a group: the original user and a number of group users. The original user initially creates shared data in the cloud, and shares it with 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, such as a third party auditor providing expert data auditing services or a data user outside the group intending to utilize shared data, is able to publicly verify the integrity of shared data stored in the cloud server.

Owner Registration: In this module an owner has to upload its files in a cloud server, he/she should register first.

Owner Login: In this module, owner have to login, they should login by giving their email id and password.

User Registration: In this module if a user wants to access the data which is stored in a cloud, he/she should register their details first.

User Login: If the user is an authorized user, he/she can download the file by using file id which has been stored by data owner when it was uploading.

3.3 Public Verifier

When a public verifier wishes to check the integrity of shared data, it first sends an auditing challenge to the cloud server. After receiving the auditing challenge, the Cloud server responds to the public verifier with an auditing proof of the possession of shared data. Then, this public verifier checks the correctness of the entire data by verifying the correctness of the auditing proof. Essentially, the process of public auditing is a challenge and response protocol between a public verifier and the cloud server.

3.4 Third Party Auditing

In this module, if a third party auditor TPA (maintainer of clouds) should register first. This system allows only cloud service providers. After third party auditor gets logged in, He/ She can see how many data owners have uploaded their files into the cloud. Here providing TPA for maintaining clouds.

3.5 Ring Signature Scheme

To maintain more data integrity and security ring signature concept is implemented. This concept is proposed by rivest et al [12].ring signature is the type of digital signature which can be performed by any group member of users that each have kays. Therefore a message is signed with ring signature endorsed by someone in a particular group of people. The best property of ring signature is that it should be difficult to identify which was the group member's kay was used to produce signature. The signature is computed using one of the group member's private key but the verifier is not able to determine which one.

4. RESULT AND DISCUSSION

Communication cost can be expressed by auditing message and auditing proof. In Table 1 communication cost of an auditing task is presented. The communication cost that TPA consumes in an auditing task is very small. When maintaining a higher detection probability TPA needs to consume more computation and communication overhead to finish work.

Table 1 represent analysis of communication cost, According to the parameters of table 1 communication cost is easily calculated.

Table 1: Analysis of communication cost.

Group size(d)	Cost1(kb)	Cost2(KB)
2	10.5	14
4	10.5	14
6	10.5	14
8	10.5	14
10	10.5	14
12	10.5	14
16	10.5	14

18	10.5	14
20	10.5	14

Fig. 2 represent the communication cost according to parameters in table 1 for different size. In fig 2 x-axis represent size of group in d and y-axis represent the communication cost in kb.

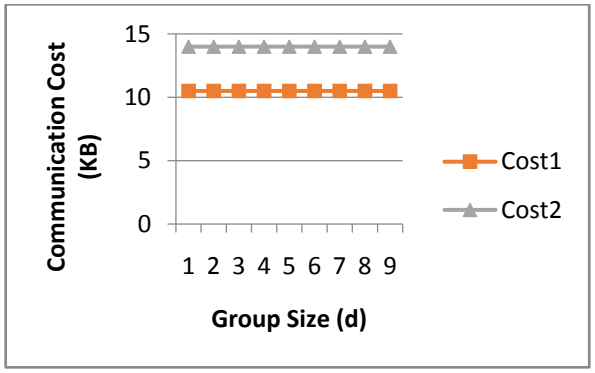

Figure 2: Communication cost for different size of the group

Table 2 is analysis of auditing time. According to below table the auditing time is linearly increasing with the size of the group. When no of group n member increases then auditing time also increases.

Figure 3 represent auditing time for different size of groups where x-axis represent group size in d and y-axis represent auditing time in sec.

Table 2: Analysis of Auditing Time

Size of the group	Auditing time1(sec)	Auditing Time2(sec)
2	0.5	0.7
5	0.7	1.1
8	0.9	1.4
11	1.1	1.8
14	1.3	2.1
17	1.5	2.4
20	1.7	2.7
23	1.9	3

In Figure 3 depending upon size of the group auditing time is different. Auditing time is directly proportional to size of the group.

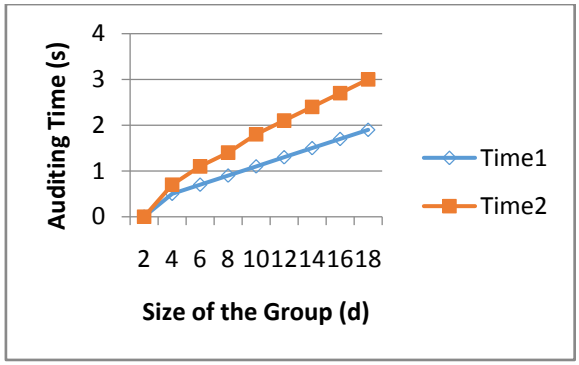

Figure 3: Auditing time for different group sizes

Table 3 represent the comparison between existing PDP and proposed Oruta with different mechanisms i.e. Public Auditing, Data Privacy, Identity Privacy.

Table 3: Comparison among different mechanisms

	PDP[9]	Oruta
Public Audit ng	✓	✓
Data Privacy	×	✓
Identity Privacy	×	✓

5. CONCLUSION

In the privacy preserving public auditing scheme which supports ring signature which ensures that during public auditing process TPA would not learn any information about the data content of group stored on the cloud server. Ring signature preserves the identity of the signer from the verifier. HARS scheme used for group of users in which they share data to each other and update and delete data in block wise manner. Also utilize ring signatures to create homomorphic authenticators, so that a community verifier is able to review distributed data integrity without accessing the whole information, yet it can't recognize who is the signer on each block furthermore it has the capacity to audit shared information integrity without retrieving the whole information. To improve the performance of confirming several review projects, will further extend the Oruta with key distribution center (KDC), which reduces the risks inherent in exchanging keys and also will propose traceability over Oruta (tracking the fake user), due to this data privacy in cloud is improved.

The interesting issues will keep on concentrating on for the future work. Data freshness is one of them; demonstrate the cloud has the most recent version of shared data while as yet preserving identity privacy.

6. ACKNOWLEDGMENTS

I would like to sincerely express thanks to my guide Dr. B. M. Patil for his appreciable support, continuous encouragement and his invaluable suggestions. I am grateful for all the suggestions and hints provided by him. It was great moment to work with him. As part of future work, ORUTA should be extended with more security features such as proofs of

retrievability, data integrity checking and search over encrypted data.

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] M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R. H.Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in Proc. ACM Conference on Computer and Communications Security (CCS), 2007, pp. 598–610.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533.

[5] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). SpringerVerlag, 2001, pp. 552–565.

[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2003, pp. 416–432.

[7] H. Shacham and B. Waters, "Compact Proofs of Retrievability," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). SpringerVerlag, 2008, pp. 90–107.

[8] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[9] B.Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013.

[10] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT'03), pp. 416-432 July 2003.

[16] Juels, B. Kaliski. "Pors: proofs of retrievability for large files[C]", Proceedings of CCS 2007. Alexandria, VA, USA, 2007. 584-597.

[17] Abhishek Mohta, Lalit Kumar Awasti, "Cloud Data Security while using Third Party Auditor", International Journal of Scientific & Engineering Research, Volume 3,Issue 6, ISSN 2229-8 June 2012.

[18] D. Shrinivas, "Privacy-Preserving Public Auditing in Cloud Storage security", International Journal of computer science and Information Technologies, vol 2, no. 6, pp. 2691-2693, ISSN: 0975-9646, 2011.

[19] K Govinda, V. Gurunathprasad and H. sathishkumar, "Third Party Auditing for Secure Data Storage in Cloud Through Digital Signature Using RSA", International Journal of Advanced science and Technical Research, vol4,no. 2, ISSN: 2249-9954,4 August 2012.

[20] Balkrishnan. S, Saranya. G, Shobana. S and KarthikeyanS, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", International Journal of computer science and Technology, vol. 2, no. 2, ISSN2229-4333 (Print) | ISSN: 0976-8491(Online), June 2012.

[21] Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. 2010 Proceedings IEEE INFOCOM. doi:10.1109/infcom.2010.5462174.