ZKG INTERNATIONAL ISSN: 2366-1313

# ENSURING PRIVACY IN CLOUD DATA SHARING: PUBLIC AUDITING APPROACH

#1GUJJULA ABHINAV,
#2KOLLAPURI SUJATHA,
#3N.SANTHOSH KUMAR, *Assistant Professor,*
**Department of Computer Science and Engineering,**
**SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.**

**ABSTRACT:** A central location of the cloud storage service allows multiple users to store and exchange data. When addressing the possibility of data sharing among several users, the question of ensuring the anonymity of individuals' identities during a public audit of the shared data remains unanswered. The breakthrough addition of a third-party auditor (TPA) to our system allows anyone to inspect shared data stored in the cloud while maintaining secrecy. A method for concealing the signatory's identity from the third-party auditor (TPA) involves partitioning the shared file into many smaller sections. The TPA can check the integrity of shared data in this manner without requiring access to the entire file. Using signatures, the Trusted Platform Agent (TPA) can determine the verification information required to confirm the veracity of shared data.

***Keywords:*** Public auditing , cloud computing , shared data, privacy-preserving.

## I. INTRODUCTION

By sharing resources, cloud service providers can give consumers with an extensible, secure, and reliable environment at a lower cost.

There is widespread skepticism about the security of data stored in the cloud due to the possibility of accidental loss, modification, technological failures, or a combination of the two. Hiring a third-party auditor (TPA) is the most effective way to ensure the accuracy of cloud data in advance of public audits.

The major goal of the proven data possession (PDP) approach to public auditing is to ensure the accuracy and completeness of data held on servers. This can be performed without having access to all of the data stored in the cloud, which is not necessarily safe. WWRL is the designated system in this case, and its goal is to create a publicly available cloud data auditing system that protects user-specific information from third-party audits.

Concerns about protecting people' privacy from a third-party investigator during a public probe of shared cloud-based data are considerable. This occurs because, if one knows which group member or portion of the shared data has been signed, that individual or chunk may become a more significant target than the rest. Consider the present situation: Bob and Alice, who are colleagues, have access to the same cloud-based file. When the file is broken into smaller portions, each participant signs them individually. When a member of the group, such as Alice or Bob, modifies a block in this shared file, they must authenticate it using their personal private key. This is done in compliance with any group member's demands to ensure the general integrity of the material. The signature information for each block must be made available to the publicly accessible file's third-party inspection.

ISSN: 2366-1313

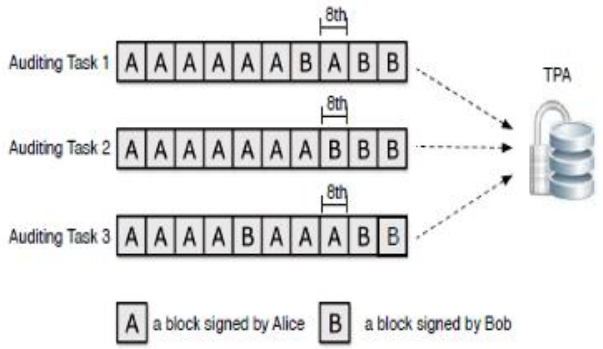


Fig. 1. Alice and Bob share a file in the cloud, and the TPA verifies the integrity of the shared data with existing mechanisms.

Once the TPA has performed the numerous auditing obligations described in Figure 1, they may be given confidential and private information. Alice validated a significant number of the blocks in the shared file. This suggests that Alice is the group's leader and has a considerable influence. Furthermore, there are people that constantly change the eighth part of the shared document. This means that this part may include crucial information that two other members of the group, Alice and Bob, will need to discuss and amend several times. As seen in the preceding picture, identifying the signatory for each shared data block may provide information about which group members or shared data blocks are more desired targets. It is therefore not advisable to divulge such confidential group information to an external reviewer. We require a mechanism to keep identities private while the broader public evaluates cloud-based shared data. However, no such mechanism has been proven in scientific literature. This article describes the first mechanism ever established for protecting privacy during public examinations of shared cloud data. It's known as Oruta.

Oruta uses ring signatures to construct homomorphic authenticators. Even if they do not have total access to the data, the Trusted Third Party (TPA) can employ these authenticators to ensure the security of shared data held by a group of users in an untrusted cloud. The Trusted Third Party (TPA) is also uninformed of the signer's identity for each unit of exchanged data, as it is hidden. Oruta allows for dynamic data operations while protecting data privacy and providing public access.

| | PDP [2] | WWRL [3] | Oruta |
|---|---|---|---|
| Public auditing | Yes | Yes | Yes |
| Data privacy | No | Yes | Yes |
| Identity privacy | No | No | Yes |

Table 1.Comparison with existing mechanisms

Table I shows how the newly implemented Oruta mechanism differs from the pre-existing mechanisms. Unfortunately, Oruta is the only project currently aiming to develop a secure means for all users to access shared data on the cloud while maintaining their privacy.

## II. RELATED WORK

Provable data possession (PDP), a concept first introduced by Ateniese et al., allows one to validate the integrity of data without receiving it entirely from an untrustworthy machine. PDP was the first system that allowed for public auditing.Despite this, it only works with inert data in order to improve testing efficiency. Ateniese et al. used symmetric keys to create a scalable and effective policy decision point (PDP). This method simplifies procedures that rely on dynamic data. Despite this, the system limits the number of verification requests that an individual may submit and prohibits public verification.

Proof of retrievability (POR), a technique devised by Juels and Kaliski, is similar to the one presented here. Furthermore, it can be used to evaluate data stored on systems whose accuracy is doubtful. This iteration adds sentinels, which are collections of blocks containing arbitrary integers, to the original file.The user sends a request to the server for a certain set of sentinel values, which the server returns in response. The user checks the accuracy of the information.

ISSN: 2366-1313

Shacham and Waters were the pioneers of improved POR. It was created using pseudorandom functions and BLS signatures.

Wang et al. created a completely dynamic data acquisition approach by applying the Merkle Hash Tree for public monitoring.

Erway et al. used a rank-based verified dictionary to show a Private Data Publishing (PDP) system that runs indefinitely.

Zhu et al. made it easier to use entirely dynamic data in the public auditing procedure by using index hashes.

Wang et al. conducted a novel analysis and identified the Trusted Public Auditor (TPA) as a technique for analyzing the security of cloud-based data. This strategy ensures the correctness of cloud data while maintaining the confidentiality of stored information. It is incorporated into this mechanism. They improved their system even more by including bulk auditing and leveraging aggregate signature capabilities to manage numerous users' auditing activities at once.

Our most recent analysis confirms that shared data for major cloud organizations is accurate; nonetheless, it is not useful in the context of public audits.

## III. ARCHITECTURE AND DESIGN

As shown in Figure 2, our team is made up of three people: consumers, a cloud server, and a third-party auditor. Individuals in a group can be split into two categories: the primary user and several other members. The group is made up of the first individual and the rest of the group members. The principal user sets up data sharing in accordance with the access control parameters. Individuals in the group can alter and access shared information that was previously created by another group member. The cloud computing system saves both the transferred data and any required verification information, such as signatures. As a result, on behalf of the group members, a third-party auditor can check the accuracy of the shared data on the cloud server.

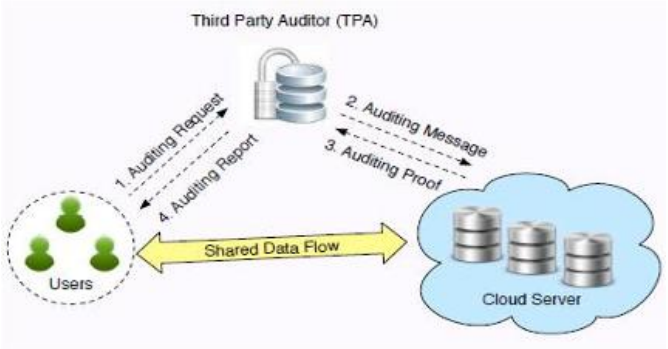


Figure. 2. System model has the cloud server, the third party auditor and users.

This paper investigates the integrity of shared data saved in the cloud, concentrating solely on immutable groups. This indicates that the group is formed prior to the formation of the users' shared data in the cloud, and that its members remain consistent throughout the data sharing process. Before uploading data to the cloud, the person or organization who created it must ensure that only authorized individuals or groups may access it.

Active users in dynamic groups can be withdrawn and replaced with new members while the data is being shared. When looking at the accuracy of data that is collectively saved in the cloud among such flexible companies, protecting people's privacy becomes a major worry. We shall postpone this assignment until a later day when we may return to it.

When a user, whether the group's initial user or a member, wants to confirm the accuracy of information supplied. When the user formally requests that the Third-Party Auditor (TPA) perform an audit, the procedure begins.In response to an auditing request, the Trusted Platform Agent (TPA) sends an auditing message to the cloud server. The cloud server then verifies the legitimacy of the shared data for the TPA. The TPA then checks the accuracy of the reporting proof. The

ISSN: 2366-1313

Third Party Administrator (TPA) provides the user with an auditing report based on the results of the verification procedure.

To protect external auditors from the group's private and sensitive information, ring signatures are used to hide the signer's identity on each block. Conventional ring signatures cannot be used in public auditing procedures because modern ring signature systems lack blockless verification.

In the absence of blockless verification, the Trusted Third Party (TPA) must get the entire data file in order to validate the accuracy of the transmitted information. This method necessitates outstanding speed and a significant quantity of time. As a result, a unique approach known as homomorphic authenticable ring signature (HARS) was developed, building on the BGLS ring signature system.

Using HARS-generated ring signatures protects identifying privacy while facilitating verification without the need for blocks.

When designing Oruta, it is also necessary to consider the provision of space for ring signatures. The HARS process for producing a ring signature defines a block m as a component of the set of numbers modulo p. G1, a circular group of p elements, has an additional d members in the Zp ring signature. A block of |p| bits necessitates a ring signature that spans d × |p| bits, requiring significant storage capacity. Customers are extremely unsatisfied with this, as cloud service providers like Amazon charge users based on the amount of storage space they utilize.

To reduce the spatial requirements of ring signatures, an aggregated technique is used. This enables the Trusted Public Auditor (TPA) to evaluate the supplied data with ease.

**A. Threat Model**

**Integrity Threats:**Two potential threats threaten the security of shared data. Initially, a hostile actor may jeopardize the integrity of the shared data, limiting users' ability to properly use the information. Furthermore, data saved in the cloud is vulnerable to loss or theft in the event of an error or technical failure.

**Privacy Threats:**A partially recognized Third Party Auditor's (TPA) job is to verify the accuracy of shared data. Using verification details, the TPA may attempt to establish who signed each block of shared data, despite the fact that this information is highly confidential and should only be shared inside the group. A Third-Party Auditor (TPA) can easily identify a lucrative target by providing the signing authority for each shared cloud data block.

**B. Design Objectives**

To allow a group of users to quickly and safely study shared data, Oruta's design must include the following features:

1. **Public Auditing:**In this scenario, the third-party auditor can verify the precision of the cloud-stored data that users disclose without having to retrieve the complete dataset.
2. **Correctness:**A third-party auditor is capable of precisely identifying any tainted data blocks in shared data.
3. **Unforgeability:**Only group members may verify information for data exchange.
4. **Identity Privacy:**Despite continual surveillance, the TPA is unable to identify which party signed each shared data block.

## IV. CONCLUSIONS AND FUTURE WORK

This is the principal source for receiving assistance in auditing publicly accessible cloud data while keeping privacy measures. As a result, the Trusted Third Party (TPA) is capable of performing verifications to ensure the accuracy of provided data. Additionally, they can protect users' privacy by preventing the TPA from determining who signed each block of exchanged data.

Individuals who are members of dynamic groups may be ejected during data exchange while new members are recruited. How to protect privacy while performing audits to validate the authenticity

ISSN: 2366-1313

of data shared by dynamic groups in the cloud is an exciting topic. We will postpone this until we have conducted a more thorough investigation of the problem.

**REFERENCES**


1. M. Armbrust, A. Fox, R. Griffith "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, April 2010.
2. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in Proc. ACM CCS, 2007, pp. 598–610.
3. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE INFOCOM, 2010, pp. 525–533.
4. R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc. ASIACRYPT. Springer-Verlag, 2001, pp. 552–565.
5. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proc. EUROCRYPT. Springer-Verlag, 2003, pp. 416–432.
6. H. Shacham and B. Waters, "Compact Proofs of Retrievability," in Proc. ASIACRYPT. Springer-Verlag, 2008, pp. 90–107.
7. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," in Proc. European Symposium on Research in Computer Security. Springer-Verlag, 2009, pp. 355–370.
8. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in Proc. ACM Symposium On Applied Computing, 2011, pp. 1550–1557.
9. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in Proc. ICST SecureComm, 2008.
10. A. Juels and B. S. Kaliski, "PORs: Proofs pf Retrievability for Large Files," in Proc. ACM CCS, 2007, pp. 584–597.