IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
Research Paper Journal Volume 11, Iss 01, 2022

ORUTA: PUBLIC AUDITING OF SHARED DATA IN THE CLOUD FOR PRIVACY PROTECTION

[#1]**Ms.RAVULA HARITHA,** *Assistant Professor*
[#2]**Ms.KAITHOJU PRAVALIKA,** *Assistant Professor*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Cloud storage providers commonly engage in both data storage and data sharing operations, which involve storing data on the cloud and distributing it among several users. However, the issue remains regarding how to safeguard individuals' identities while simultaneously enabling public scrutiny of the shared data. This study presents a novel approach that ensures users' privacy while allowing transparent auditing of shared data stored in the cloud. To precisely calculate the verification data required for an audit of the integrity of the shared data, we utilize ring signatures. Our methodology enables a third-party auditor (TPA) to assess the integrity of published material without the need to download the entire file. This is achieved while maintaining the signer's privacy on each specific block. The test results demonstrate the efficacy of our proposed strategy in auditing shared data.
Keywords: Cloud computing, Shared Data, public auditing, identity, privacy

1. INTRODUCTION

Because they combine their resources, cloud service providers are able to consistently supply customers with a reliable system. When given by enterprises, customers now have access to an environment that is reliable, secure, scalable, and cost-effective.

Users of different cloud storage systems, such as Dropbox and Google Docs, routinely exchange files with one another. The vast majority of platforms that are analogous to cloud storage often come equipped with this feature as standard fare. Data that is stored in an environment that cannot be relied upon to be secure, such as the cloud, has a lower degree of reliability since both technological and human faults have the potential to cause the data to become corrupted or lost. The most efficient method for putting public auditing into reality is to hire a third-party auditor (TPA) who possesses more advanced processing and communication abilities than typical users. This can be achieved by delegating the responsibility to another party. When done in this way, the veracity of the data that is stored in the cloud can be protected from potential compromise.

The first PDP technique for public auditing is designed to check the authenticity of data that is held on a server that is unreliable without requiring the user to download the entire data set. This technique was developed for use in public auditing. This is the primary goal that this method aims to achieve. Wang et al. (henceforth referred to as WWRL) are working on a project to construct a public auditing strategy for cloud data. The objective of this project is to protect users' personal information from prying eyes by obscuring it with the public auditing approach. The project has been given the acronym PATCCD, which stands for Public Auditing approach for Cloud Data.

We have a strong opinion that one of the key reasons behind the rapid rise in popularity of cloud storage is the fact that it enables numerous users to concurrently exchange and trade data. This is because cloud storage allows for multiple users to share and trade data simultaneously. This is one of the most important variables that contributed to the problem.

System architecture

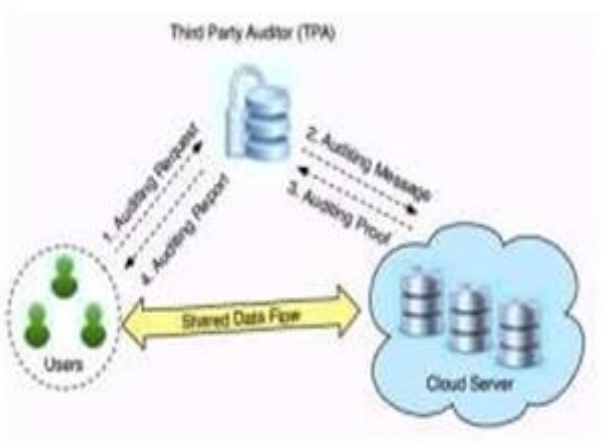

Fig 1.System Architecture

Our Contributions

- The following is a rundown of some of the most noteworthy discoveries that came out of this research project.
- One approach that may be utilized to protect data that is stored in the cloud is the utilization of distributed access control. This method makes certain that only users who are permitted to access the data are able to do so.
- A validation step is required to be completed and then the information must be stored in the cloud before it can be uploaded or updated.
- During the authentication process, private information related to the user is in no way uploaded to a cloud storage service under any circumstances.
- Due to the fact that key maintenance is not a centralized operation, it is possible to assign this responsibility to a distributed network of Key Distribution Centers (KDCs).
- If neither individual has individual authority to access the data or authenticate themselves, then a collusion-resistant access control system will prevent the two users from working together to gain the data or authenticate themselves. This is because working together to obtain the data would violate the terms of the access control system.
- If the user's permission to access the data is revoked for any reason, the user will no longer be able to access the data at any point in the future.
- The technique that has been suggested is robust enough to survive a wide variety of different kinds of attacks. If the author does not have their prior authorization and access, they will not be allowed to write anything that is more than a few years out of date.
- Cloud-based operations are mostly to blame for the high costs, which are comparable to those of previously implemented centralized systems but have the same level of expense.
- On cloud-based data storage, the protocol provides support for a comprehensive selection of I/O operations. Operations that are performed in the cloud are the primary cause of the high prices.

2. RELATED WORK

Because they pool their resources, cloud service providers are in the unique position of being able to consistently and dependably offer their customers with a system. This is made possible by the fact that cloud service providers operate in the cloud.

When businesses give their customers with an environment, their customers now have access to an environment that is dependable, secure, scalable, and cost-effective. It is normal practice for users of different cloud storage platforms, such as Dropbox and Google Docs, to share data with one another. This sort of information exchange takes place in a setting that utilizes cloud storage. This functionality is often supplied as standard fare in the vast majority of systems that function in a manner that is analogous to cloud storage.

This is because this functionality allows users to share and collaborate on files. Data that is stored in an environment that cannot be relied upon to be secure, such as the cloud, has a lower level of dependability than data that is stored in another environment. This is because both technology failures and human errors have the ability to cause the data to get corrupted or lost. The reason for this is due to the fact that human

errors are more likely to occur.

Employing a third-party auditor (TPA) who has more advanced processing and communication abilities than regular users is the most effective way to make public auditing a reality. This can be accomplished by hiring a professional who specializes in auditing businesses. This is due to the fact that TPAs are not affiliated with the company that is being audited. One method for achieving this objective is to transfer responsibility for fulfilling the commitment to a third party, be it a person or an organization. If it is carried out in such a manner, the validity of the data that is stored in the cloud can be protected from the risk of having its integrity compromised.

The first PDP technique for public auditing is designed to check the validity of data that is stored on a server that is unreliable without requiring the user to download the entire data set. This can be done without the user needing to sign up for a PDP account. This is feasible due to the fact that the server that stores the data is specifically intended to validate the data's credibility at regular intervals.

This procedure was developed specifically for use in the oversight of public agencies and organizations. This is the primary purpose that this strategy is meant to achieve, and it has been created to do so. A project to provide a public auditing technique for cloud data is now being worked on by Wang and colleagues, who will be referred to in the following as WWRL. This project's goal is to protect the private information of users from the prying eyes of third parties by adopting a technique of public auditing that obscures the information.

This will be accomplished by using a method of public auditing. The project has been given the name "Public Auditing approach for Cloud Data," which can also be abbreviated as "PATCCD." PATCCD is an acronym that stands for "Public Auditing approach for Cloud Data." We are firmly of the idea that one of the key reasons behind the meteoric rise in popularity of cloud storage is the fact that it enables a huge number of users to simultaneously exchange and trade data. This is one of the primary reasons we are of the strong belief that this is one of the primary reasons behind the meteoric rise in popularity of cloud storage.

This is something that is supported by a substantial body of evidence that we have. This is because cloud storage makes it possible for several people to simultaneously share and trade data with one another. This is one of the most important aspects that contributed to the problem developing into the state that it is in right now.

3. PROPOSED METHOD

We offer Oruta, which is a ground-breaking public auditing system that protects the privacy of users, as a viable solution to the aforementioned privacy risk that is related with shared data. This risk is associated with the fact that shared data is inherently public. Within the Oruta framework, we are able to construct homomorphic authenticators by making use of ring signatures as the building blocks.

When this is done, the public verifier will not be able to see the signer's private information, and the verifier will be able to verify the data's integrity without having to download the entire file. This protects the signer's right to privacy.

In addition to this, by including batch auditing into our entire approach, we have streamlined the process of certifying a wide variety of auditing activities.

This was previously a complex and time-consuming process. Oruta makes a contribution to the method of random masking, which is used in WWRL to hide crucial information from independent auditors.

Oruta was designed to work with a diverse range of masking systems, each of which is tailored to a particular scenario. In addition, in order to better handle dynamic data, we have borrowed index hash tables from a preexisting open auditing system.

This step was taken in order to improve the administration of dynamic data. On a more expansive level, Oruta is contrasted with other systems that have already been constructed.

4. IMPLEMENTATION OWNER REGISTRATION:

The owner needs to finish the registration process first in order for the user to be able to make use of this module. As a direct result of this, the owner of a company is required to register for an account before they are given authorization to store data in the cloud. It is feasible to get entry to a database that has pertinent information on the person in question.

Owner login:

This module should be utilized by everyone on the list that I just established, and each person on the list should log in. In order to participate in this activity, you will need to be in possession of a user's email address as well as their password.

User registration:

Users are required to first register in this section by entering their information in order to gain access to any data that is saved in the cloud. After successful registration, users will be granted permission to access any data that is stored in the cloud. A database is used to store the information so that it can be accessed and utilized at a later time.

User login:

Users that are granted permission to view the file will be required to submit the file ID that was provided by the data owner at the time that the file was uploaded.

Third Party Auditor Registration

A cloud service must first be registered with the module by a cloud provider, who is also frequently referred to as a third-party auditor. Only after this step may a cloud offering be taken into consideration. When implementing this technique, consumers are prohibited from employing more than three cloud service providers at the same time.

Third party auditor login:

Once permission to access the system is granted, a third-party auditor from the outside world can determine the number of data owners who have saved files using cloud storage. Each of the three cloud infrastructures that we support will receive an annual budget of three megabytes to distribute to their respective budgets.

Data sharing:

If the data in question is kept on the cloud, then and only then will we consider employing static groups in the process of establishing whether or not shared data is consistent. This means that the group is formed before any data is shared in the cloud, and its membership is maintained at an accurate count for the entirety of the process of sharing data by means of routine additions and deletions of members.

The original owner of the data should first decide who has access to the data and who does not have access to the data before migrating the data to the cloud. Before information stored in the cloud is made available to mobile teams, it is necessary to confirm that the information is accurate. This is an additional important consideration to take into account. New users can join the club by registering with a pseudonym, while existing members have the option to have their membership revoked.

5. CONCLUSION

Oruta is a state-of-the-art auditing tool that was designed for the goal of guaranteeing that user privacy is protected when examining data stored in public cloud environments. This was accomplished through Oruta's ability to perform audits in a way that is completely decentralized. It is the first of its sort to be made available to the general public, and it is unique.

To protect the identities of those who contribute to a network without compromising the safety of the network as a whole, we develop homomorphic

authenticators that are founded on ring signatures. In this way, the TPA will be able to examine the data's integrity without jeopardizing the data's safety in the process. In order to ensure that all of our auditing tasks are checked in the most efficient manner possible, we are constantly trying to develop and improve our batch auditing technique.

When we continue in this line of study, one of the difficulties that we will strive to overcome is the difficulty of detecting the authenticity of shared data within continually shifting groups while still concealing the identity of the signer. This is one of the issues that we will attempt to tackle. We plan to include consideration of this issue in the work that we are carrying out in the not-too-distant future.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R. H.Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, Stoica, and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 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 Conference on Computer and Communications Security (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 International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533.

[4] 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). 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. In- ternational Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2003, pp. 416–432.

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

[7] 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 (SAC), 2011, pp. 1550–1557.