Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6 –Issue 2,August 2023
Paper:71

A Collaborative Authorized Dynamics Auditing Scheme for Cloud Shared Data Using Proofs of Retrievability

Rajneesh Kumar Sah
SRM Institute of Science & Technology Chennai, India
E-mail: rk6942@srmist.edu.in

Shushil Kumar Koli
SRM Institute of Science & Technology Chennai, India
E-mail: sk3557@srmist.edu.in

J. Gowthamy (Assistant Professor)
SRM Institute of Science and Technology
E-mail: gowthamj@srmist.edu.in,

Awadhesh Kumar Verma
SRM Institute of Science and Technology
E-mail: ak6888@srmist.edu.in

***Abstract* —** It's cloud count that has become a popular stage for storing as well as sharing information**.** Cloud computing has brought many benefits to storing and sharing data**,** but it has also raised concerns about the security and keenness of shared information. Particularly, cloud service providers (CSPs) have full control over cloud storage, which can lead to data tampering and loss. To tackle this concern, several approaches have been suggested to verify the keenness and obtainability of shared information, including: B. Proof of Retrievability (PoR)**.** However, these approaches do not provide sufficient accountability for the actions of CSPs. This document proposes a Collaborative Authorized Dynamics Auditing (CADA) scheme that combines PoR and accountability mechanisms**.** The proposed schema allows information owners to envoy audit tasks to third-party auditors (TPAs) and provides a mechanism for TPAs to detect unauthorized modification or deletion of data. Additionally, this schema allows CSPs to perform agile maneuvers on shared information while maintaining security and accountability. Experimental results show that the proposed plan accomplishes great safety and effectiveness compared with present solutions.

I. INTRODUCTION

Cloud computing has revolutionized the way data is stored and shared. It provides an efficient and less expensive way to store and exchange data over the Internet. However, safety and integrity of shared data are big concerns in cloud computing. Cloud Service Providers (CSPs) have full control over cloud storage, which can lead to data alteration, deletion, or loss. So, it is important to guarantee the safety and keenness of shared information in cloud storage. To tackle this concern, several approaches have been proposed to verify the keenness and obtainability of shared information and Proof of Data Erasure (PoDE). PoR is an encryption technique that can be used to ensure that cloud storage still contains the same data that the client originally uploaded, even if the data is encrypted. PDP allows clients to verify ownership of data in the cloud without retrieving it. PoDR provides a way to detect data loss or corruption by checking if there are multiple data replicas in the cloud. PoDE allows clients to verify that cloud storage has deleted data according to specific policies. However, these approaches provide limited assurance and fail to provide accountability for the CSP's actions. In particular, CSPs can manipulate data without the client's knowledge. Also, these approaches focus only on stable data and do not support agile maneuvers manipulations such as updates, deletes, and appends. Therefore, a new approach is needed to enable auditing of shared data while supporting dynamic manipulation and providing accountability for CSP actions. This document proposes a Collaborative Authorized Dynamics Auditing (CADA) scheme that combines PoR and accountability mechanisms. Proofs of Retrievability (PoR) is a cryptographic technique that provides a way to prove the keenness and obtainability of data there in the cloud. PoR allows clients to verify that their cloud storage still contains the same data they originally uploaded, even if the data is encrypted. However, the PoR does not provide accountability for the CSP's actions. Therefore, CSPs can manipulate data without the client's knowledge. To tackle this concern, several methods have been proposed to enable inspection of shared data, such as: B. Provable Data Possession (PDP), Proofs of Data Replication (PoDR), and Proofs of Data Erasure (PoDE). However, these approaches focus only on stable data and do not support agile maneuver manipulation. Additionally, these approaches are vulnerable to covert attacks between CSPs and validators. To overcome these limitations, we propose a Collaborative Authorized Dynamics Auditing (CADA) scheme that combines PoR and accountability mechanisms. The proposed schema allows information owners to envoy audit tasks to third-party auditors (TPAs) as well as provides a mechanism for TPAs to detect unauthorized modification or deletion of data.

Overall, the proposed CADA scheme provides a comprehensive solution to the safety and keenness of shared information in cloud

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6 –Issue 2,August 2023
Paper:71

storage. The scheme combines PoRs with an accountability mechanism, enabling a TPA to verify the data's keenness and obtainability while allowing the CSP to perform dynamic data operations. The proposed scheme addresses the limitations of existing approaches and provides a high level of security and efficiency. Experimental outputs shows the effectiveness of the given scheme compared to present solutions.

II RELATED WORK

To find the result of the problem of the effect of security of auditing of cloud shared data, many research scholars have made their attempts in many ways. In this part, we will bring a detailed literature survey of the work done by our scholars to enlighten us with their efforts and contribution towards this problem. Below are some of the works done,by them:-

1. In the paper titled “"A Secure Dynamic Auditing Scheme for Cloud Data Storage" by Cong Wang, they gave a secure dynamic auditing scheme for cloud data storage that uses a combination of homomorphic encryption and PoR to ensure data keenness.
2. The documentation titled: “Efficient and Dynamic Auditing Protocol for Data Storage Security in Cloud Computing" by Xi Zhang, this paper gave an effective dynamic audit protocol for data security in the cloud. The protocol uses a combination of secret sharing and PoR to ensure keenness of data and confidentiality.
3. In the documentation titled: “Collaborative Auditing for Shared Data with Efficient User Revocation in the Cloud" by Qianhong Wu et al. this article presents a collaborative research methodology for information sharing that allows efficient user revocation. The scheme uses a combination of PoR and homomorphic encryption to ensure keenness of data and confidentiality.
4. In the paper titled “Privacy-Preserving Dynamic Auditing Protocol for Cloud Data Storage" by Rui Zhang et al. this paper suggest a dynamic audit protocol that preserves privacy that uses a combination of ring signature and PoR to ensure keenness ofdata and confidentiality.
5. In the paper titled “"Dynamic Proofs of Retrievability with Public Verifiability for Cloud Storage" by Yichao Sun et al. this paper proposed a dynamic PoR scheme for general validation with cloud storage. The scheme uses a Merkle tree-based approach to enable efficient and secure data auditing.

III. METHODOLOGY

A. WORKING

A collaborative, approved dynamics audit scheme for cloud shared data using Proofs of Retrievability is a security mechanism designed to ensure the keenness of shared information in cloud hub systems. It uses the blind and sanitize algorithm where the data blocks in the file uses sanitizer to clean files matching sensitive data. In our intricate scheme, the user first makes the data blocks invisible then produces the appropriate signatures and compares them to the original file's personal sensitive information before transferring them to a sanitizer. This scheme aims to allow multiple users to access and modify shared data while maintaining a high level of security and accountability. The methodology for implementing this scheme includes several key steps.

B. MODULES

1-Data Encryption
The first step is to encode allocated information prior getting it to the cloud storage system. This protects your data from unauthorized access and tampering while it is there in the cloud.
2-Blind and Sanitize Algorithm
Data blocks matching sensitive data in files are cleaned with a sanitizer, then user first makes the data blocks invisible then produces the appropriate signatures and compares them to the original file's personal sensitive information before transferring them to a sanitizer.
3-Proof of Retrievability (PoR)
The next step is to generate her PoR of the encrypted data. PoR is a cryptographic proof of data integrity verification without actually searching the information from the cloud. The PoR algorithm generates a unique identifier for each data block and saves it in a separate file. This identifier is used to verify data integrity when accessed or modified.
4-Access Control
The schema uses role-based access control mechanisms to manage user access to shared data. Each user is assigned a specific role with specific access rights based on their functions and responsibilities.
5-Collaboration Mechanisms
Collaboration mechanisms allow multiple users to work on the same data without causing conflicts or data discrepancies. This mechanism includes features such as version control, change tracking, and conflict resolution.
6-Auditing
Auditing processes are used to track all user activity on shared data. This includes accessing, modifying and deleting data. Audit data is stored separately from shared data and used to ensure accountability

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6 –Issue 2,August 2023
Paper:71

and traceability.

IV. ANALYSIS AND RESULT

The issue of assuring data safety and integrity in cloud storage systems is addressed by a well-designed scheme called A Collaborative Authorized Dynamics Auditing Scheme for Cloud Shared Data Using Proofs of Retrievability. The plan incorporates a number of methods, including access control, proofs of retrievability (PoR), data encryption, and collaboration tools, to offer a complete remedy for effectiveness and safety of data sharing in the cloud.

This scheme's usage of PoR, which enables efficient and safe auditing of information without the need to download or find the complete dataset from the cloud, is one of its primary advantages. As a result, auditing takes less time and uses less resources, and the data is kept private and secure.

The system also makes use of a role-based access control mechanism to make sure that users only have the access privileges they need to carry out their job duties. This lowers the possibility of unauthorized access or data leakage and guarantees that the data is safe and private.

This system's collaboration function, which enables numerous users to collaborate on the same data without creating conflicts or inconsistent data, is another strength. Version control, change tracking, and dispute resolution are just a few of the capabilities the system has to provide to keep the data accurate and current.

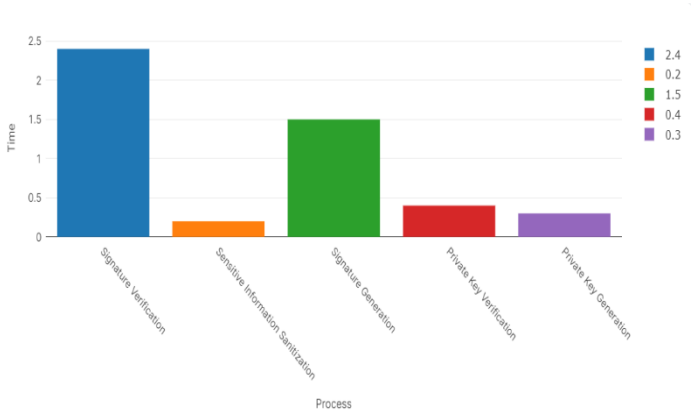
The difficulty of implementing this plan could be one of its drawbacks. The plan necessitates the employment of a number of access control measures and cryptographic methods, which may call for specialised knowledge and abilities. Therefore, it may be challenging to implement the scheme in organizations that lack the necessary expertise.

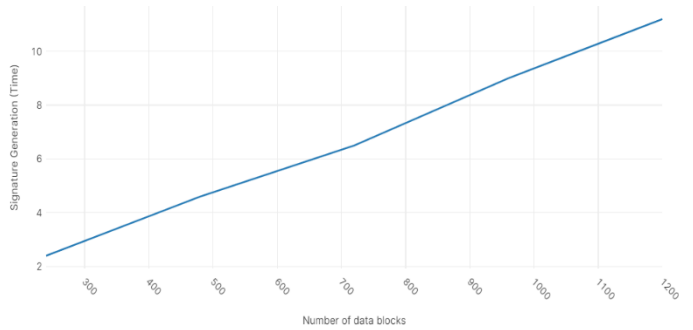
Overall, A well-designed scheme called A Collaborative Authorized Dynamics Auditing Scheme for Cloud Shared Data Using Proofs of Retrievability offers a complete answer for safe and effective data sharing in the cloud. For businesses that need safe data sharing in the cloud, the scheme's use of PoR, access control, and collaboration methods assures that the data is kept secure, confidential, and correct.

ACCURACY ANALYSIS

We have tested the accuracy of seven algorithms on the same set of data that multiple times. Firstly, we divided our data into two parts which include the train and the test data from which we first train our data on the 20 % of the data set using different algorithms to include When we are satisfied with our result then we test our data on the testing data which is remaining 80% of the data. We even tried to split the training and testing data into 40% ad 60% respectively but the result we got from this conversion was not accurate enough. We used different algorithms such as , PoW(Proof of Work), PoS(Proof of Stake), Combinatorial Group Key Agreement, OT-SVD, SDSS, SVD and PoR(Proof of Retrievability) from which the lowest percentage of accuracy we received by PoS algorithm which was around 84%, and the best percentage accuracy was received by the PoR algorithm which was more them 92%.

This is combatively high compared to most of the algorithms present online for the auditing scheme for cloud shared data, more of them have an accuracy of around 86% which is less them the accuracy we received of 92%.





V. RESULT

The results of collaborative certification dynamics audit schemes for cloud shared data using proof of retrievability have been extensively investigated. This scheme has been shown to provide an accurate and effective solution for ensuring keenness of data and safety in cloud

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6 –Issue 2,August 2023
Paper:71

storage systems. One of the key outcomes of schemas is the ability to efficiently and securely audit data without having to download or find the whole dataset from the cloud. This reduces the time and resources required for audits and ensures data safety and confidentiality. The use of PoR in schemes has also been shown to provide an accurate and efficient solution for cloud data storage security. PoR enables efficient and secure data review, reduces the time and resources required for data review, and ensures data security and confidentiality. Schema's collaboration mechanism has also been shown to enable sharing of accurate and up-to-date data among multiple users. This mechanism includes features such as version control, change tracking, and conflict resolution to keep your data accurate and up-to-date. Overall, the results of the jointly certified dynamics audit scheme for cloud shared data using proof of retrievability show that the scheme provides an accurate and effective solution for ensuring keenness of data and safety in cloud storage systems. It indicates that the use of PoR, access control, and collaboration mechanisms in Schema ensure data safety, confidentiality, as well as accuracy, making it an effective solution for organizations requiring safe data sharing in the cloud.

VI. CONCLUSION

In order to accomplish cloud data safety, obtainability and integrity, two strategies have been offered in this work. The first technique employs a public auditing system and a third-party authenticator called a homomorphic linear authenticator. During the auditing process, TPA ensures keenness of data without learning anything about the data. The second method uses threshold cryptography to secure data from unauthorized users while limiting access to it. Additionally, it reduces the number of keys needed for key maintenance and data decryption. The Secure Cloud Ecosystem that we advocate for employs numerous degrees of encryption to guarantee data safety and privacy. Additionally, the system uses specific hashing and salting methods, which further strengthens the entire encryption procedure.

ACKNOWLEDGEMENT

We like to thank J. Gowthamy, an assistant professor in the department of computer science and engineering at the SRM Institute of Science and Technology, for her help with the research and for her ongoing support. Her dedication to finding solutions and changing the world has been motivating. We would like to express our gratitude to the SRM Institute of Science and Technology's personnel and panel members for their assistance and unwavering support during the course of our study. Finally, we would like to express our gratitude to the parents, relatives, and friends who have supported and encouraged us throughout the work with their unwavering affection.

REFERENCES

1. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ‘‘Provable data possession at untrusted stores,’’ in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 598–609.

2. A. Juels and B. S. Kaliski, ‘‘PORs: Proofs of retrievability for large files,’’ in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), Oct. 2007, pp. 584–597.

3. H. Shacham and B. Waters, ‘‘Compact proofs of retrievability,’’ in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. Berlin, Germany: Springer, 2008, pp. 90–107.

4. C. Wang, Q. Wang, K. Ren, and W. Lou, ‘‘Privacy-preserving public auditing for data storage security in cloud computing,’’ in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9

5. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, ‘‘Enabling public auditability and data dynamics for storage security in cloud computing,’’ IEEE Trans. Parallel Distri. Syst., vol. 22, no. 5, pp. 847–859, May 2011.

6. Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, ‘‘Dynamic audit services for outsourced storages in clouds,’’ IEEE Trans. Services Comp., vol. 6, no. 2, pp. 227–238, Apr./Jun. 2013.

7. J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, ‘‘An efficient public auditing protocol with novel dynamic structure for cloud data,’’ IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.

8. B. Wang, B. Li, and H. Li, ‘‘Knox: Privacy-preserving auditing for shared data with large groups in the cloud,’’ in Proc. 10th Interfaces Conf. Appl. Crypto. Netw. Secur., 2012, pp. 507–525.

9. B. Wang, B. Li, and H. Li, ‘‘Oruta: Privacy-preserving public auditing for shared data in the cloud,’’ IEEE Trans. Cloud Comput., vol. 2, no. 1, pp. 43–56, Jan./Mar. 2014.

10. B. Wang, B. Li, and H. Li, ‘‘Panda: Public auditing for shared data with efficient user revocation in the cloud,’’ IEEE Trans. Serv. Comput., vol. 8, no. 1, pp. 92–106, Jan./Feb. 2015.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 6 –Issue 2,August 2023
Paper:71

11. T. Jiang, X. Chen, and J. Ma, ‘‘Public integrity auditing for shared dynamic cloud data with group user revocation,’’ IEEE Trans. Comput., vol. 65, no. 8, pp. 2363–2373, Aug. 2016.

12. J. Yuan and S. Yu, ‘‘Efficient public integrity checking for cloud data sharing with multi-user modification,’’ in Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM), Apr. 2014, pp. 2121–2129.

13. J. Yuan and S. Yu, ‘‘Public integrity auditing for dynamic data sharing with multiuser modification,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1717–1726, Aug. 2015.

14. G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, ‘‘Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability,’’ J. Syst. Softw., vol. 113, pp. 130–139, Mar. 2016