iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55021

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Public Auditing with Secure Team Management for Shared Data in the Cloud with Maintaining the Confidentiality

Supriya[1], Sreerambabu[2], Nimmy Pailochan[3], MohammedRiyaz[4]
[1]PG Scholar, [2]Head of the Department, [3, 4]Assistant Professor

Abstract: ***The cloud computing based public auditing data preserving refers to the process of conducting audits on data stored in the cloud to ensure its integrity, authenticity, and confidentiality are maintained. It involves allowing external entities, such as auditors or regulators, to verify the correctness of data without compromising its security.***
In this paper, we proposed a scheme for shared data that supports privacy, identity traceability and group dynamics. Cloud storage auditing is an extremely important technique for resolving the problem of ensuring the integrity of stored data in cloud storage. This scheme is secure against collusion attacks between CSPs and revoked users. This concept is for public auditing with secure group management.
This scheme is useful for the people auditing purpose in this scheme the auditing details the auditor will upload the files to the cloud and the one group management will maintain a detail in the secure management. This group contains Third party auditor one who uploads the auditing details, a Group manager one who manages the group, Group members who work in that group and Cloud Service Provider that is providing the cloud service to the group management and will maintain the data. In this, the security will be provided to the group manager and group members so that the information will be secure before as by OTP process and after the data will be secure through attribute-based encryption of the process.
Index Terms: Public auditing, Cloud storage, Cryptographic techniques, Data security, Group access control, Cloud security

I. INTRODUCTION

The public auditing is an essential mechanism for ensuring the integrity of data stored in the cloud. It allows data owners to delegate the task of data verification to an external auditor, who can independently validate the integrity of the data without accessing its content. This approach offers transparency and strengthens trust between cloud service providers and data owners. Nevertheless, public auditing alone does not address the challenges related to secure team management and collaborative data sharing within the cloud environment

Secure team management becomes crucial when multiple users or entities need to collaborate and access shared data in the cloud. Traditional access control mechanisms are insufficient to address the complexities of group-based data sharing and the need to maintain data confidentiality. Ensuring that only authorized members of a team can access specific data while preserving securely is a discouraging task, particularly when users may belong to different organisations or have varying levels of clearance.

In this paper, we propose a novel framework that combines public auditing with secure team management to address the challenges of shared data integrity and security in cloud storage systems. This primary objective of our framework is twofold: first, to enable efficient and provable public auditing for verifying the correctness of shared data, and second, to establish robust access control policies that maintain data confidentiality while facilitating secure collaboration among authorized team members. To achieve these goals, our framework leverages state-of-the-art cryptographic techniques, advanced access control models, and secure communication protocols. By integrating public auditing and secure team management, we provide a comprehensive solution that enhances the overall security and usability of cloud storage systems.

II. RELATED WORKS

A. Cloud Storage Auditing With Deduplication Support Strong Privacy Protection

In the cloud, a number of cloud storage auditing schemes were proposed. Ateniese et al. firstly proposed a notion of ‘‘Provable Data Possession’’ (PDP) and designed a publicly verifiable PDP scheme by utilizing homomorphic authenticators and random sample technique.

In this scheme, an auditor is allowed to verify the integrity of cloud data without downloading the entire data from the cloud. Juels and Kaliski constructed a model of ‘‘Proof of Retrievability’’ (PoR) and proposed a concrete scheme, which combines error-correcting codes and spot-checking technique to guarantee the retrievability and integrity of cloud data.[4]

B. Provable Data Possession

Deswarte et al. and Filho et al. provide techniques to verify that a remote server stores a file using RSA-based hash functions. Unlike other hash-based approaches, it allows a client to perform multiple challenges using the same metadata. In this protocol, communication and client storage complexity are both O(1). The limitation of the algorithm lies in the computational complexity at the server, which must exponentiate the entire file, accessing all of the file’s blocks.[6]

III. PROPOSED SYSTEM MODEL

A. Third Party Auditor Send Data

The Third-Party Auditor performs a main role in this to upload the details in the cloud database and management database. TPA collects the auditing details or data from the public for auditing purposes. Then, collects the public auditing data. TPA register and login then send data by uploading a file and can view the uploaded file and also details of the group manager.

B. Group Manager Accept Requests

The Group manager register and login then can view the uploaded file. The Group manager receives the request from a team member or group member. The request could be related to tasks, permissions, resources, or any other action that requires the manager's approval. The Group manager, after reviewing the request, The Group manager provides relevant details and context about the request, including any necessary instructions, deadlines, or supporting materials. This information helps the recipients understand the purpose, expectations, and requirements of the request.

C. Group Member Request Data

Group members register and log in. To view the uploaded data and download the data they want to get access from the group manager by an access token. A Group member initiates a request by specifying the action they want to perform or the permission they require. The Group members can send the request. This can be a single group member or multiple members, depending on the system's design. finally, when the acceptance is done by group manager will receive a secret key and download the file and also view the status.

D. Cloud Service Provider Maintains Data

Cloud service provider, login then can view the data which are uploaded then view the status and download history and data maintained. Cloud service providers typically have privacy policies and terms of service agreements that outline how customer data is handled and protected. They are responsible for complying with relevant data protection regulations and ensuring that customer data is not accessed or used inappropriately.

E. Conclusion

The systematic approach developed a public auditing with secure team management for shared data in the cloud. Dataset collection, model architectures, ethical considerations, and were key aspects of the methodology.

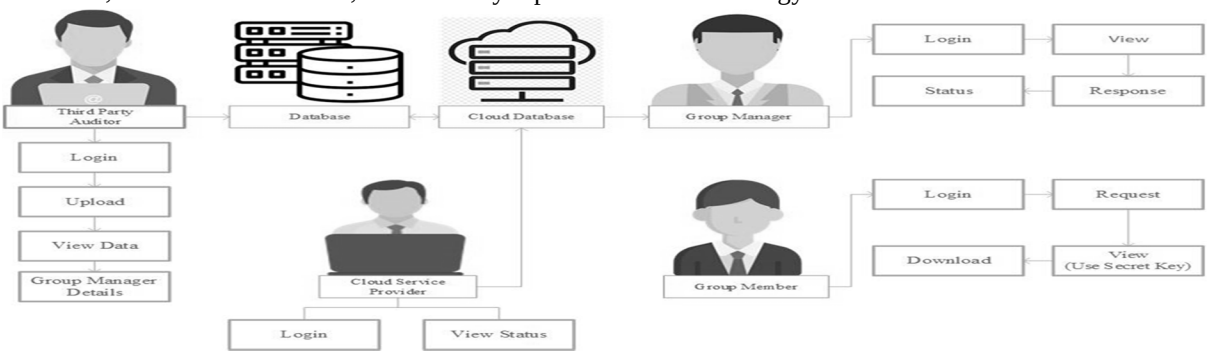


Figure 2-Architecture Diagram

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

IV. RESULTS

A. Data Privacy Performance

Privacy of the data, the data which are uploaded in the database that are secured using the encryption and decryption method. The uploaded data will upload in the encrypted form and after the secret key generation the data will changed into decrypted form.

B. Access Key Generation Performance

The group member requests the group manager to view the file, the manager accepts the request after that secret key or access key will generate, using that secret key the group member can view and download the file.

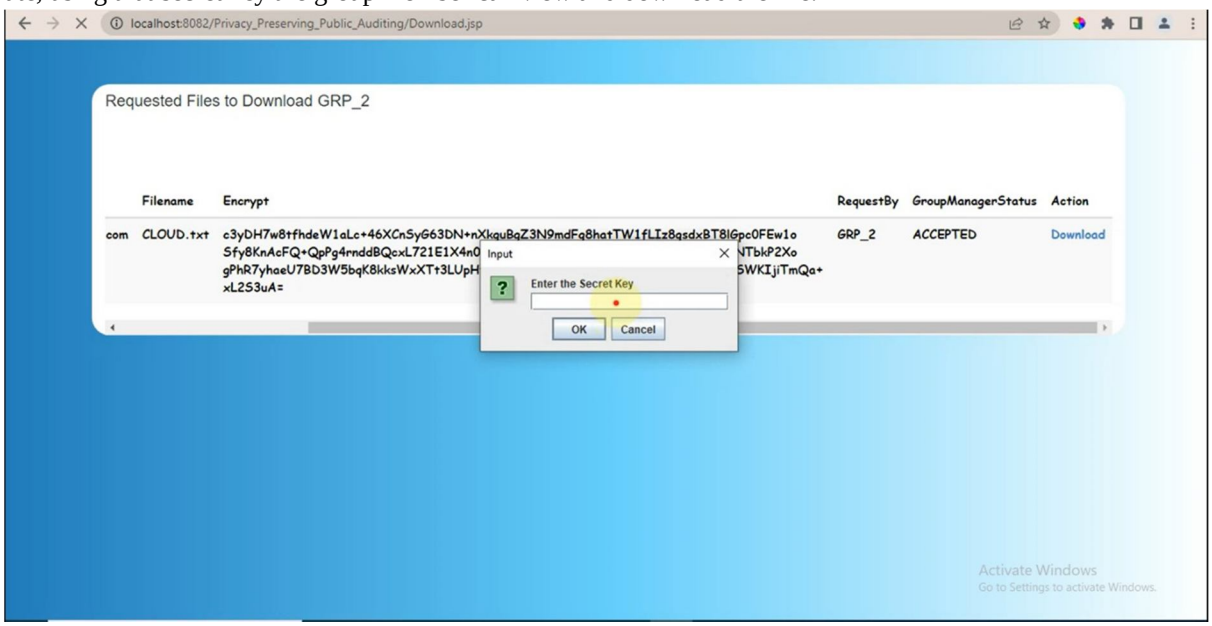


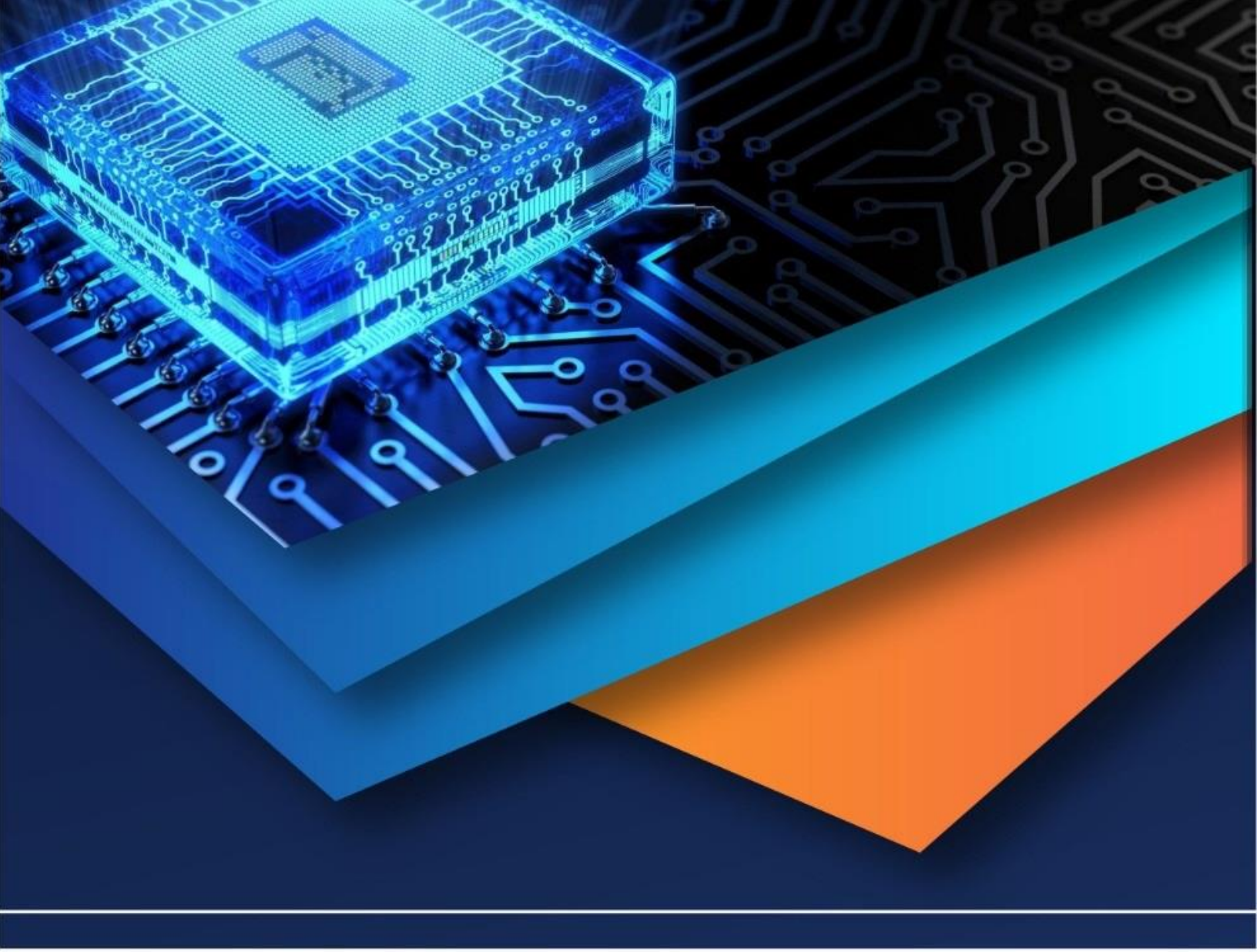
Figure 3-Sample output

V. CONCLUSION

In this project, we introduced secure group management scheme to secure the data and the need for the concept is shared, many schemes providing different functions and security levels have been proposed a scheme that supports data privacy, identity traceability, and group dynamics and claimed that their scheme is secure against collusion attacks between the CSPs and revoked users. In this the security will be provided to the group manager and group members so that the information will be secure before as by OTP process and after the data will be secure through attribute-based encryption of the process.

REFERENCES

[1] Z. Yan, L. F. Zhang, W. X. Ding, and Q. H. Zheng, "Heterogeneous data storage management with deduplication in cloud computing," IEEE Transactions on Big Data, pp. 1–1, 2017.
[2] Cong wang, Sherman s, Qian wang, Kui ren, "Privacy-preserving public auditing for secure cloud storage," International Association for Cryptologic Research
[3] Z. Yan, M. J. Wang, Y. X. Li, and A. V. Vasilakos, "Encrypted data management with deduplication in cloud computing," IEEE Cloud Computing, vol. 3, no. 2, pp. 28–35, 2016.
[4] W. Shen, Y. Su, and R. Hao, "Lightweight cloud storage auditing with deduplication supporting strong privacy protection," IEEE Access, vol. 8, pp. 44 359–44 372, 2020.
[5] Q. Zheng and S. Xu, "Secure and efficient proof of storage with deduplication," in CODASPY '12, New York, NY, USA, 2012, p. 1–12.
[6] A. Giuseppe, R. Burns, and C. Reza, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, 2007, pp. 598–609.
[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, Z. Peterson, and D. Song, "Remote data checking using provable data possession," ACM Transactions on Information and System Security, vol. 14, pp. 1– 34, 2011.
[8] Z. Wen, J. Luo, H. Chen, J. Meng, X. Li, and J. Li, "A verifiable data deduplication scheme in cloud computing," in INCOS '14, USA, 2014, p. 85–90.
[9] P. Meye, P. Raïpin, F. Tronel, and E. Anceaume, "A secure two-phase data deduplication scheme," in HPCC '14, CSS '14, ICESS '14, 2014, pp. 802–809.
[10] D. Vasilopoulos, M. Önen, K. Elkhiyaoui, and R. Molva, "Message locked proofs of retrievability with secure deduplication," in Proceedings of the 2016 ACM on Cloud Computing Security Workshop, 2016, pp. 73– 83.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY