e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 12, December 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712033

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Privacy-Preserving Data Share with Secure Group Management

Mr. M. Ajay Kumar[1], Ms. Azra Fatima[2], Ms. Afia Noorain[3], Mr. Bhokray Sohan Kumar[3]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India[1]

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India[2,3,4]

ABSTRACT: With cloud storage services, users can store their data in the cloud and efficiently access the data at any time and any location. However, when data are stored in the cloud, there is a risk of data loss because users lose direct control over their data. To solve this problem, many cloud storage auditing techniques have been studied. The proposed a public auditing scheme for shared data that supports data privacy, identity traceability, and group dynamics. In this project, we point out that their scheme is which means that, even if the cloud server has data. We then propose a new scheme that provides the same functionalities and is secure against the above attacks. Moreover, we compare the results with other schemes in terms of computation and communication costs

I. INRODUCTION

Cloud storage provides users with significant storage capacity and advantages such as a cost reduction, scalability, and convenient access to the stored data. Therefore, cloud storage that is managed and maintained by professional cloud service providers (CSPs) is widely used by many enterprises and personal clients [1]. Once the data are stored in cloud storage, the clients lose direct control over the stored data. Despite this, the CSPs must ensure that the client data are placed in cloud storage without any modification or substitution. The simplest way to achieve this is by checking the integrity of the stored data after downloading. When the capacity of the stored data is large, it is quite inefficient, and thus many methods for verifying the integrity of the data stored in the cloud without a full download have been proposed [2]_[34].These techniques are called cloud storage auditing and can be classified into private auditing and public auditing according to the subject of the integrity verification. In private auditing, verification is achieved by users who have ownership of the stored data. Public auditing is conducted by a third-party auditor (TPA) on behalf of the users to reduce their burden, and thus public auditing schemes are more widely employed for cloud storage auditing. Public auditing schemes provide various properties depending on the environment, such as privacy preservation [5]_[9], data dynamics [10]_[13], and shared data [14]_[33]. Privacy-preserving auditing is used to conduct an integrity verification while protecting data information from the TPA, and dynamic data auditing is where legitimate users are free to add, delete, or change the stored data. Shared data auditing means freely sharing data with in a legitimate user group. In this case, a legitimate user group should be defined, and user addition and revocation should be carefully considered. Recently, schemes that satisfy identity traceability, a concept that can trace the abnormal behavior of legitimate users in shared data auditing, have also been proposed.

Tian *et al.* [25] proposed a scheme that supports privacy preservation, data dynamics, and identity traceability in shared data auditing. For efficient user enrollment and revocation, the authors adopted the lazy revocation technique. Moreover, to secure the design against collusion attacks between the revoked user and server, they apply a technique in which the group manager manages messages and tag blocks generated by the revoked user to the scheme. Because the lazy-revocation technique is applied to the scheme, even ifa user is revoked, no additional operation occurs until additional changes are made to the block.

In this project, we show that Tian *et al.*'s scheme [25] is insecure against two types of attacks, a tag forgery and a proof forgery, and proposed a new scheme that provides the same functionality and is secure against the above attacks. In this scheme, a tag forgery is possible by exploiting the vulnerability in which the tag is created in a malleable way, and a proof forgery is possible by exploiting the secret value being exposed to the server when additional changes to the block occur after the user is revoked. In general, the contributions of this study can be summarized as follows

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1. We show that Tian *et al.*'s scheme [25] is insecure against two types of attacks: tag and proof forgeries .In tag forgery, we show that an attacker can create a valid tag for the modified message without knowing any secret values. In the proof forgery, we show that an attacker can create a valid proof for the given challenged message even if some stored on the cloud have been deleted.
2. We design a new public auditing scheme that is secure against the above attacks and has the same functionalities, such as privacy preservation, data dynamics, data sharing, and identity traceability. We changed the tag generation method to eliminate the malleable property and the data proof generation method to enhance the privacy preservation. We also changed the lazy revocation process to protect the secret information from the CSP and proposed an active revocation process to Flexibly apply the various environments.
3. We formally prove the security of the proposed scheme. According to the theorems, the attacker cannot generate a valid tag and proof without knowing the secret values or the original messages, respectively. We also provide comparison results with other schemes in terms of the computation and communication costs.

II. LITERATURE SURVEY

The project "Privacy-preserving public auditing for data storage security in cloud computing" by C. Wang, Q. Wang, K. Ren, and W. Lou addresses the challenge of ensuring data integrity in cloud environments while preserving user privacy. It proposes a framework that employs a trusted third-party auditor (TPA) to verify data integrity without accessing the actual data, leveraging public key-based homomorphic authenticators and random masking for privacy preservation. To enhance scalability, the framework incorporates bilinear aggregate signatures, enabling efficient handling of multiple auditing tasks in multi-user settings. The proposed system is designed to be secure, efficient, and suitable for users with limited computational resources. Extensive analysis demonstrates its robustness and practicality, making it a valuable solution for secure cloud storage systems.

The project "Identity-preserving public auditing for shared cloud data" by K. He, C. Huang, K. Yang, and J. Shi introduces an efficient and privacy-preserving framework for auditing shared data in cloud storage. The proposed scheme addresses limitations of existing methods by ensuring identity privacy through proxy re-signature, which converts user signatures into challenge user signatures, preventing the auditor from identifying individual users. It supports user revocation without requiring re-signing of data by revoked users, maintaining data integrity checks. The auditing process is optimized, with the number of pairing operations independent of the number of blocks or users involved. Additionally, the scheme supports batch auditing across multiple groups, enhancing scalability. Security analysis confirms its robustness, while simulations show lower computational and communication costs compared to existing solutions, making it highly practical for real-world applications.

The project "Shared dynamic data audit supporting anonymous user revocation in cloud storage" by Y. Zhang, C. Chen, D. Zheng, R. Guo, and S. Xu presents a secure auditing scheme for cloud storage that addresses the risks posed by collusion between revoked users and cloud service providers. The framework combines vector commitments and group signatures with anonymous revocation to ensure both data integrity and user privacy. It supports dynamic data operations by group users while enabling secure revocation of misbehaving members by the group manager. The anonymity of group signatures prevents unauthorized access to user identities, even by the cloud server. Additionally, a trusted third party can audit the server's correctness in storing modified data. Security analysis and experimental results validate the scheme's efficiency and robust protection against data breaches, making it suitable for secure and dynamic cloud storage environments.

The project "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability" by G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao proposes a novel public auditing framework that balances identity privacy and traceability in shared cloud storage. While previous schemes prioritized identity anonymity to protect users, they introduced vulnerabilities where malicious modifications could go untraced. This framework resolves the issue by introducing a group manager to generate authenticators for identity protection and maintain two lists that track the latest modifications for traceability. It employs blind signature techniques to preserve data privacy during authenticator generation. The solution is practical and efficient, with a secure and traceable auditing system tailored to

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

real-world scenarios. Security analyses and implementations demonstrate its robustness and performance, ensuring usability without compromising security.

The project "An efficient public auditing protocol with novel dynamic structure for cloud data" by J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo introduces an advanced public auditing protocol to ensure the secure storage of outsourced data in cloud environments. The protocol employs global and sampling blockless verification alongside batch auditing, enabling efficient data dynamics compared to existing solutions. A key innovation is its dynamic structure, comprising a doubly linked info table and a location array, which significantly reduces computational and communication overheads. Security analysis confirms the protocol's robustness, while numerical and experimental evaluations demonstrate its practical efficiency, making it a valuable tool for secure and scalable cloud storage management.

The project "Privacy-preserving public auditing for shared data in the cloud" by B. Wang, B. Li, and H. Li addresses the challenge of maintaining data integrity and contributor privacy in shared cloud storage. It introduces a public auditing mechanism that allows a third-party verifier to check the correctness of shared data without accessing the data itself or revealing group members' identities. To efficiently manage group dynamics, such as user addition and revocation, the framework employs a secure proxy re-signature scheme that outsources signature updating operations to the cloud, minimizing computational overhead for users. Experimental results validate the scheme's efficiency and scalability, making it a practical solution for dynamic group scenarios in cloud environments.

III. METHODOLOGY

The framework employs advanced techniques such as secure multi-party computation, homomorphic encryption, and differential privacy to ensure robust privacy-preserving data processing and sharing. These cryptographic techniques safeguard data confidentiality and integrity during computations and transmissions. Access control mechanisms enforce strict authorization policies, ensuring that only legitimate users can access or modify the data. Group management techniques facilitate dynamic user operations, such as additions and revocations, while maintaining privacy and security. Furthermore, scalability and performance optimization strategies, including parallel processing and efficient data structures, ensure the framework remains effective and responsive even in large-scale and high-demand environments. Together, these components create a secure, efficient, and scalable system for privacy-preserving applications.

DISADVANTAGES OF EXISTING SYSTEM:

- No Security
- It's hard to communicate between group manager and the group user.
- No Access data anybody can attacks a file.

PROPOSED SYSTEM

- In this project, we point out that their scheme is insecure, which means that, even if the cloud server has a that the server had accurately stored the data.
- We then propose a newscheme that provides the same functionalities and is secure against the above attacks.
- Once the data are stored in cloud storage, the clients lose direct control over the stored. Despite this, the CSPs must ensure that the client data are placed in cloud storage without any modification.

ADVANTAGES OF PROPOSED SYSTEM:

- Stronger authentication
- Easy communication between group manager and group user.
- Any user can access the shared data

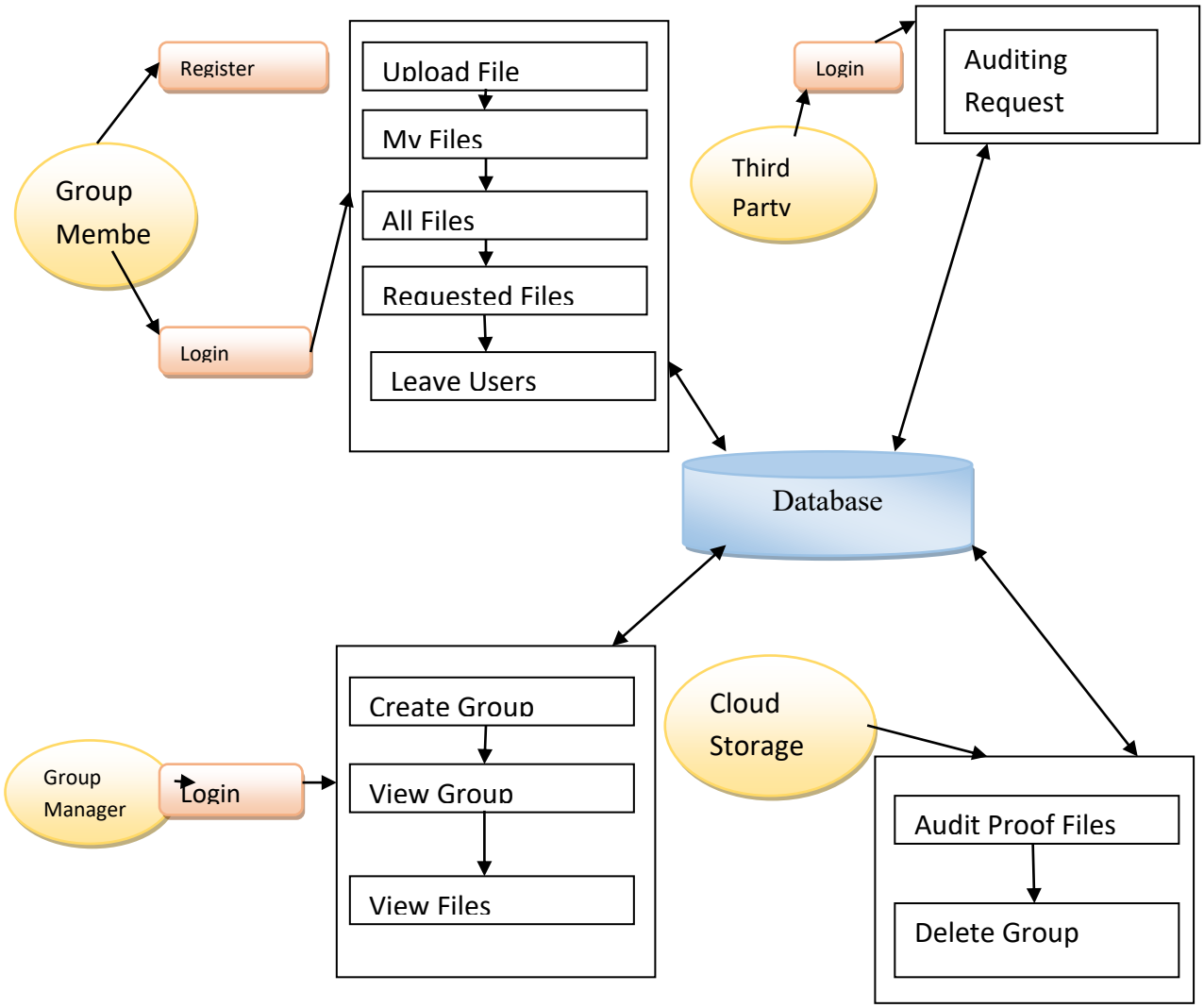
© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712033

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

SYSTEM ARCHITECTURE:



MODULES:

1. User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

3. Group Manager

The Group manager can also login. Group manager can a create a group. Group manager can view a group member. Group manager can see a files. Group manager can also have a delete groups.

4. Third Party Auditor

Third party can login. After login third party can have an auditing request.

5. Cloud Storage Server

Cloud storage server can a audit proof files. The cloud storage server can also a delete a group member.

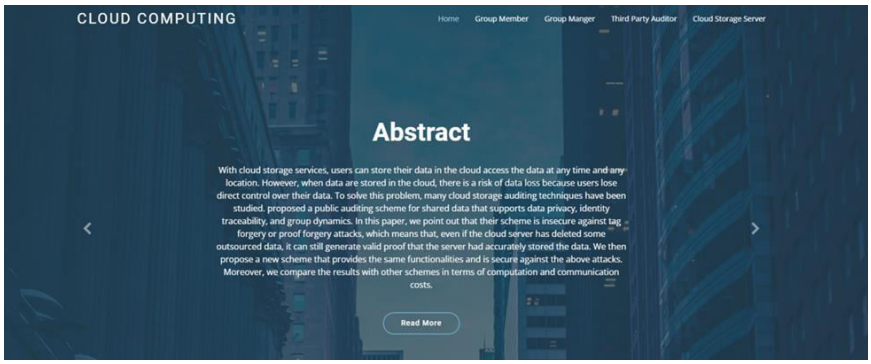
© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712033

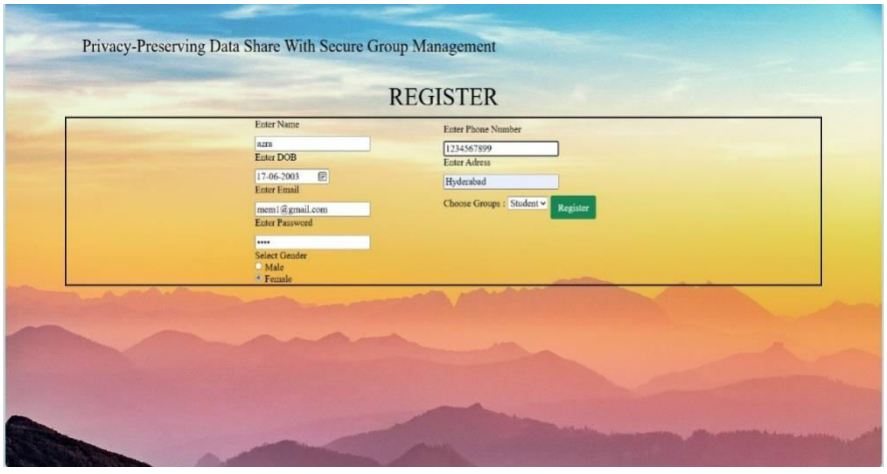
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. EXPERIMENTAL RESULTS



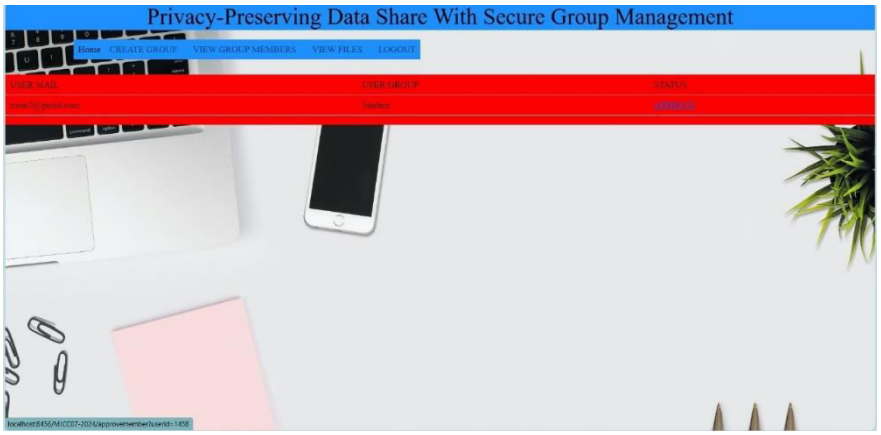


© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712033

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

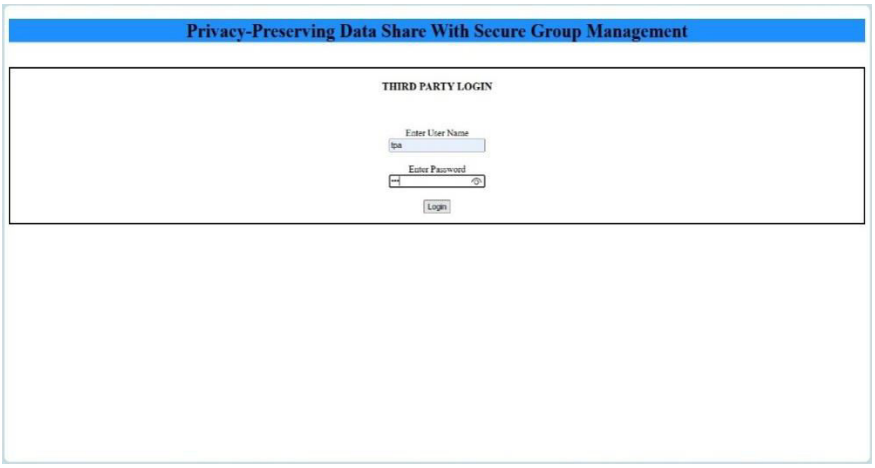
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

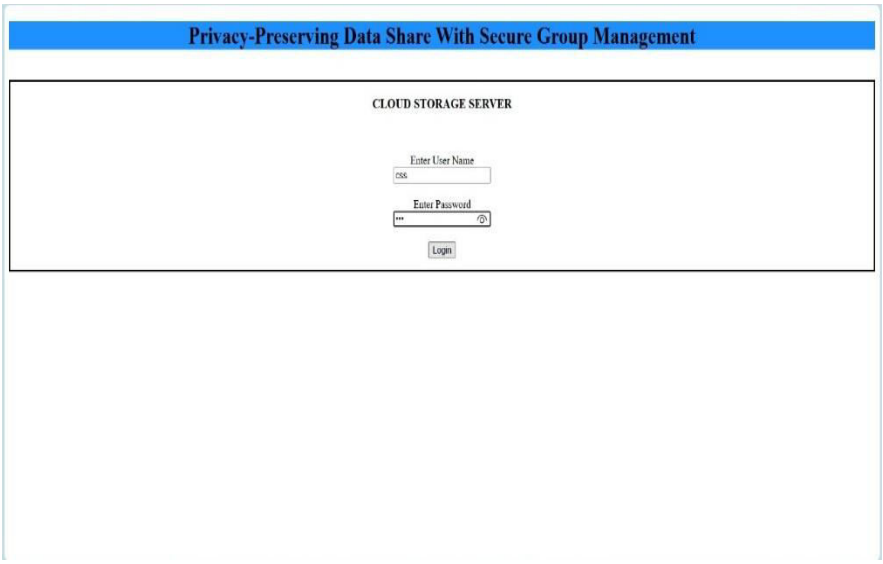


ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

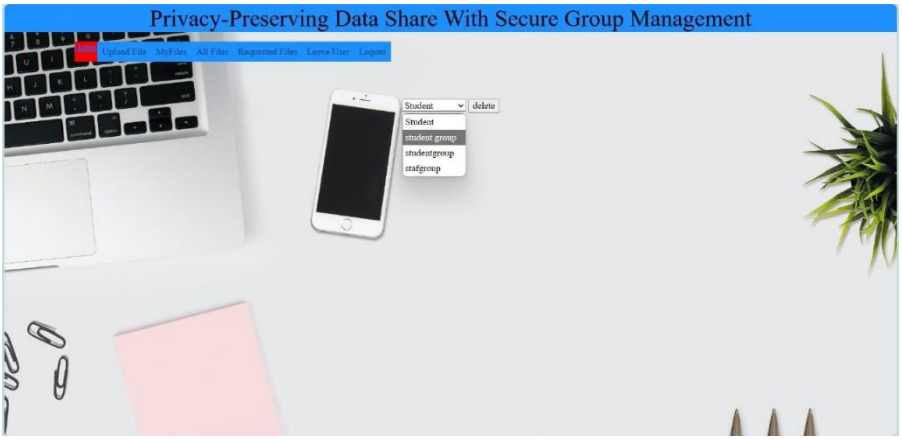




ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



V. CONCLUSION

Cloud storage auditing is an extremely important techniquefor resolving the problem of ensuring the integrity of storeddata in cloud storage. Because the need for the conceptis shared, many schemes providing different functions andsecurity levels have been proposed. In 2019, Tian *et al.* [25]proposed a scheme that supports data privacy, identity traceability,and group dynamics and claimed that their schemeis secure against collusion attacks between the CSPs andrevoked users. In this project, we showed in their scheme thata tag can be forged from a valid message and tag pair withoutknowing any secret values. We also showed that a proof canbe forged by a collusion attack, even if some challengedmessages have been deleted. We then proposed a new schemethat is secure against the above attacks while providing thesame functionality as their approach. We also provided formalsecurity proofs and an analysis of the computation costs ofboth schemes.

VI. FUTURE ENHANCEMENT

The Future Enhancement of project is we can improve more security to the group members to approve. it is sufficient to show that a valid poof can be simulated without any message block information in the random oracle model.

REFERENCES

[1] (Apr. 2021). Cloud Storage-Global Market Trajectory and Analytics. [Online]. Available: https://www.researchandmarkets.com//reports/5140992/cloud-storage-global-market-trajectory-and.
[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, ``Provable data possession at untrusted stores," in Proc. 14thACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 598_609.
[3] A. Juels and B. S. Kaliski, ``PORs: Proofs of retrievability for large _les,"in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), Oct. 2007,pp. 584_597.
[4] 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.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou, ``Privacy-preserving publicauditing for data storage security in cloud computing," in Proc. IEEEINFOCOM, Mar. 2010, pp. 1_9.
[6] Z. Hao, S. Zhong, and N. Yu, ``A privacy-preserving remote data integritychecking protocol with data dynamics and public verifiability," IEEETrans. Knowl. Data Eng., vol. 23, no. 9, pp. 1432_1437, Sep. 2011.
[7] K. Yang and X. Jia, ``An ef_cient and secure dynamic auditing protocolfor data storage in cloud computing," IEEE Trans. Parallel Distrib. Syst.,vol. 24, no. 9, pp. 1717_1726, Sep. 2013.
[8] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ``Privacypreservingpublic auditing for secure cloud storage," IEEE Trans. Comput.,vol. 62, no. 2, pp. 362_375, Feb. 2013.
[9] K. He, C. Huang, K. Yang, and J. Shi, ``Identity-preserving public auditingfor shared cloud data," in Proc. IEEE 23rd Int. Symp. Quality Service(IWQoS), Jun. 2015, pp. 159_164.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[10] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, ``Dynamic provabledata possession," in Proc. 16th ACM Conf. Comput. Commun. Secur.(CCS), New York, NY, USA, 2009, pp. 213_222.
[11] Q.Wang, C.Wang, K. Ren,W. Lou, and J. Li, ``Enabling public auditabilityand data dynamics for storage security in cloud computing," IEEE Trans.Parallel Distrib. Syst., vol. 22, no. 5, pp. 847_859, May 2011.
[12] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, ``Dynamicaudit services for outsourced storages in clouds," IEEE Trans. ServicesComput., vol. 6, no. 2, pp. 227_238, Apr./Jun. 2013.
[13] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, ``An ef_cient publicauditing protocol with novel dynamic structure for cloud data," IEEETrans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402_2415, Oct. 2017.
[14] B. Wang, B. Li, and H. Li, ``Knox: Privacy-preserving auditing for shareddata with large groups in the cloud," in Proc. 10th Interfaces Conf. Appl.Crypto. Netw. Secur., 2012, pp. 507_525.
[15] B. Wang, B. Li, and H. Li, ``Oruta: Privacy-preserving public auditingfor shared data in the cloud," IEEE Trans. Cloud Comput., vol. 2, no. 1,pp. 43_56, Jan./Mar. 2014.
[16] 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.
[17] T. Jiang, X. Chen, and J. Ma, ``Public integrity auditing for shared dynamiccloud data with group user revocation," IEEE Trans. Comput., vol. 65,no. 8, pp. 2363_2373, Aug. 2016.
[18] J. Yuan and S. Yu, ``Efficient public integrity checking for cloud data sharingwith multi-user modi_cation," in Proc. IEEE Conf. Comput. Commun.(IEEE INFOCOM), Apr. 2014, pp. 2121_2129.
[19] 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.
[20] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, ``Enabling publicauditing for shared data in cloud storage supporting identity privacy andtraceability," J. Syst. Softw., vol. 113, pp. 130_139, Mar. 2016.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com