IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Double Blind Peer Reviewed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305564 |

Secure Group Management Enables Privacy Preserving Public Auditing for Shared Cloud Data

C Uma Sree[1], Dr. K.V.Uma Maheswari[2], Dr.C.Gulzar[3]

U.G. Student, Department of Computer Science Engineering, Dr. K. V. Subba Reddy Institute of Technology, Andhra Pradesh, India [1]

Associate Professor, Department of Computer Science Engineering, Dr. K. V. Subba Reddy Institute of Technology, Andhra Pradesh, India[2]

Head of Department, Department of Computer Science Engineering, Dr. K. V. Subba Reddy Institute of Technology, Andhra Pradesh, India[3]

ABSTRACT: With distributed storage administrations, clients can store their information in the cloud and productively access the information whenever and any area. Be that as it may, when information are put away in the cloud, there is a gamble of information misfortune since clients lose direct command over their information. To take care of this issue, many distributed storage evaluating methods have been examined. In 2019, Tian et al. proposed a public inspecting plan for shared information that upholds information protection, character discernibility, and collective vibes. In this paper, we call attention to that their plan is uncertain against label imitation or evidence falsification assaults, and that truly intends that, regardless of whether the cloud server has erased a few rethought information, it can in any case create substantial verification that the server had precisely put away the information. We then, at that point, propose a new conspire that gives similar functionalities and is secure against the above assaults. Besides, we contrast the outcomes and different plans as far as calculation and correspondence costs.

KEYWORDS: Cloud Computing, Cloud Service Providers.

I. INTRODUCTION

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 _les. 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 within a legitimate user group. In this

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Double Blind Peer Reviewed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305564 |

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 if a user is revoked, no additional operation occurs until additional changes are made to the block.

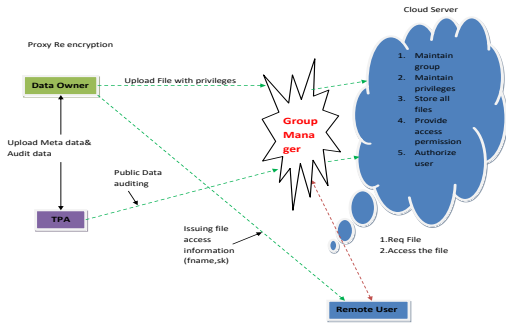
In this paper, we show that Tian et al.'s scheme [25] is insecure against two types of attacks, a tag forgery and a proof forgery, and proposed a new scheme that provides the same functionality and is secure against the above attacks. In this scheme, a tag forgery is possible by exploiting the vulnerability 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 V

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 _les 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.

The rest of this paper is organized as follows. In Section II, we introduce the background, and in Section III, we review Tian et al.'s scheme [25].We present our detailed scheme for public auditing in Section IV, and provide the security and efficiency of our scheme in Section V. Finally, we conclude this paper in Section VI.

.

Architecture Diagram



|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Double Blind Peer Reviewed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305564 |

II. RELATED WORK

Title: "Protection Saving Public Examining for Imparted Cloud Information To Get Gathering The executives: A Writing Review"

1. Title: Protection Saving Public Inspecting for Secure Distributed storage through Gathering Based Validation Convention
- Creator: Qiuliang Xu, Hai Jin, Xiaofeng Chen, Kim-Kwang Raymond Choo
- Depiction: This paper presents a protection safeguarding public reviewing plan for secure distributed storage utilizing a gathering based verification convention. It centers around guaranteeing the respectability and legitimacy of information put away in the cloud while safeguarding the protection of clients. The proposed conspire utilizes bunch based mark and intermediary re-encryption strategies to accomplish effective inspecting and secure information dividing between bunch individuals.

2. Title: Improved Security Safeguarding Public Examining Plan for Distributed storage
- Creator: Chunhua Su, Yanmin Zhu, Geyong Min, Qian Wang, Laurence T. Yang
- Portrayal: This paper presents an upgraded protection saving public evaluating plan for distributed storage, which refines existing techniques by tending to different security and protection concerns. The plan uses homomorphic direct authenticators and irregular covering procedures to permit an outsider reviewer to confirm the uprightness of rethought information without learning any data about the information content.

3. Title: PPACloud: Protection Saving Examining for Shared Information in Distributed storage
- Creator: Hui Zhu, Wenhai Sun, Zhibo Wang, Jin Li, Huanguo Zhang
- Depiction: This paper proposes PPACloud, a security saving reviewing plan intended for shared information in distributed storage conditions. PPACloud utilizes homomorphic authenticators and intermediary re-encryption procedures to empower proficient and secure evaluating of shared information while safeguarding client protection. It likewise presents a powerful gathering the executives instrument to proficiently deal with client disavowal and expansion.

4. Title: Effective and Protection Safeguarding Public Reviewing Plan for Cloud Information
- Creator: Xinyi Huang, Jingwei Li, Jin Li, Hui Li
- Portrayal: This paper presents an effective and protection saving public reviewing plan for cloud information, zeroing in on the two information trustworthiness and client security. The proposed plot uses progressive personality based encryption and homomorphic authenticators to accomplish effective inspecting and secure information sharing. It likewise acquaints a clever disavowal component with handle client bunch changes without compromising security or effectiveness.

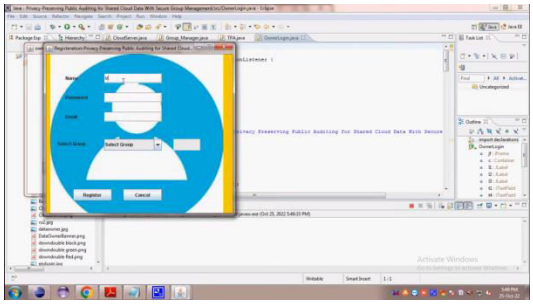
5. Title: Security Protecting Public Evaluating for Imparted Information to General vibe in Distributed storage
- Creator: Jiguo Yu, Yilei Wang, Jin Li, Chunfu Jia, Yong Jiang
- Portrayal: This paper proposes a security protecting public examining plan for imparted information to dynamic gathering the board in distributed storage. The plan utilizes a mix of trait based encryption and intermediary re-encryption procedures to guarantee information protection and honesty. It likewise presents a unique gathering component that permits proficient client denial and expansion while keeping up with information security and auditability.

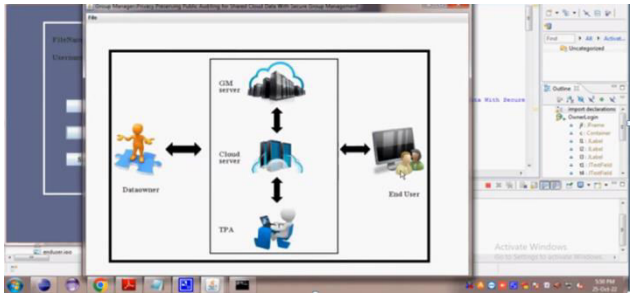
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Double Blind Peer Reviewed Journal |

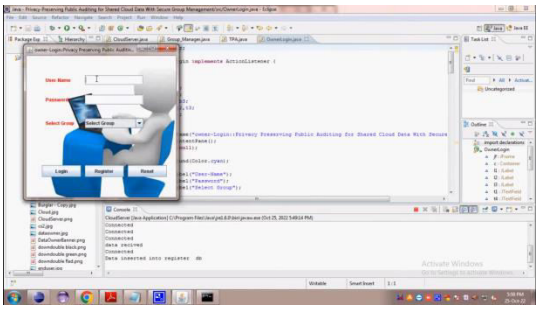
|| Volume 13, Issue 5, May 2024 ||

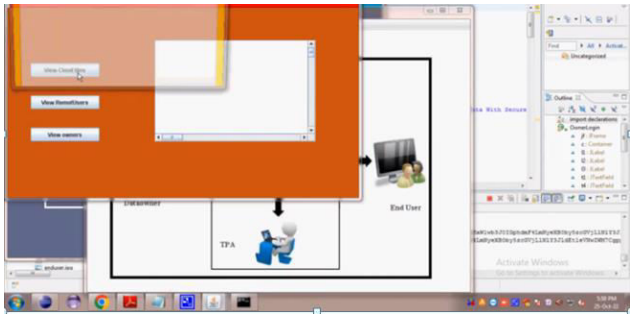
| DOI:10.15680/IJIRSET.2024.1305564 |

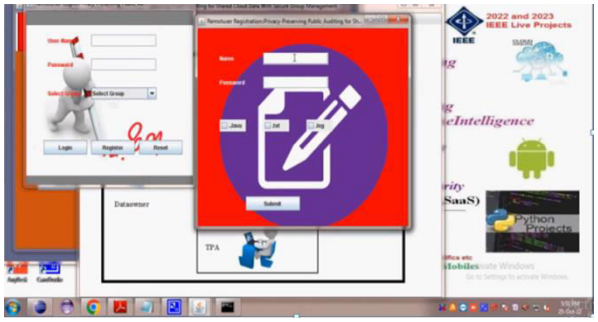
III. EXPERIMENTAL RESULTS

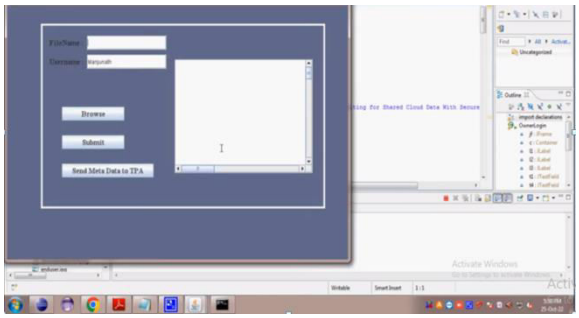


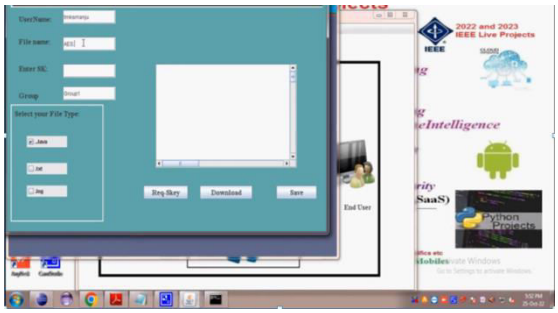


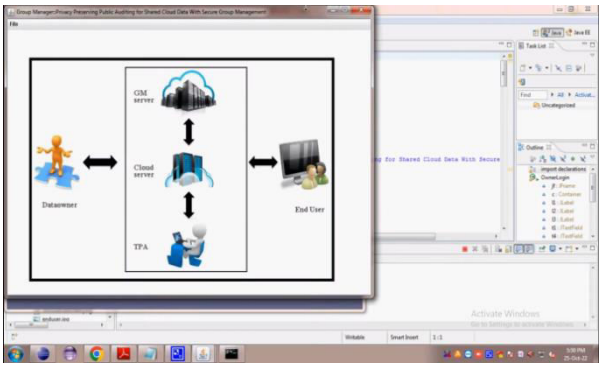








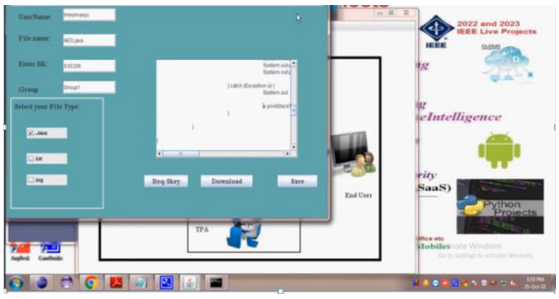


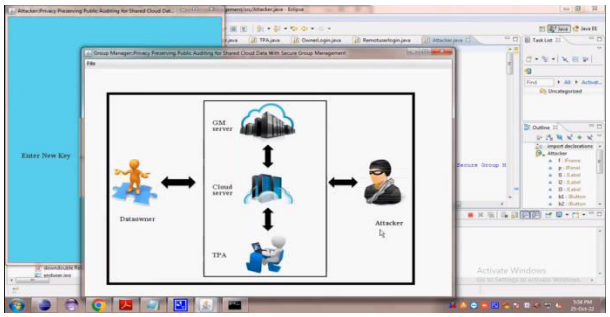


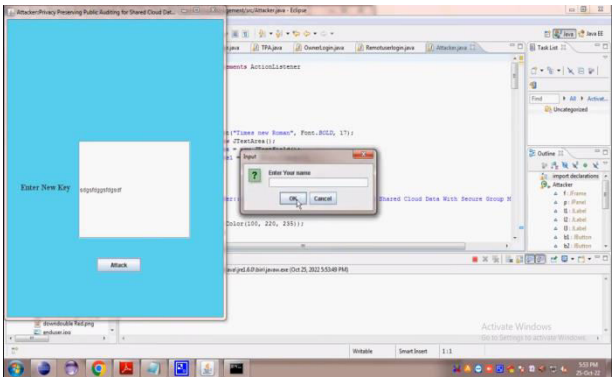
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Double Blind Peer Reviewed Journal |

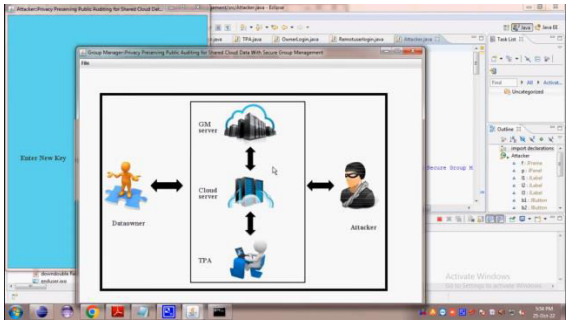
|| Volume 13, Issue 5, May 2024 ||

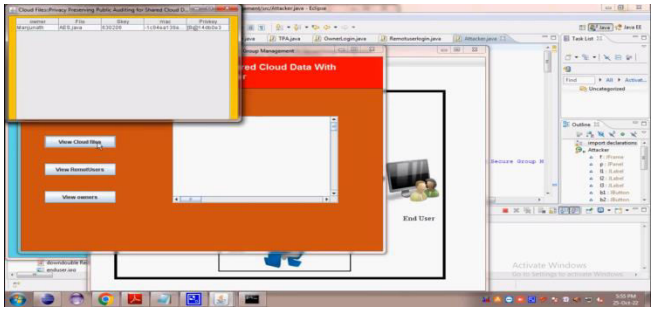
| DOI:10.15680/IJIRSET.2024.1305564 |











IV. CONCLUSION

One promising bearing for future examination is the improvement of proficiency and adaptability. Many existing plans depend on computationally serious cryptographic methods, for example, homomorphic encryption and zero-information confirmations, which can be asset concentrated, particularly for huge scope frameworks. Future work could zero in on growing more proficient calculations or utilizing equipment speed increase strategies to work on the presentation of examining processes while keeping up serious areas of strength for with ensures.

One more critical viewpoint for future investigation is the combination of cutting edge access control systems. While existing plans frequently give instruments to bunch the board, they might need fine-grained admittance control capacities. Future examination could zero in on creating plans that empower more granular command over admittance to shared information, permitting managers to characterize and uphold complex access arrangements in light of qualities or jobs.

Besides, upgrading versatility to assaults and guaranteeing heartiness against different dangers is fundamental. Future work could include investigating new cryptographic natives or planning plans versatile to cutting edge goes after, for example, intrigue assaults or insider dangers. Furthermore, examination could

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Double Blind Peer Reviewed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305564 |

zero in on creating procedures to distinguish and moderate information altering or spillage endeavors, accordingly improving the general security stance of the reviewing framework.

Interoperability and similarity across various cloud stages and capacity frameworks address one more region for future work. As distributed computing conditions become progressively heterogeneous, with clients using different cloud suppliers or half breed cloud designs, there is a developing requirement for examining plans that can consistently work across assorted conditions. Future examination could zero in on creating normalized conventions or similarity layers to work with interoperability and guarantee predictable reviewing across various stages.

Also, ease of use and client experience are basic variables for the reception of examining arrangements. Future work could investigate easy to understand connection points and association ideal models to improve on the evaluating system for end-clients and reviewers. Moreover, teaching clients about the significance of protection safeguarding reviewing and giving apparatuses to overseeing inspecting boundaries could assist with expanding client mindfulness and acknowledgment of such frameworks.

At last, taking into account the advancing administrative scene and security prerequisites, future work could include adjusting examining plans with arising norms and guidelines, like the Overall Information Insurance Guideline (GDPR) or the California Buyer Protection Act (CCPA).

REFERENCES

[1] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 1-9,

[2] Z. Hao, S. Zhong and N. Yu, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability," in IEEE Transactions on Knowledge and Data Engineering, vol. 23, no. 9, pp. 1432-1437, Sept. 2011, doi: 10.1109/TKDE.2011.62.

[3] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717-1726, Sept. 2013, doi: 10.1109/TPDS.2012.278.

[4] C. Wang, S. S. M. Chow, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," in IEEE Transactions on Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013, doi: 10.1109/TC.2011.245.

[5] K. He, C. Huang, K. Yang and J. Shi, "Identity-preserving public auditing for shared cloud data," 2015 IEEE 23rd International Symposium on Quality of Service (IWQoS), Portland, OR, USA, 2015, pp. 159-164, doi: 10.1109/IWQoS.2015.7404727.

[6] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011, doi: 10.1109/TPDS.2010.183.

[7] 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," in IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227-238, April-June 2013, doi: 10.1109/TSC.2011.51.

[8] J. Shen, J. Shen, X. Chen, X. Huang and W. Susilo, "An Efficient Public Auditing Protocol With Novel Dynamic Structure for Cloud Data," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 2402-2415, Oct. 2017, doi: 10.1109/TIFS.2017.2705620.

[9] B. Wang, B. Li and H. Li, "Oruta: privacy-preserving public auditing for shared data in the cloud," in IEEE Transactions on Cloud Computing, vol. 2, no. 1, pp. 43-56, Jan.-March 2014, doi: 10.1109/TCC.2014.2299807.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Double Blind Peer Reviewed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305564 |

[10] B. Wang, B. Li and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," in IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92-106, Jan.-Feb. 2015, doi: 10.1109/TSC.2013.2295611.

[11] T. Jiang, X. Chen and J. Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation," in IEEE Transactions on Computers, vol. 65, no. 8, pp. 2363-2373, 1 Aug. 2016, doi: 10.1109/TC.2015.2389955.

[12] J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, Toronto, ON, Canada, 2014, pp. 2121-2129, doi: 10.1109/INFOCOM.2014.6848154.

[13] J. Yuan and S. Yu, "Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1717-1726, Aug. 2015, doi: 10.1109/TIFS.2015.2423264.

[14] A. Fu, S. Yu, Y. Zhang, H. Wang and C. Huang, "NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users," in IEEE Transactions on Big Data, vol. 8, no. 1, pp. 14-24, 1 Feb. 2022, doi: 10.1109/TBDATA.2017.2701347.

[15] W. Shen, J. Qin, J. Yu, R. Hao and J. Hu, "Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 331-346, Feb. 2019, doi: 10.1109/TIFS.2018.2850312.

[16] Y. Zhang, C. Chen, D. Zheng, R. Guo and S. Xu, "Shared Dynamic Data Audit Supporting Anonymous User Revocation in Cloud Storage," in IEEE Access, vol. 7, pp. 113832-113843, 2019, doi: 10.1109/ACCESS.2019.2935180.

[17] Y. Xu, L. Ding, J. Cui, H. Zhong and J. Yu, "PP-CSA: A Privacy-Preserving Cloud Storage Auditing Scheme for Data Sharing," in IEEE Systems Journal, vol. 15, no. 3, pp. 3730-3739, Sept. 2021, doi: 10.1109/JSYST.2020.3018692.

[18] Y. Zhang, J. Yu, R. Hao, C. Wang and K. Ren, "Enabling Efficient User Revocation in Identity-Based Cloud Storage Auditing for Shared Big Data," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 3, pp. 608-619, 1 May-June 2020, doi: 10.1109/TDSC.2018.2829880.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details