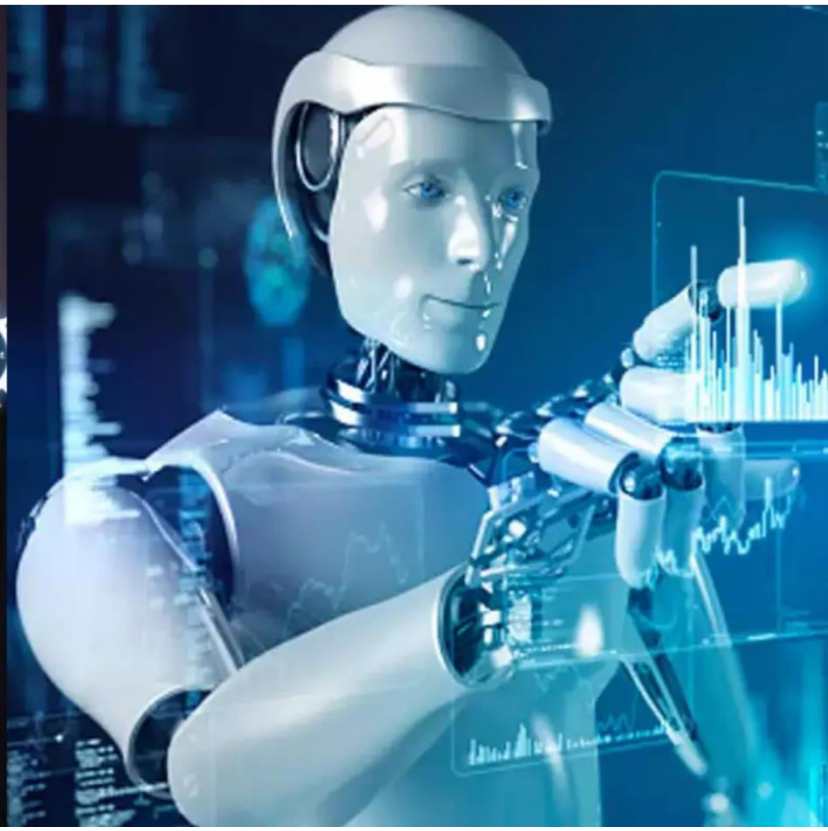
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

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

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



Impact Factor: 9.935

Volume 15, Issue 6, June 2026

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

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506095|

A Secure and Efficient Certificateless Public Auditing Scheme for Cloud Data Integrity Verification

Gore Arti, Kasare Ankita, Hajare Rushikesh, Prof. S.A. Dhage

U.G. Student, Department of Computer Engineering, VACOE Engineering College, Ahilyanagar, India

U.G. Student, Department of Computer Engineering, VACOE Engineering College, Ahilyanagar, India

U.G. Student, Department of Computer Engineering, VACOE Engineering College, Ahilyanagar, India

Associate Professor, Department of Computer Engineering, VACOE Engineering College, Ahilyanagar, India

ABSTRACT: With the rapid growth of cloud computing, cloud storage has become a popular platform for storing and sharing data among multiple users. However, ensuring the integrity and security of group-shared data in cloud environments has become a major challenge. Traditional integrity verification methods based on Public Key Infrastructure (PKI) require complex certificate management, which increases administrative overhead and system complexity.

To overcome these limitations, this project proposes a certificate-less public integrity checking mechanism for secure cloud storage. The proposed approach uses certificateless cryptography to eliminate the need for certificate management while still maintaining strong security. This mechanism allows authorized users or third-party auditors to verify the integrity of shared data stored in the cloud without accessing the actual data, thereby preserving data confidentiality.

The system also supports dynamic group management, enabling users to join or leave the group without affecting the integrity verification process. This improves flexibility and usability in collaborative environments. Experimental results demonstrate that the proposed scheme reduces computational and storage overhead compared to traditional PKI-based methods while maintaining high levels of security and efficiency.

Therefore, the proposed certificateless approach provides a scalable, secure, and efficient solution for public integrity verification in cloud-based collaborative data storage systems.

KEYWORDS: Cloud Storage Security, Group Shared Data, Certificate-less Cryptography, Public Integrity Checking, Data Integrity Verification.

I. INTRODUCTION

Cloud computing has significantly transformed the way organizations and user groups store, share, and collaborate on data. Cloud storage services allow multiple users to access and modify shared information from any location, providing advantages such as scalability, flexibility, and cost efficiency.

Due to these benefits, cloud storage has become widely adopted by collaborative environments including businesses, educational institutions, and research communities. Any unauthorized modification of data, whether intentional or accidental, can compromise data reliability and lead to serious consequences in applications where data accuracy is critical.

Public Key Infrastructure (PKI) is commonly used in cloud environments to support user authentication and data integrity verification. PKI-based systems utilize digital certificates to establish trust between users and the data they access, ensuring that only authorized individuals can modify or verify stored information. Although PKI provides effective security mechanisms, it introduces considerable administrative overhead due to certificate generation,

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

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506095|

distribution, and management. These challenges become more complex in group-sharing environments where users frequently join or leave the system. Managing certificates for multiple members also increases computational and storage costs, which limits the scalability and efficiency of PKI- based integrity verification in dynamic collaborative settings.

To overcome these limitations, this project proposes a certificateless public integrity-checking protocol specifically designed for group-shared data stored in cloud environments. The proposed approach eliminates the need for digital certificates by utilizing certificateless cryptography. This mechanism allows authorized group members or third-party auditors to verify the integrity of stored data without accessing the actual content, thereby preserving data confidentiality.

The proposed protocol is also designed to support dynamic group management. New members can be added and existing members can be removed without affecting the integrity verification process or requiring the regeneration of group keys. This capability makes the system more practical for real-world collaborative applications where group membership frequently changes. Additionally, the protocol ensures privacy-preserving integrity verification, allowing auditors to confirm data correctness without exposing the original data, which is particularly important in cloud environments where protecting sensitive information is essential.

This research contributes to the field of cloud security by presenting an efficient, secure, and scalable certificateless integrity-checking mechanism for group data sharing. Experimental evaluation demonstrates that the proposed scheme achieves performance comparable to or better than conventional PKI-based approaches. Therefore, the proposed method offers a practical solution for improving trust, security, and efficiency in modern cloud-based collaborative storage systems.

II. LITERATURE SURVEY

1. Certificate-Less Public Integrity Checking of Cloud Data Using Cryptographic Techniques (S. S. Rao, V. R. Patil, R. S. Kumar, 2018)
This research presents a certificateless cryptographic model developed to support public verification of data integrity in cloud storage systems. The framework applies hash-based signature methods along with a secure key management strategy, thereby removing the requirement for traditional digital certificates. By eliminating certificate dependency, the system simplifies the authentication procedure and reduces administrative overhead. Experimental evaluations demonstrate that the proposed approach is scalable and capable of supporting large-scale cloud environments while maintaining strong security and reliable integrity verification.

2. Efficient Integrity Checking in Cloud Storage: A Certificate-Free Approach (L. Zhang, Y. Zhang, D. Wu, 2017)
The authors introduce a certificate-free integrity verification scheme that allows public auditing of cloud data without relying on conventional Public Key Infrastructure (PKI). The method employs homomorphic signature techniques and cryptographic proof mechanisms to perform efficient and privacy-preserving integrity verification. This approach significantly reduces both computational and storage overhead, making it more suitable for practical cloud storage applications. The study concludes that the certificate-free model offers security levels comparable to, or better than, traditional PKI-based methods while improving overall resource efficiency.

3. Scalable Integrity Auditing for Group Shared Data in Cloud Storage (J. Wang, L. Zhang, X. Liu, 2020)
This study proposes a scalable certificateless integrity auditing framework designed for cloud environments where data is shared among multiple users. The system supports dynamic group membership, enabling users to join or leave without affecting the integrity verification process. In addition, the framework incorporates an efficient key management mechanism that simplifies access control in collaborative settings. Experimental findings indicate that the proposed approach provides both scalability and adaptability, making it suitable for organizations that manage large and frequently updated datasets in cloud storage.

4.Privacy-Preserving Public Integrity Verification for Cloud Data Without Certificates (M. Ahmed, S. Kumar, A. Jain, 2019)
This paper introduces a privacy-preserving certificateless auditing mechanism aimed at verifying cloud data integrity.

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

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506095|

The proposed system combines cryptographic hash functions with zero-knowledge proof techniques to ensure that the integrity verification process does not expose the actual data during third-party audits. By protecting sensitive information while performing integrity checks, the approach enhances data privacy in cloud environments. The results demonstrate that this method is effective for group-shared cloud systems and serves as a secure and efficient alternative to traditional certificate-based verification techniques.

III. METHODOLOGY

The proposed Certificateless Public Auditing System for Cloud Data Integrity consists of five major entities: User (Data Owner), Key Generation Center (KGC), Cloud Service Provider (CSP), Third-Party Auditor (TPA), and Group Members. These components interact with each other to maintain data confidentiality, integrity, and efficient auditing while eliminating the need for traditional digital certificates.

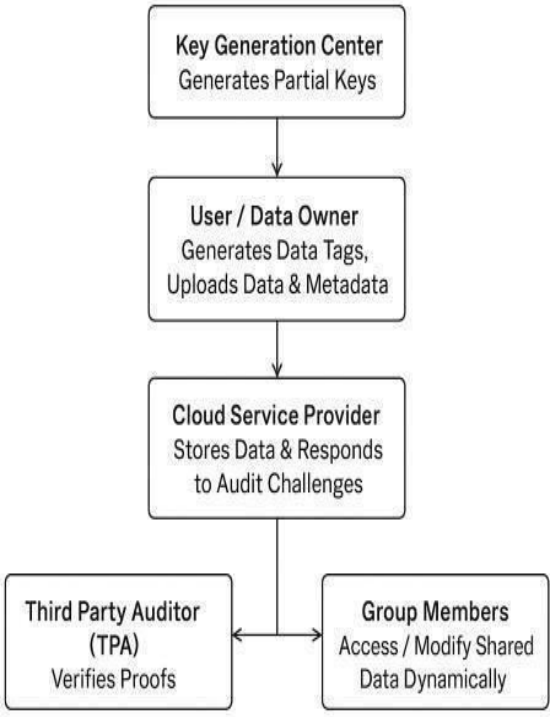


Fig.1

[1] User/ Data Owner

The The data owner is responsible for uploading files to the cloud storage system. Before uploading, the data is divided into multiple blocks, and cryptographic algorithms are applied to generate integrity verification metadata. Each data block is signed using a certificateless signature technique. The user then sends the encrypted data along with the corresponding verification tags to the Cloud Service Provider (CSP) for storage.

[2] Cloude Service Provider(CSP)

The Cloud Service Provider is responsible for storing the user's data and the associated integrity verification metadata. When an audit request is initiated, the CSP responds to the challenge issued by the Third-Party Auditor (TPA). It generates a proof of data possession (PDP) to demonstrate that the stored data remains intact and has not been altered, without exposing the actual content of the data.

[3] Third-Party Auditor

The Third-Party Auditor performs public integrity verification on behalf of users. It sends random challenge requests to the CSP and verifies the correctness of the responses using cryptographic computations. During this process, the TPA cannot access or derive the original data, which ensures that the auditing mechanism remains privacy-preserving.

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

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506095|

[4] Group Members

The In collaborative cloud environments, multiple users may share and manage the same dataset. The proposed system supports dynamic group management, allowing members to join or leave the group without requiring certificate reissuance or revocation. Each group member can independently verify the integrity of the shared data or delegate the verification process to the TPA when necessary.

Working Procedure of the Proposed System

1. System Initialization:

The Key Generation Center (KGC) initializes the system by defining the necessary cryptographic parameters and distributing partial private keys to registered users.

2. Key Generation:

Each user generates their complete public and private key pair by combining their personal secret value with the partial private key provided by the KGC.

3. Data Uploade:

Before uploading data to the cloud, the user divides the file into several blocks and generates verification tags for each block. The data along with its integrity metadata is then uploaded to the Cloud Service Provider (CSP).

4. Audit Challenge:

The Third-Party Auditor (TPA) initiates the integrity verification process by sending a random challenge request to the CSP.

5. Proof Generation:

Upon receiving the challenge, the CSP calculates a proof of data possession using the stored data blocks and their corresponding verification metadata. This proof is then sent back to the TPA.

6. Verification Process:

The TPA validates the received proof using the user's public key. If the verification is successful, the system confirms that the stored data remains intact and has not been modified.

7. Dynamic Group Management:

When new members join or existing members leave the group, only minor updates to the verification metadata are required. This mechanism ensures efficient scalability without affecting the overall integrity verification process.

IV. EXPERIMENTAL RESULTS

The proposed certificateless public auditing framework can be extended in several ways to further enhance scalability, privacy, and practical implementation. Future research may explore the integration of blockchain technology to enable decentralized verification, thereby minimizing dependence on third-party auditors. In addition, the use of lightweight cryptographic algorithms could make the system more suitable for Internet of Things (IoT) devices and mobile cloud environments where computational resources are limited.

Another potential direction involves designing multi-authority key management schemes, which can improve security and reduce the risk of insider attacks. Furthermore, incorporating real-time auditing mechanisms along with artificial intelligence (AI)based anomaly detection techniques may help in identifying suspicious activities and maintaining continuous data integrity monitoring in large-scale cloud infrastructures.

- **Fig. (a)** This page is used to **register new group members** in the system.
- After submitting the form, the member's information is **stored in the database**.
- The registered member can later **log in using their email and password**.

- **Fig. (b)** The Login Page provides authentication for group members.
- Group members can use their registered email ID and private key for secure login.
- After verification, the group member is logged in to the system.

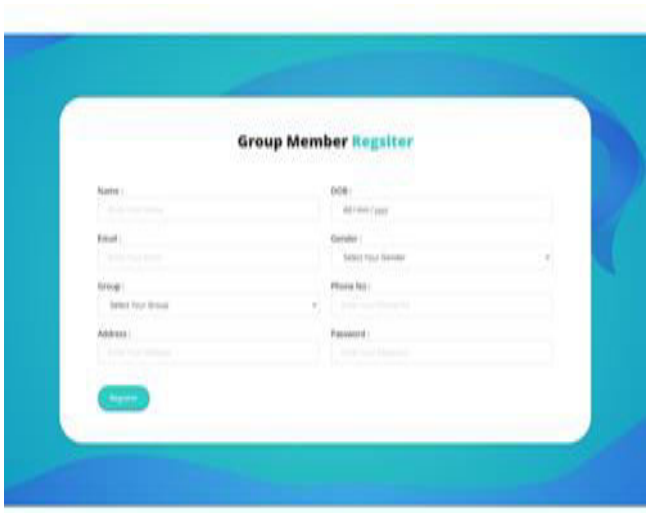
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

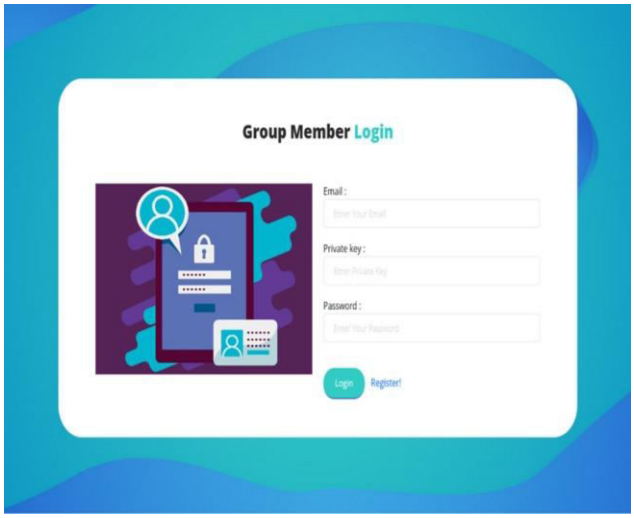
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506095|

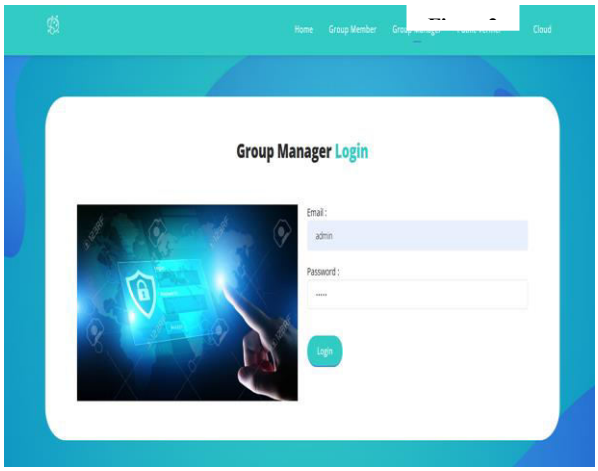


(a)

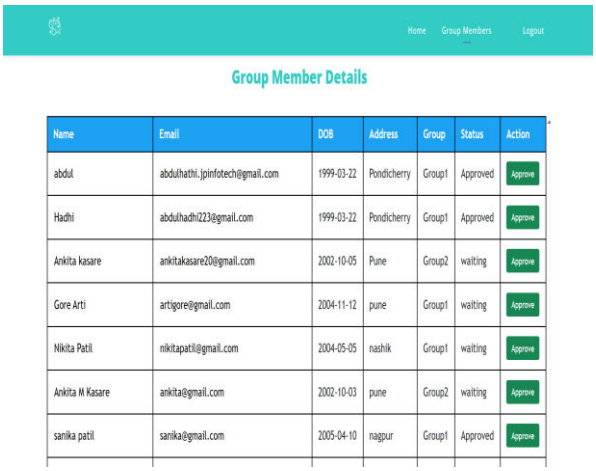


(b)

- **Fig. (c)** The Group Manager registers users, gives them a unique identity, and provides a partial key so they can securely create their own full private key.
- **Fig. (d)** To make sure **only valid users** join the system
- To prevent **fake or unauthorized users**
- To maintain **security and trust**



(c)



(d)

- **Fig. (e)** User requests to join → Group Manager approves → Private key is generated (partial + user secret)
- After key generation, user logs in using email and password
- **Fig. (f)** Public Verifier checks whether the data is correct and trustworthy without needing special permission.

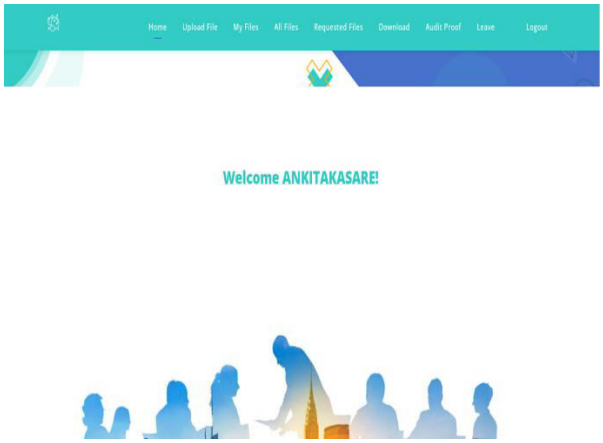
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

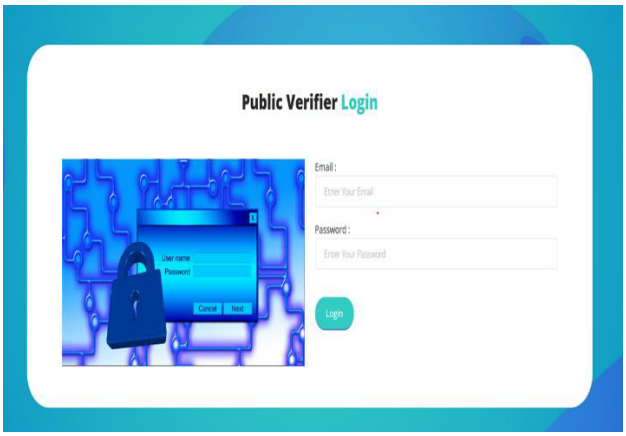
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506095|

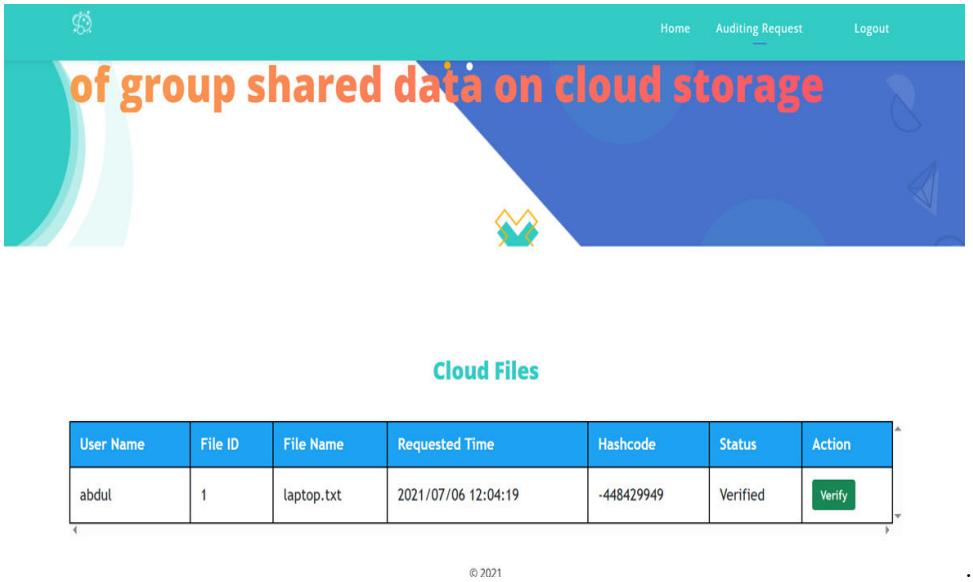


(e)



(f)

- **Fig. (g)** Cloud storage allows you to store, access, and protect your files online anytime from anywhere.



(g)

V. CONCLUSION

In summary, the proposed certificateless public integrity verification framework for group-shared cloud data offers a secure and efficient alternative to conventional certificate-based systems. By utilizing advanced cryptographic techniques such as hash functions, digital signatures, and optimized key. management mechanisms, the framework reduces administrative overhead while ensuring strong data confidentiality and integrity. The system also improves scalability and operational efficiency in dynamic cloud environments where multiple users frequently access and modify shared data. As a result, it is well suited for practical collaborative applications in modern cloud storage systems. Overall, the proposed approach provides a privacy preserving and scalable solution for secure cloud data auditing, contributing to the advancement of reliable cloud storage security technologies.

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

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506095|

REFERENCES

1) S. S. Rao, V. R. Patil, and R. S. Kumar, "Certificate-less public integrity checking of cloud data using cryptographic techniques,"International Journal of Computer Science and Engineering, vol. 10, no. 6, pp. 123–132, 2018.
2) L. Zhang, Y. Zhang, and D. Wu, "Efficient integrity checking in cloud storage: A certificate-free approach," Cloud Computing and Security, vol. 9, no. 4, pp. 147–159, 2017.
3) J. Wang, L. Zhang, and X. Liu, "Scalable integrity auditing for group shared data in cloud storage," International Journal of Information Technology, vol. 8, no. 3, pp. 231–240, 2020.
4) M. Ahmed, S. Kumar, and A. Jain, "Privacy-preserving public integrity verification for cloud data without certificates," Security and Privacy in Cloud Computing, vol. 11, no. 2, pp. 102–111, 2019.
5) X. Qin, T. Li, and Y. Wu, "Cloud data integrity checking and verification in the cloud environment," IEEE Transactions on Cloud Computing, vol. 4, no. 3, pp. 354–361, 2016.
6) S. Wang and M. Xu, "Public integrity auditing in cloud storage using a certificate-less cryptographic framework," Journal of Cloud Computing, vol. 12, no. 1, pp. 5–18, 2015.
7) W. Lin and S. Wei, "Data integrity assurance and public verification in cloud storage," International Journal of Computer Applications, vol. 6, no. 2, pp. 140–146, 2016.
8) Y. Chen and B. Li, "Privacy-preserving integrity checking for cloud data using public auditing," International Journal of Security and Privacy, vol. 8, no. 3, pp. 29–36, 2017.
9) Y. Xie, X. Zhang, and J. Jiang, "A survey of integrity verification for cloud data in cloud computing," Journal of Cloud Computing, vol. 16, no. 1, pp. 33–48, 2020.
10) J. Sun and M. Yang, "Efficient and secure data integrity checking for cloud storage," IEEE Transactions on Cloud Computing, vol. 6, no. 4, pp. 201–213, 2018.
11) A. M. Bessani and M. Correia, "Ensuring integrity and privacy in cloud storage," in Proceedings of the 6th International Conference on Cloud Computing, pp. 245–251, 2015.
12) X. Li and H. Wang, "Privacy-preserving data integrity verification for cloud data," Journal of Network and Computer Applications, vol. 104, no. 7, pp. 61–68, 2019.
13) J. Wang and Q. Li, "Certificate-less integrity auditing for group shared data in cloud storage," Journal of Cloud Computing Research, vol. 13, no. 5, pp. 140–151, 2017.
14) S. Chen and Z. Sun, "A review of cryptographic techniques for integrity verification in cloud storage," International Journal of Information Security and Privacy, vol. 13, no. 3, pp. 50– 67, 2016.
15) W. Liu and J. Liu, "Efficient public auditing for integrity verification of shared data in cloud storage," Journal of Network and Computer Security, vol. 18, no. 3, pp. 20–33, 2019.
16) A. Patel and R. Shah, "Scalable and secure integrity checking for cloud data with certificate-less public verification," in Proceedings of the International Conference on Security and Privacy, pp. 230–238, 2018.
17) J. Cheng and J. Xie, "Public auditing for group shared data integrity in cloud storage," Cloud Computing and Security Innovations, vol. 9, no. 4, pp. 135–145, 2017.
18) H. Xu and X. Zhang, "A survey of cloud data integrity checking methods and techniques," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 80–92, 2016.
19) J. Li and W. Zhang, "Privacy-preserving integrity verification for cloud data in a certificate-less framework," in Proceedings of the International Conference on Data Security and Privacy, pp. 212–221, 2020.
20) W. Zhang and Y. Li, "Cloud data integrity checking without certificats," International Journal of Computational Intelligence and Secuity, vol. 14, no. 6, pp. 143–151, 2019.
21) R. Zhang and M. Li, "Efficient certificate-less integrity checking for public cloud storage," International Journal of Cloud Computing and Services Science, vol. 7, no. 2, pp. 92–103, 2018.
22) Y. Zhang and D. Wu, "Public integrity auditing for group shared data in cloud storage," IEEE Transactions on Cloud Computing, vol. 4, no. 1, pp. 13–22, 2015.
23) H. Gao and X. Zhao, "Cloud storage integrity verification with efficient public auditing," Security and Communication Networks, vol. 9, no. 8, pp. 783–795, 2017.

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