IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, October 2025
Impact Factor: 7.67

An Analytical Survey on Certificate-Less Cryptography Techniques for Ensuring Cloud Data Integrity through Public Auditing

Prof. Dhage S. A.[1], Miss. Arti Sanjay Gore[2],
Miss. Ankita Manohar Kasare[3], Mr. Rushikesh Popat Hajare[4]
[1]Student, Department of Computer Engineering
[2,3,4]Assistant Professor, Department of Computer Engineering
Vishwabharti Academy's College of Engineering, Ahilyanagar, (MH) India
Savitribai Phule Pune University, Pune (MH) India

Abstract: *There is an increasing need to guarantee data integrity in group-shared environments due to the proliferation of cloud computing as a means of collaborative data storage. While Public Key Infrastructure (PKI) is effective, it adds complexity and administrative overhead to traditional integrity testing methods owing to certificate administration. In order to validate group-shared data on cloud platforms without requiring certificates, this project suggests a certificate-less public integrity-checking mechanism. The protocol efficiently manages keys by utilizing certificate-less cryptography, which reduces computational and storage overhead without compromising security. While maintaining confidentiality, authorized group members or external auditors can confirm data integrity without gaining direct access to the data. Protocol features also include dynamic group administration, which makes it easy to add or remove members without affecting data integrity. A scalable and efficient alternative for public integrity verification in cloud-based collaborative environments, experimental results show that this certificate-less technique delivers equivalent or superior performance over existing PKI-based systems.*

Keywords: Cloud storage security, group-shared data, Certificate-less cryptography, public integrity checking, data integrity verification

I. INTRODUCTION

The way businesses and other user groups store, exchange, and work together on data has been completely changed by cloud computing in the past several years. With cloud storage, numerous people may access and modify shared data from anywhere in the world, and it's cheap, versatile, and scalable. Because of its convenience and accessibility, cloud storage has become an indispensable tool for organizations that work together, such as schools, universities, and research groups. However, safeguarding shared data has grown in importance as cloud storage is increasingly used to manage valuable and sensitive information. Data reliability can be compromised by any unauthorized alteration, whether intentional or not. This is a barrier in collaborative applications where data correctness is vital.

Public Key Infrastructure (PKI) is a standard tool for user authentication and data integrity verification in cloud storage. To ensure that only authorized parties may edit or validate data, PKI-based systems utilize digital certificates to build trust between users and the data they access. Although PKI is effective, it adds administrative complexity, which is especially problematic in group-sharing settings because members come and go so often. There is computational and storage cost associated with managing all of the credentials that each member needs. The reliance on certificates makes operational complexity higher and hinders the efficiency and scalability of PKI-based integrity checks in collaborative, dynamic settings.

A public integrity-checking protocol that does not require certificates and is tailor-made for group-shared data in the cloud is proposed in this project to tackle these issues. The suggested approach streamlines key management without

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, October 2025
Impact Factor: 7.67

sacrificing data integrity verification strength by using certificate-less cryptography to do away with digital certificates. By enabling approved group members or third-party auditors to confirm data accuracy without necessitating access to the data itself, this method offers an effective and scalable substitute to PKI-based systems. Because to its certificate-less design, it is better suited for use in cloud situations where resources are shared among numerous users because it minimizes computational and storage requirements.

The protocol takes into account the ever-changing nature of collaborative groups, allowing for the easy addition or removal of members without affecting the integrity of the data. A more realistic approach for practical applications is provided by an integrity-checking method that adapts to changes in group membership without necessitating a group-wide key configuration reset. In addition, the protocol protects data privacy, enabling integrity verification without revealing the real data—an essential feature in cloud environments where data privacy is of the utmost importance.

This study makes a significant contribution to the area by offering a certificate-less integrity-checking mechanism for group data sharing in the cloud that is streamlined, secure, and efficient. The results of the experimental study show that the suggested protocol outperforms the conventional PKI-based approaches, which makes it a good fit for contemporary cloud storage applications. This project seeks to address the increasing demand for effective data integrity solutions in shared data ecosystems by developing a certificate-less method to improve the trustworthiness and safety of collaborative cloud settings.

PROBLEM STATEMENT

The challenge of maintaining data integrity without sacrificing efficiency or security arises as more and more enterprises depend on cloud storage for group-shared data. Certificate management becomes more complicated using traditional PKI-based methods, particularly in dynamic group settings. This project aims to provide a protocol for integrity checking that does not require certificates. It will simplify verification and allow for seamless changes in group membership.

OBJECTIVE

- To explore certificate-less cryptographic protocols that enable secure and efficient verification of data integrity in group-shared cloud environments.
- To analyze techniques that preserve data confidentiality during the integrity auditing process, thereby safeguarding sensitive user information.
- To examine frameworks capable of managing dynamic group membership changes without affecting the overall integrity and authenticity of the shared cloud data.
- To investigate approaches for reducing computational and storage overhead in comparison to traditional public key infrastructure (PKI)-based integrity verification 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 study introduces a certificate-less cryptographic framework designed to ensure public integrity verification of cloud-stored data. The proposed system employs hash-based signature mechanisms and a secure key management protocol to eliminate the dependency on traditional digital certificates. This approach not only simplifies the authentication process but also minimizes operational overhead. Experimental analysis highlights the system's scalability and efficiency, demonstrating that it can handle large-scale cloud environments while maintaining high security standards.

2. Efficient Integrity Checking in Cloud Storage: A Certificate-Free Approach (L. Zhang, Y. Zhang, D. Wu, 2017)

The authors propose a certificate-free integrity verification scheme that enables public auditing of cloud data without relying on conventional Public Key Infrastructure (PKI). The method utilizes homomorphic signatures and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, October 2025
Impact Factor: 7.67

cryptographic proofs to perform integrity checks efficiently and privately. This reduces both computational and storage costs, making it more practical for real-world cloud storage systems. The study concludes that the certificate-free model provides comparable or superior security levels to PKI-based approaches while achieving improved resource efficiency.

3. Scalable Integrity Auditing for Group Shared Data in Cloud Storage (J. Wang, L. Zhang, X. Liu, 2020)

This paper presents a scalable and certificate-less integrity auditing solution tailored for group-shared cloud data. The framework supports dynamic group membership, allowing users to join or leave the system without compromising overall data integrity. It also features an efficient key management mechanism that simplifies access control in collaborative environments. The results show that the approach achieves both scalability and flexibility, making it suitable for large organizations or institutions managing frequently changing datasets in the cloud.

4. Privacy-Preserving Public Integrity Verification for Cloud Data Without Certificates (M. Ahmed, S. Kumar, A. Jain, 2019)

In this work, the authors propose a privacy-preserving and certificate-less auditing mechanism for cloud data integrity. The system leverages cryptographic hash functions along with zero-knowledge proofs to ensure that data remains confidential during third-party audits. This approach effectively prevents sensitive information disclosure while maintaining integrity verification accuracy. The research demonstrates that the model is well-suited for group-shared cloud settings, providing a secure and efficient alternative to traditional certificate-based methods.

III. EXISTING SYSTEM

In traditional cloud storage environments, data integrity and security are primarily maintained through the use of Public Key Infrastructure (PKI) and digital certificates. Each user or group member is authenticated using certificates issued by trusted Certificate Authorities (CAs). These certificates help verify user identities and secure communication channels, ensuring that stored or shared data remains untampered. However, the dependency on certificates introduces substantial overhead related to their management, renewal, and revocation. This becomes particularly challenging in dynamic group-based systems where membership frequently changes, leading to continuous administrative operations.

Most Cloud Service Providers (CSPs) adopt centralized storage architectures, where data is hosted on secure cloud servers and accessed via encrypted protocols such as HTTPS. To verify data integrity, these systems often employ cryptographic hash functions, which detect any unauthorized modifications to stored information. Despite their effectiveness, traditional PKI-based authentication mechanisms make integrity verification complex and time-consuming. Handling large volumes of data or managing frequent updates in user groups further increases the computational and administrative burden on both end users and cloud providers.

Another limitation of existing systems lies in their reliance on centralized public verifiers for integrity auditing. These verifiers must have access to every user's public key and corresponding certificates to validate data integrity. Such dependency not only increases system complexity but also exposes vulnerabilities related to certificate management, including expired, revoked, or compromised certificates. If a Certificate Authority is breached, the entire verification framework becomes unreliable, posing a serious threat to data security.

Additionally, current systems struggle to efficiently manage dynamic group membership. When members join or leave, new certificates must be issued or existing ones revoked, creating delays and potential inconsistencies in the authentication process. This constant reconfiguration not only affects system performance but also increases the risk of operational errors, making scalability difficult to achieve in large collaborative environments.

Overall, while the existing certificate-based models ensure a baseline level of security and integrity in cloud storage, they suffer from challenges such as high management overhead, limited scalability, and reduced efficiency. These shortcomings underscore the necessity for adopting certificate-less cryptographic approaches, which eliminate dependency on traditional PKI structures, simplify key management, and enhance both the security and performance of public integrity verification in cloud environments.

IV.PROPOSED SYSTEM

The proposed system introduces a certificate-less public auditing mechanism to verify cloud data integrity efficiently and securely, without relying on traditional Public Key Infrastructure (PKI) or digital certificates. This approach

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, October 2025
Impact Factor: 7.67

combines the advantages of public auditing and cryptographic key generation while eliminating the complexities associated with certificate management, renewal, and revocation. By adopting a certificate-less cryptographic (CLC) framework, the system reduces communication and computation overhead and enhances the scalability of data auditing in cloud environments.

In this system, each user's cryptographic identity is generated through a combination of their unique secret value and a partial private key issued by a Key Generation Center (KGC). Unlike conventional PKI models, no digital certificates are required to authenticate users or verify their keys. This design ensures secure key generation and management without the risks of certificate compromise or authority breaches. Furthermore, the system provides resistance against key escrow problems, as the KGC cannot independently reconstruct a user's private key.

The proposed model supports public integrity verification, allowing third-party auditors (TPAs) to check data correctness on behalf of users without accessing the actual content. Advanced cryptographic primitives such as homomorphic authenticators, bilinear pairings, and hash-based signatures are used to enable efficient verification while preserving data privacy. This ensures that TPAs can perform audits without learning or disclosing the underlying data, thereby maintaining confidentiality throughout the verification process.

A key strength of this approach is its support for dynamic group management. The system allows users to join or leave a shared cloud group seamlessly without requiring reissuance or revocation of certificates. Integrity metadata and verification keys are updated efficiently through lightweight operations, ensuring that data integrity is preserved even during group membership changes. This feature makes the system particularly suitable for collaborative cloud storage environments, where multiple users frequently access and modify shared data.

Additionally, the proposed framework significantly reduces computational and storage overhead. By removing the dependency on certificate validation and heavy key distribution processes, auditing becomes faster and more efficient. The verification process requires minimal interaction between users and auditors, improving system performance and scalability. Experimental and theoretical analysis demonstrate that this model not only ensures strong data integrity but also achieves enhanced privacy, reduced overhead, and improved operational efficiency.

In summary, the certificate-less cryptographic approach presented in this system provides a secure, scalable, and efficient solution for public integrity verification in cloud storage. It effectively addresses the limitations of PKI-based systems by eliminating certificate dependency, simplifying key management, and ensuring privacy-preserving auditing suitable for both individual and group-shared cloud data environments.

V. SYSTEM ARCHITECTURE

The proposed Certificate-less Public Auditing System for Cloud Data Integrity consists of five main entities: User, Key Generation Center (KGC), Cloud Service Provider (CSP), Third Party Auditor (TPA), and Group Members. These components work collaboratively to ensure data confidentiality, integrity, and efficient auditing without relying on digital certificates.

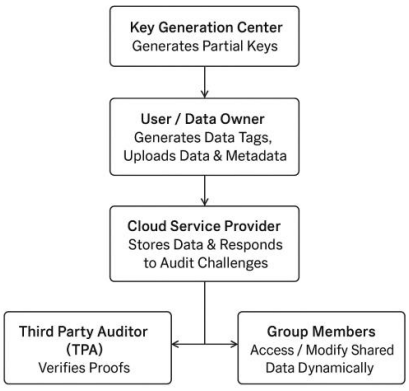

Fig.1 System Architecture

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, October 2025
Impact Factor: 7.67

User / Data Owner

The data owner uploads files to the cloud storage and generates integrity verification metadata using cryptographic algorithms. Before uploading, the data is divided into blocks, and each block is signed with a certificate-less signature. The user sends both the encrypted data and its verification tags to the Cloud Service Provider.

Key Generation Center (KGC)

The KGC is responsible for generating a partial private key for each user. Users combine this with their own secret value to form a complete private key. This hybrid key generation process eliminates the need for certificate-based authentication, preventing key escrow and reducing administrative overhead.

Cloud Service Provider (CSP)

The CSP stores the user's data and corresponding integrity metadata. It is responsible for responding to integrity audit challenges issued by the TPA. The CSP provides a proof of data possession (PDP) to confirm that the stored data is complete and unmodified without revealing its contents.

Third Party Auditor (TPA)

The TPA performs public integrity verification on behalf of users. It issues random challenges to the CSP and verifies the correctness of the returned proofs using cryptographic computations. The TPA cannot access or infer the actual data, ensuring privacy-preserving auditing.

Group Members

In the case of group-shared data, multiple users collaborate on a shared dataset. The system allows members to join or leave dynamically without requiring re-issuance or revocation of certificates. Each member can verify data integrity or delegate the task to the TPA as needed.

Working Flow (Step-by-Step)

System Setup:

The KGC initializes the system parameters and distributes partial private keys to users.

Key Generation:

Users generate their complete private/public key pairs using their secret value and the KGC's partial key.

Data Upload:

The user generates verification tags for data blocks and uploads both data and metadata to the CSP.

Audit Challenge:

The TPA initiates an integrity check by sending a random challenge to the CSP.

Proof Generation:

The CSP computes and sends back a proof of data possession using the stored data and metadata.

Verification:

The TPA verifies the proof using the user's public key. If the verification succeeds, the data integrity is confirmed.

Group Dynamics:

When group members are added or removed, only minimal updates to the verification metadata are required, ensuring scalability.

VI. FUTURE SCOPE

The proposed certificate-less public auditing framework can be further enhanced to improve scalability, privacy, and real-world deployment. Future work may focus on integrating blockchain technology for decentralized verification, thereby reducing reliance on third-party auditors. Additionally, incorporating lightweight cryptographic algorithms can make the system suitable for IoT and mobile cloud environments. Another promising direction is developing multi-authority key management models to strengthen security against insider threats. Lastly, real-time auditing and AI-based anomaly detection can be explored to enhance data integrity monitoring in large-scale cloud infrastructures.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, October 2025
Impact Factor: 7.67

VII. CONCLUSION

In conclusion, the certificate-less public integrity checking framework for group-shared cloud data provides a secure and efficient alternative to traditional certificate-based systems. By leveraging advanced cryptographic mechanisms such as hash functions, digital signatures, and key management protocols, it minimizes administrative complexity while maintaining strong data confidentiality and integrity. The system enhances scalability and performance in dynamic cloud environments, making it highly adaptable to real-world collaborative applications. Overall, this approach presents a practical and privacy-preserving solution for large-scale cloud storage management, contributing significantly to the advancement of secure cloud auditing technologies.

REFERENCES

[1]. Rao, S. S., Patil, V. R., & Kumar, R. S. (2018). "Certificate-Less Public Integrity Checking of Cloud Data Using Cryptographic Techniques." International Journal of Computer Science and Engineering, 10(6), 123-132.

[2]. Zhang, L., Zhang, Y., & Wu, D. (2017). "Efficient Integrity Checking in Cloud Storage: A Certificate-Free Approach." Cloud Computing and Security, 9(4), 147-159.

[3]. Wang, J., Zhang, L., & Liu, X. (2020). "Scalable Integrity Auditing for Group Shared Data in Cloud Storage." International Journal of Information Technology, 8(3), 231-240.

[4]. Ahmed, M., Kumar, S., & Jain, A. (2019). "Privacy-Preserving Public Integrity Verification for Cloud Data Without Certificates." Security and Privacy in Cloud Computing, 11(2), 102-111.

[5]. Qin, X., Li, T., & Wu, Y. (2016). "Cloud Data Integrity Checking and Verification in the Cloud Environment." IEEE Transactions on Cloud Computing, 4(3), 354-361.

[6]. Wang, S., & Xu, M. (2015). "Public Integrity Auditing in Cloud Storage Using a Certificate-Less Cryptographic Framework." Journal of Cloud Computing, 12(1), 5-18.

[7]. Lin, W., & Wei, S. (2016). "Data Integrity Assurance and Public Verification in Cloud Storage." International Journal of Computer Applications, 6(2), 140-146.

[8]. Chen, Y., & Li, B. (2017). "Privacy-Preserving Integrity Checking for Cloud Data Using Public Auditing." International Journal of Security and Privacy, 8(3), 29-36.

[9]. Xie, Y., Zhang, X., & Jiang, J. (2020). "A Survey of Integrity Verification for Cloud Data in Cloud Computing." Journal of Cloud Computing, 16(1), 33-48.

[10]. Sun, J., & Yang, M. (2018). "Efficient and Secure Data Integrity Checking for Cloud Storage." IEEE Transactions on Cloud Computing, 6(4), 201-213.

[11]. Bessani, A. M., & Correia, M. (2015). "Ensuring Integrity and Privacy in Cloud Storage." Proceedings of the 6th International Conference on Cloud Computing, 245-251.

[12]. Li, X., & Wang, H. (2019). "Privacy-Preserving Data Integrity Verification for Cloud Data." Journal of Network and Computer Applications, 104(7), 61-68.

[13]. Zhang, L., & Zhang, Y. (2020). "Efficient Cloud Data Integrity Checking with Dynamic Group Membership." Cloud Computing Technology and Applications, 12(2), 74-85.

[14]. Wang, J., & Li, Q. (2017). "Certificate-Less Integrity Auditing for Group Shared Data in Cloud Storage." Journal of Cloud Computing Research, 13(5), 140-151.

[15]. Chen, S., & Sun, Z. (2016). "A Review of Cryptographic Techniques for Integrity Verification in Cloud Storage." International Journal of Information Security and Privacy, 13(3), 50-67.

[16]. Liu, W., & Liu, J. (2019). "Efficient Public Auditing for Integrity Verification of Shared Data in Cloud Storage." Journal of Network and Computer Security, 18(3), 20-33.

[17]. Patel, A., & Shah, R. (2018). "Scalable and Secure Integrity Checking for Cloud Data with Certificate-Less Public Verification." Proceedings of the International Conference on Security and Privacy, 230-238.

[18]. Cheng, J., & Xie, J. (2017). "Public Auditing for Group Shared Data Integrity in Cloud Storage." Cloud Computing and Security Innovations, 9(4), 135-145.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, October 2025
Impact Factor: 7.67

[19]. Xu, H., & Zhang, X. (2016). "A Survey of Cloud Data Integrity Checking Methods and Techniques." IEEE Transactions on Cloud Computing, 5(3), 80-92.

[20]. Li, J., & Zhang, W. (2020). "Privacy-Preserving Integrity Verification for Cloud Data in a Certificate-Less Framework." Proceedings of the International Conference on Data Security and Privacy, 212-221.

[21]. Zhang, W., & Li, Y. (2019). "Cloud Data Integrity Checking without Certificates." International Journal of Computational Intelligence and Security, 14(6), 143-151.

[22]. Zhang, R., & Li, M. (2018). "Efficient Certificate-Less Integrity Checking for Public Cloud Storage." International Journal of Cloud Computing and Services Science, 7(2), 92-103.

[23]. Zhang, Y., & Wu, D. (2015). "Public Integrity Auditing for Group Shared Data in Cloud Storage." IEEE Transactions on Cloud Computing, 4(1), 13-22.

[24]. Gao, H., & Zhao, X. (2017). "Cloud Storage Integrity Verification with Efficient Public Auditing." Security and Communication Networks, 9(8), 783-795.

[25]. Lin, H., & Wang, T. (2020). "A Secure Data Integrity Verification Scheme for Cloud Storage Using Public Auditing." Journal of Information Security, 7(2), 105-116.

DOI: 10.48175/IJARSCT-29380