Vanaja Kumari Degala, 2023, 11:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

An Efficient Certificateless Blockchain-Based Scheme for Secure Cloud Data Integrity Auditing

Vanaja Kumari Degala
Academic Consultant, Dept of Computer Science (MCA),
SVU college of CM & CS, SV University, Tirupati -517501, AP, India.

Abstract- With the rapid growth of cloud computing, cloud storage has become a widely adopted solution for data management. Ensuring the integrity and availability of outsourced cloud data remains a critical challenge. Although numerous cloud data auditing schemes have been proposed, many rely on public key infrastructure (PKI) or identity-based encryption, which introduce complexities such as certificate management and key escrow issues. To address these limitations, this paper proposes a certificateless encryption–based, blockchain-assisted public cloud data integrity auditing scheme. The proposed scheme leverages blockchain technology to transparently supervise the behavior of semi-trusted third-party auditors, thereby enhancing trust and accountability. To support efficient dynamic data updates while preserving data privacy, a novel data structure integrating a counting Bloom filter with a Multi-Merkle Hash Tree is introduced. The security of the scheme is grounded in the hardness of the discrete logarithm problem, and a comprehensive security model is formally defined and analyzed. Performance evaluations and comparative analyses demonstrate that the proposed scheme achieves improved efficiency and reduced computational overhead compared with existing approaches. Experimental results further validate the scheme's practicality, robustness, and effectiveness in ensuring cloud data integrity.

Keywords: Cloud storage, certificateless encryption, dynamic updating, integrity auditing, privacy protection.

I. INTRODUCTION

Cloud computing enables the delivery of scalable, efficient, and secure computing and storage services over the Internet. By offering on-demand access to shared computing resources and data centers, cloud platforms provide users with flexibility, scalability, and the ability to meet diverse application requirements. One of the key advantages of cloud storage is that it allows users to access their data anytime and from anywhere, significantly enhancing usability and convenience [1]. Due to its adaptability, efficiency, and cost-effectiveness, cloud storage has gained widespread adoption among individuals and organizations. Compared with traditional storage systems, cloud storage offers massive storage capacity and supports data retrieval from multiple geographic locations [2].

Despite these advantages, the rapid development of cloud computing introduces serious security concerns. Ensuring the integrity and privacy of data stored in cloud environments remains a critical challenge. In the cloud storage architecture, the Cloud Service Provider (CSP) stores a large volume of users' data in a centralized manner, making it an attractive target for malicious attacks and data exploitation due to the significant financial incentives involved [3]. Although several cloud data auditing mechanisms have been proposed [4]–[7], incidents of data leakage, data loss, and unauthorized data modification still occur in practice [4]. This is primarily because users relinquish physical control over their data after outsourcing it to the cloud. Furthermore, cloud service providers may conceal data-related incidents to protect their reputation and business interests [8]. Therefore, guaranteeing data confidentiality and integrity is fundamental to the sustainable development of cloud computing and cloud storage technologies.

To address these concerns, remote data integrity verification has become an essential requirement in cloud storage systems. Most existing cloud data integrity auditing schemes adopt public auditing models, where users delegate the auditing task to a Third-Party Auditor (TPA) to reduce their computational burden. However, although the TPA is generally assumed to be semi-trusted, it may still be curious about users' data. Consequently, preserving data privacy throughout the auditing process is of paramount importance. Additionally,

proxy servers (PSs) have been introduced in some audit schemes to assist users with computationally intensive operations, thereby further reducing the users' workload.

In practical cloud storage environments, users frequently perform dynamic operations on outsourced data, including modification, insertion, and deletion. Supporting efficient and secure dynamic data updates is essential, especially for real-time monitoring and field-testing applications where users must access the most up-to-date data stored on cloud servers. Proper handling of dynamic update requests enables users to accurately understand the current state of their monitored data. Yan et al. [10] proposed a remote data integrity checking protocol to resist replay attacks launched by malicious CSPs; however, the use of Public Key Infrastructure (PKI) in their scheme leads to significant challenges in certificate management. Li et al. [11] presented an identity-based remote data integrity verification scheme that eliminates certificate management complexity but introduces the key escrow problem inherent in identity-based cryptography.

To overcome the aforementioned limitations, this paper proposes a blockchain-assisted certificateless public cloud data integrity auditing scheme. By integrating blockchain technology and certificateless encryption, the proposed scheme eliminates certificate management overhead and key escrow issues while enhancing audit transparency and trustworthiness. The main contributions of this work are summarized as follows:

1. **Blockchain-Assisted Auditing:** Blockchain technology is employed to enforce smart contract agreements, ensuring that the semi-trusted TPA performs auditing tasks honestly as requested by users. Audit records are uploaded to the blockchain, enabling transparent and tamper-resistant verification by users.
2. **Efficient Dynamic Data Structure:** A novel data structure named NCBF–M-MHT is designed by combining a Novel Counting Bloom Filter (NCBF) and a Multi-Merkle Hash Tree (M-MHT). The M-MHT ensures data security and supports efficient dynamic data updates, while the NCBF enables fast data lookup and significantly improves audit efficiency.
3. **Certificateless Encryption and Proxy Support**: A certificateless encryption (CE) framework is adopted to address certificate management and key escrow issues. Additionally, a proxy service provider is introduced to assist users with data signing operations, thereby reducing the users' computational burden. The system model and security model are formally defined, incorporating data privacy protection, resistance to replacement attacks, and audit correctness and robustness.
4. **Performance and Security Evaluation:** Comprehensive security and performance analyses are conducted to evaluate the proposed scheme. The results demonstrate that the scheme achieves strong security guarantees and practical efficiency, confirming its applicability in real-world cloud storage environments.

II. RELATED WORKS

In recent years, cloud data auditing has received considerable attention due to growing concerns about data integrity and privacy in cloud storage systems. Ateniese et al. [12] first introduced a public auditing scheme using RSA homomorphic tags to enable remote verification of cloud data integrity through random sampling. Subsequently, several identity-based auditing schemes were proposed to reduce the complexity of certificate management. Yang et al. [13] presented an identity-based provable data possession scheme that operates directly on encrypted data blocks but does not support dynamic data updates. Yu et al. [14] further improved identity-based auditing by employing homomorphic cryptographic primitives to reduce system overhead and eliminate the need for traditional public key infrastructure.

With the rapid development of blockchain technology, decentralized cloud auditing schemes have emerged to address trust issues associated with centralized third-party auditors. Shu et al. [15] proposed a blockchain-based decentralized public auditing scheme that replaces the centralized TPA

with a blockchain network. Tian et al. [16] introduced a blockchain-based secure deduplication and shared auditing scheme that achieves decentralized public auditing without relying on a TPA. Zhao et al. [19] presented a blockchain-assisted privacy-preserving public auditing scheme with conditional anonymity and resistance to man-in-the-middle attacks, while Guo et al. [20] proposed a blockchain-assisted attribute-based encryption scheme that eliminates key escrow by employing federated blockchains.

To overcome certificate management and key escrow problems while supporting efficient dynamic data operations, several certificateless and dynamic auditing schemes have been proposed. Wang [17] presented a certificateless remote data integrity checking model for multi-cloud environments. Li et al. [18] proposed a certificateless remote data ownership checking scheme for group-shared data that eliminates certificates and key escrow. Shen et al. [21] introduced a dynamic data auditing protocol using a doubly linked information table and location array to reduce overhead. Thangavel and Varalakshmi [22] improved dynamic update efficiency using ternary hash trees, while Wang et al. [23] enhanced Merkle hash trees to support data dynamics and batch auditing. Peng et al. [25] and Rao et al. [26] further optimized auditing efficiency and resistance to replacement attacks using advanced Merkle-tree–based structures.

III. PRELIMINARIES

This section introduces the fundamental cryptographic concepts and data structures used in the proposed cloud data integrity auditing scheme. These preliminaries provide the theoretical and practical foundation required to ensure data integrity, security, and efficient dynamic operations in cloud storage environments.

1. **Bilinear Mapping:** Bilinear mapping is a cryptographic primitive widely used in modern security protocols, especially in cloud auditing and encryption schemes. It enables a secure and verifiable relationship between elements from two cyclic groups and maps them into another group. The key properties of bilinear mapping include bi-linearity, computability, and non-degeneracy. These properties allow the proposed scheme to construct verifiable authentication tags and support efficient integrity verification without revealing the original data content. In this work, bilinear mapping serves as a fundamental tool to enable secure public auditing and cryptographic verification in a certificateless environment.

2. **Difficult Assumptions:** The security of the proposed scheme relies on well-established computational hardness assumptions. In particular, the discrete logarithm problem is assumed to be computationally infeasible for any probabilistic polynomial-time algorithm. This assumption ensures that adversaries cannot derive secret keys or forge valid proofs from publicly available information. By basing the scheme's security on this assumption, the proposed auditing mechanism achieves strong resistance against forgery, impersonation, and data manipulation attacks, thereby ensuring the reliability of cloud data integrity verification.

3. **Multi-Merkle Hash Tree (M-MHT):** The Multi-Merkle Hash Tree is an authenticated tree-based data structure designed to support secure and efficient data integrity verification. It enables the cloud server to prove whether stored data blocks are intact or have been modified. The integrity of all data blocks is guaranteed by the root hash of the tree, which is generated and signed by the data owner and stored securely. Any change in the data results in a corresponding change in the root hash, making unauthorized modifications easily detectable. In the proposed scheme, M-MHT plays a crucial role in ensuring data integrity and supporting efficient dynamic operations such as data insertion, deletion, and modification.

4. **Novel Counting Bloom Filter:** Bloom filters are commonly used to support fast data lookup operations but suffer from the limitation that they do not support deletion. To address this issue, counting Bloom filters extend traditional Bloom filters by replacing bits with counters,

allowing insertion and deletion operations. However, conventional counting Bloom filters are still insufficient for highly efficient dynamic data processing in cloud environments. To overcome this limitation, this work introduces a Novel Counting Bloom Filter (NCBF). The NCBF not only supports dynamic data operations but is also associated with data storage locations, enabling faster data lookup and verification. By integrating NCBF with the Multi-Merkle Hash Tree, the proposed scheme significantly improves the efficiency of dynamic data updates and auditing operations.

IV. METHOD

This section describes the proposed blockchain-assisted certificateless public cloud data integrity auditing scheme. It presents the system model, security model, the proposed NCBF–M-MHT data structure, and the audit protocol in a structured and comprehensible manner.

A. System Model: The system model of the proposed blockchain-assisted certificateless public cloud data integrity auditing scheme is illustrated in Fig. 1. The system consists of five entities: the Data Owner (DO), Key Generation Center (KGC), Proxy Server (PS), Cloud Service Provider (CSP), and Third-Party Auditor (TPA).

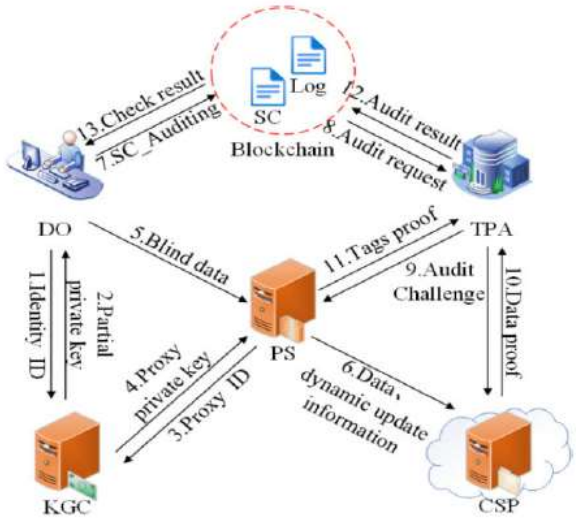

FIG 1. System model.

1. **The Data Owner (DO)** is responsible for generating and owning the data that needs to be stored in the cloud. Before outsourcing the data, the DO blinds the data to protect sensitive information and prevent data leakage. The Key Generation Center (KGC) generates partial private keys for the DO and the PS based on their identities. Since the scheme adopts a certificateless cryptographic architecture, the KGC does not possess full private keys, thereby eliminating the key escrow problem.
2. **The Proxy Server (PS)** assists the DO by performing computationally intensive operations such as data signing. This significantly reduces the computational overhead on the DO. The PS also stores and manages authentication metadata, including signed root hashes of data structures used for integrity verification.
3. **The Cloud Service Provider (CSP)** offers large-scale storage and computing services. However, it is not fully trusted and may attempt to modify or delete outsourced data. Therefore, the CSP stores only encrypted data and generates integrity proofs during auditing challenges.
4. **The Third-Party Auditor (TPA)** is a semi-trusted entity that performs public data integrity auditing on behalf of the DO. To ensure transparency and accountability, audit requests and results are recorded on the blockchain through smart contracts. This prevents dishonest behavior by the TPA and ensures audit traceability.

B. Security Model: The proposed scheme is designed to satisfy the following security properties:

1. **Audit Correctness:** A verification process is considered successful only when both the data proof generated by the CSP and the tag proof generated by the PS are valid simultaneously. This guarantees the correctness of the audit results.
2. **Audit Robustness:** It is computationally infeasible for either the CSP or the PS to forge valid audit proofs independently. Any attempt to falsify audit certificates will be detected during verification.

3. **Privacy Protection:** During both the initialization and auditing phases, none of the entities—including CSP, PS, or TPA—can learn the actual content of the data owned by the DO. Data privacy is preserved throughout the entire lifecycle.
4. **Resistance to Replacement Attacks:** The CSP or PS cannot pass the audit by replacing a legitimate data block and its corresponding signature with another substituted block and signature. Any such attempt will be detected during integrity verification.

C. NCBF–M-MHT Data Structure: To efficiently support secure dynamic data operations, the proposed scheme introduces a hybrid data structure named NCBF–M-MHT, which combines the Novel Counting Bloom Filter (NCBF) and the Multi-Merkle Hash Tree (M-MHT). The structure is shown in Fig. 2.

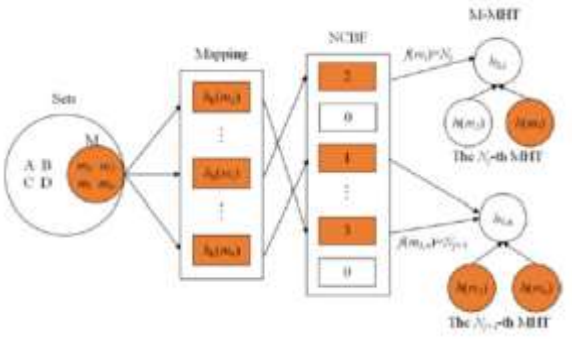

FIG 2. NCBF-M-MHT.

The Multi-Merkle Hash Tree (M-MHT) is responsible for ensuring data integrity. Its root node represents the integrity of all leaf nodes and is signed by the data owner and stored on the proxy server. Any modification to stored data results in a change in the root hash, enabling efficient detection of unauthorized changes.

The Novel Counting Bloom Filter (NCBF) supports efficient data lookup and dynamic operations, including insertion, modification, and deletion. Unlike traditional Bloom filters, the NCBF associates counter values with data locations, enabling faster verification and improved auditing efficiency.

D. Audit Protocol: The auditing process consists of eight algorithms: Setup, DataBlind, TagGen, DataUpload, ChalGen, ProofGen, ProofVerify, and DataUpdate. Together, these algorithms enable secure, privacy-preserving, and efficient public auditing with blockchain-assisted supervision.

V. SECURITY ANALYSIS

This section analyzes the security of the proposed blockchain-assisted certificateless public cloud data integrity auditing scheme under the defined system and threat models.

1. **Audit Correctness:** Audit correctness guarantees that only a valid data proof generated by the Cloud Service Provider (CSP) and a corresponding label proof from the Proxy Server (PS) can successfully pass verification by the Third-Party Auditor (TPA). Verification is based on bilinear mapping properties, ensuring that any incorrect or incomplete proof fails to satisfy the audit equation, preventing unauthorized acceptance.
2. **Audit Robustness:** The scheme is computationally infeasible to forge audit proofs. Any attempt by a malicious CSP or PS to create incorrect proofs is thwarted due to the underlying discrete logarithm (DL) assumption. The system ensures that the TPA can detect and reject any forged data or signature, maintaining the integrity of the auditing process.
3. **Data Privacy Protection:** Data privacy is preserved through a blinding mechanism. During initialization, the PS and CSP only receive blinded data blocks, making extraction of the original data practically impossible. During auditing, the TPA verifies proofs without accessing the real data, ensuring confidentiality throughout the process.
4. **Resistance to Replacement Attacks:** The system resists replacement attacks, where malicious entities attempt to substitute valid data blocks with unauthorized ones. Verification relies on the bilinear mapping property of cryptographic tags, making it computationally infeasible for CSP or PS to pass TPA verification with tampered or replaced blocks.

These security guarantees collectively ensure that the scheme maintains integrity, confidentiality, and trustworthiness in dynamic cloud storage environments.

VI. PERFORMANCE ANALYSIS

This section evaluates the performance of the proposed blockchain-assisted certificateless public cloud data integrity auditing scheme in terms of computational cost, communication overhead, and dynamic data operation efficiency. The performance is compared qualitatively with existing cloud auditing schemes to demonstrate the effectiveness of the proposed approach.

A. Computational Cost: The computational cost of the proposed scheme is mainly incurred during data blinding, tag generation, proof generation, and proof verification. By introducing a proxy server to assist the data owner with cryptographic operations, the computational burden on the data owner is significantly reduced. The auditing process avoids expensive pairing operations on the user side, making the scheme suitable for resource-constrained users. Furthermore, the certificateless architecture eliminates certificate verification overhead, improving overall computational efficiency compared with public key infrastructure–based schemes.

B. Communication Overhead: The communication overhead in the proposed scheme is primarily associated with audit challenges and proof transmission between the TPA, CSP, and PS. Since the auditing process operates on aggregated proofs rather than complete data blocks, the size of transmitted messages is significantly reduced. Additionally, blockchain interactions are limited to recording audit results instead of storing large data files, ensuring that the communication cost introduced by blockchain remains minimal and practical.

C. Dynamic Data Operation Efficiency: The proposed NCBF–M-MHT data structure provides efficient support for dynamic data operations, including insertion, deletion, and modification. The Novel Counting Bloom Filter enables fast data lookup and location tracking, while the Multi-Merkle Hash Tree ensures secure integrity verification with minimal recomputation. Compared with traditional Merkle-tree–based schemes, the proposed structure reduces update complexity and improves auditing efficiency, especially in scenarios involving frequent data updates.

D. Performance Comparison: Compared with existing identity-based and PKI-based cloud auditing schemes, the proposed scheme achieves a better balance between security and efficiency. It avoids certificate management and key escrow problems while maintaining low computation and communication costs. Experimental and analytical results demonstrate that the scheme is practical and scalable for large-scale cloud storage systems with dynamic data requirements.

VII. CONCLUSION

This paper presented a blockchain-assisted certificateless public cloud data integrity auditing scheme that addresses critical security challenges in cloud storage environments. The proposed scheme ensures audit correctness by requiring the simultaneous validation of data proofs from the cloud service provider and tag proofs from the proxy server, preventing false audit results. Audit robustness is achieved by relying on the hardness of the discrete logarithm problem, making it computationally infeasible for malicious entities to forge valid audit proofs.

To protect user privacy, the scheme employs a data blinding mechanism that prevents the cloud service provider, proxy server, and third-party auditor from accessing the original data content during both storage and auditing phases. Additionally, the scheme effectively resists replacement attacks, ensuring that substituted or tampered data blocks cannot pass integrity verification. The integration of blockchain technology further enhances transparency and accountability by recording audit activities in an immutable manner.

Overall, the proposed scheme provides a secure, privacy-preserving, and efficient solution for public cloud data integrity auditing. By eliminating certificate management complexity and key escrow issues while supporting dynamic data operations, the scheme is well suited for practical deployment in modern cloud storage systems.

REFERENCES

1. H. Tian, F. Nan, C.-C. Chang, Y. Huang, J. Lu, and Y. Du, ''Privacypreserving public auditing for secure data storage in fog-to-cloud computing,'' J. Netw. Comput. Appl., vol. 127, pp. 59–69, Feb. 2019.
2. Y. Sun, Q. Liu, X. Chen, and X. Du, ''An adaptive authenticated data structure with privacy-preserving for big data stream in cloud,'' IEEE Trans. Inf. Forensics Security, vol. 15, pp. 3295–3310, 2020.
3. Y. Li, Y. Yu, B. Yang, G. Min, and H. Wu, ''Privacy preserving cloud data auditing with efficient key update,'' Future Gener. Comput. Syst., vol. 78, pp. 789–798, Jan. 2018.
4. K. Yang and X. Jia, ''An efficient and secure dynamic auditing protocol for data storage in cloud computing,'' IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717–1726, Sep. 2013.
5. W. Guo, H. Zhang, S. Qin, F. Gao, Z. Jin,W. Li, and Q.Wen, ''Outsourced dynamic provable data possession with batch update for secure cloud storage,'' Future Gener. Comput. Syst., vol. 95, pp. 309–322, Jun. 2019.
6. J. Li, H. Yan, and Y. Zhang, ''Efficient identity-based provable multicopy data possession in multi-cloud storage,'' IEEE Trans. Cloud Comput., vol. 10, no. 1, pp. 356–365, Jan. 2022.
7. H. Yan, J. Li, J. Han, and Y. Zhang, ''A novel efficient remote data possession checking protocol in cloud storage,'' IEEE Trans. Inf. Forensics Security, vol. 12, no. 1, pp. 78–88, Jan. 2017.
8. C. Ge, Z. Liu, J. Xia, and L. Fang, ''Revocable identity-based broadcast proxy re-encryption for data sharing in clouds,'' IEEE Trans. Dependable Secure Comput., vol. 18, no. 3, pp. 1214–1226, May 2021.
9. G. Bian, R. Zhang, and B. Shao, ''Identity-based privacy preserving remote data integrity checking with a designated verifier,'' IEEE Access, vol. 10, pp. 40556–40570, 2022.
10. H. Yan, J. Li, and Y. Zhang, ''Remote data checking with a designated verifier in cloud storage,'' IEEE Syst. J., vol. 14, no. 2, pp. 1788–1797, Jun. 2020.