iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69403

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Mechanisms and Challenges in Public Auditing for Cloud Computing

Abu Salim[1], Rajesh Kumar Tiwari[2], Aasif Aftab[3], Shams Tabrez Siddiqui[4]
[1, 3, 4]*Department of Computer Science, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia*
[2]*Department of Computer Science and Engineering, RVS College of Eng. & Tech, Jamshedpur, Jharkhand, India*

Abstract: ***Cloud computing has revolutionized data storage and processing by offering scalable, on-demand access to computing resources. However, outsourcing sensitive information to cloud service providers (CSPs) introduces critical challenges in ensuring data security and integrity. Public auditing mechanisms enable third-party auditors (TPAs) to verify the integrity of cloud-stored data without compromising data privacy. This paper explores public auditing in cloud computing, highlighting mechanisms, challenges, and recent developments, including blockchain integration, artificial intelligence (AI), and quantum-resistant cryptography. A comprehensive review of cryptographic techniques, auditing protocols, and privacy-preserving mechanisms is presented, along with an analysis of future trends and open research areas.***
Keywords: cloud computing, public auditing, data Security, third-party auditors, cloud service providers

I. INTRODUCTION

Cloud computing has emerged as a transformative technology, enabling organizations and individuals to access vast storage and computational resources without the need for large-scale, on-premises infrastructure investments. This shift allows businesses to focus on core operations while leveraging the scalability, flexibility, and cost-effectiveness of cloud services. The cloud model allows for dynamic resource allocation, optimizing performance and reducing costs. Moreover, cloud services alleviate the burden of managing hardware, software, and network infrastructure, which would otherwise require significant financial and technical resources [1].

Despite its advantages, outsourcing data to the cloud introduces substantial security and privacy risks. Since data stored in the cloud is managed by CSPs, users effectively relinquish direct control over their data. The CSPs are responsible for ensuring data availability, integrity, and confidentiality, but the lack of user control introduces challenges in maintaining trust. Data breaches, unauthorized access, and server-side attacks are prevalent risks that can compromise the security of cloud-stored data [2]. Ensuring data remains intact and unmodified, even without the user's constant oversight, is paramount to the success and adoption of cloud computing. A primary concern with outsourcing data to the cloud is the integrity of the stored data. Since CSPs maintain full control over physical storage systems, there is always the possibility that data could be accidentally lost, corrupted, or maliciously altered. Users cannot continuously monitor their cloud-stored data or frequently download it to check for integrity, especially with large datasets. Therefore, ensuring data integrity without requiring constant supervision becomes crucial in establishing trust between cloud users and providers [3].

To address these concerns, public auditing has emerged as a promising solution. Public auditing allows data owners to delegate the verification of their data's integrity to a trusted TPA. The TPA verifies the correctness and completeness of the stored data on behalf of the data owner. The key advantage of public auditing is that it eliminates the need for users to directly monitor cloud-stored data, reducing the burden on users and enhancing the scalability of cloud services [4].

A critical aspect of public auditing is ensuring that the auditing process does not compromise data privacy. Since the TPA is not the data owner, exposing the content of the data to the auditor would breach confidentiality and create further security risks. To mitigate this, public auditing protocols are designed to ensure that integrity verification can be completed without revealing actual data to the auditor. Cryptographic techniques, such as homomorphic encryption, are employed to ensure that auditors can perform operations on encrypted data, verifying integrity without learning the actual content [5].

In addition to privacy preservation, public auditing protocols must ensure that data is both accurate and unmodified. This involves verifying that cloud-stored data has not been tampered with, either by the CSP or external threats. Techniques such as Proof of Retrievability (PoR) and Provable Data Possession (PDP) provide strong guarantees of data integrity. These protocols enable the TPA to challenge the CSP to prove it still holds the original, unmodified data without requiring the entire dataset to be downloaded for verification [3 ,6].

Public auditing schemes face several challenges, including maintaining auditing efficiency, especially with large datasets, and supporting dynamic data operations such as updates, insertions, and deletions. Additionally, privacy preservation and preventing collusion between the CSP and the TPA remain ongoing concerns. Research continues to evolve, with new protocols and cryptographic techniques being developed to address these issues and improve the robustness of public auditing systems [7].

This paper investigates key challenges, solutions, and advancements in public auditing for cloud computing, focusing on cryptographic foundations and protocols that ensure data integrity and privacy preservation. By exploring recent developments, the paper aims to provide insights into how public auditing can evolve to meet growing demands for cloud security.

II. PROBLEM STATEMENT

The main challenge in cloud computing lies in ensuring the integrity of data stored remotely, especially when users have limited access to physical storage infrastructure. Public auditing allows a trusted TPA to verify data integrity on behalf of the user. The auditor's role is to check whether the cloud server holds the data as promised without downloading it, which must be done efficiently and securely. However, privacy concerns arise as auditors could potentially access sensitive information during the auditing process.

Key challenges addressed in this research include

1) *Ensuring Data Integrity Without Compromising Confidentiality:* Verifying the integrity of cloud-stored data while maintaining confidentiality requires privacy-preserving auditing protocols that allow integrity checks without exposing data content.
2) *Protecting Against Data Breaches, Unauthorized Access, and Server Misbehaviour:* Designing public auditing mechanisms that detect unauthorized modifications and provide protection against server misbehaviours and external threats is essential.
3) *Developing Lightweight and Efficient Auditing Protocols:* Auditing protocols must be computationally efficient to be deployed on resource-constrained devices, minimizing overhead in computation, communication, and storage.
4) *Supporting Dynamic Data Operations:* Auditing mechanisms must support dynamic data operations without requiring a full re-audit after every modification, ensuring scalability and efficiency.
5) *Batch Auditing and Scalability:* Designing scalable auditing protocols that maintain security while reducing computational and communication overhead is crucial for large-scale systems.
6) *Mitigating Collusion Between Cloud Providers and Auditors:* Developing mechanisms to ensure auditors act independently and honestly, providing strong integrity guarantees even in the presence of colluding entities.

III. PUBLIC AUDITING MODELS

A. Traditional Auditing Methods

Traditionally, data owners were responsible for checking the integrity of their data stored on remote servers. However, this approach is impractical in cloud computing environments, given the large volume of outsourced data and limited computing resources available to users.

B. Third-Party Auditing (TPA)

Third-party auditing introduces a trusted auditor to verify the integrity of outsourced data. The TPA ensures that:

1) The cloud provider maintains data accurately.
2) Auditing is performed without accessing or altering the data.
3) The process is efficient, minimizing overhead on both the user and the CSP.

C. Public Auditing Schemes

Public auditing schemes leverage cryptographic techniques to ensure privacy and security during the auditing process. These schemes can be categorized into:

1) *Privacy-Preserving Public Auditing:* Ensures that the auditor cannot learn actual data content during verification.
2) *Batch Auditing:* Enables a TPA to simultaneously verify the integrity of data from multiple users or across multiple cloud servers, significantly improving auditing efficiency.
3) *Dynamic Auditing:* Supports updates, deletions, and insertions in cloud-stored data while maintaining auditing correctness and efficiency. Techniques such as Merkle Hash Trees (MHTs) are commonly used for dynamic data integrity verification [8].

4) *Homomorphic Authenticators:* Allow TPAs to verify the correctness of data blocks without retrieving them. These cryptographic primitives support operations on encrypted or authenticated data and form the foundation of many privacy-preserving auditing protocols .

IV. CRYPTOGRAPHIC TECHNIQUES IN PUBLIC AUDITING

Public auditing systems rely heavily on cryptography to ensure security and privacy.

A. *Key Cryptographic Techniques Include*

1) Homomorphic Authenticators: These enable the auditor to compute verifiable information over encrypted data without needing to decrypt it. This is essential in ensuring privacy during the auditing process [9].
2) Bilinear Pairing: Bilinear maps allow for efficient construction of cryptographic protocols, especially in public key-based systems. Many public auditing schemes use bilinear pairings to construct verifiable proofs of data possession and retrievability [10].
3) Provable Data Possession (PDP): PDP schemes enable a verifier to check if the cloud stores the original data without downloading it. It uses spot checking and probabilistic proofs to ensure data integrity [3].
4) Proof of Retrievability (PoR): PoR provides stronger guarantees than PDP by ensuring that the entire data file can be retrieved intact. It often incorporates error-correcting codes and spot checking [6].

B. *Recent Developments includes*

1) Blockchain-Integrated Public Auditing: Blockchain is being used to enhance transparency and tamper-resistance in auditing logs. With smart contracts, blockchain allows for verifiable, immutable auditing records without centralized control, minimizing trust assumptions on TPAs [11].
2) AI-Driven Anomaly Detection: Machine learning techniques are increasingly employed to identify unusual access patterns, data manipulation behaviours, or performance anomalies that may indicate integrity breaches. AI-driven auditors can dynamically prioritize verification tasks based on risk profiling [12].
3) Lightweight Auditing for IoT and Edge ComputingRecent efforts focus on designing lightweight protocols that can run on edge devices and IoT nodes. These schemes reduce computational and communication costs, making cloud auditing feasible in resource-constrained environments [13].
4) Quantum-Resistant Public Auditing: With the advent of quantum computing, traditional cryptographic techniques may become vulnerable. Research is now exploring post-quantum cryptographic primitives (e.g., lattice-based cryptography) for building quantum-secure auditing schemes [14].
5) Privacy-Enhanced Audit with Zero-Knowledge Proofs (ZKPs): Zero-knowledge proofs allow a TPA to verify data integrity without learning anything about the data. ZKP-based auditing mechanisms are gaining traction as they provide strong privacy guarantees even when the auditor is semi-trusted [15].
6) Blockchain-Based Certificateless Public Auditing for Cyber-Physical Systems: The work [16] introduced a blockchain-based certificateless public auditing scheme tailored for cloud-based cyber-physical systems. This approach addresses the key-escrow problem and enhances privacy by masking original data proofs using random functions during transmission.
7) Entangled Merkle Forest for Efficient Auditing and Version Control: In [17] authors proposed the "Entangled Merkle Forest," a Merkle Hash Tree-based architecture designed to support version control and dynamic auditing in centralized cloud environments. This framework aims to achieve blockchain-like immutability while mitigating synchronization and performance challenges associated with decentralized architectures.
8) AI-Driven Anomaly Detection in Cloud Auditing: In [18] the author developed "MoniLog," an automated log-based anomaly detection system for cloud computing infrastructures. MoniLog utilizes machine learning techniques to detect sequential and quantitative anomalies in real-time, enhancing the scalability and efficiency of cloud monitoring systems.
9) Blockchain-Based Privacy-Preserving Public Auditing for Group Shared Data: In [19] authors presented a blockchain-based public auditing scheme that ensures privacy preservation for group-shared data. The scheme employs smart contracts to facilitate secure and efficient auditing processes without compromising data confidentiality.
10) Key-Exposure Resistant Auditing Scheme for Industrial IoT: In the [20] authors proposed a blockchain-based data auditing scheme with key-exposure resistance specifically designed for Industrial Internet of Things (IIoT) environments. This scheme enhances security by preventing unauthorized access even if secret keys are exposed.

The Table 1 shows a tabular comparison of the key cryptographic techniques used in public auditing, including the method used, purpose, and key advantages:

TABLE 1
KEY CRYPTOGRAPHIC TECHNIQUES USED IN PUBLIC AUDITING

Work	Method Used	Purpose	Key Advantage
Homomorphic Authenticators (Shacham & Waters, 2008)	Verifiable operations on encrypted data	Integrity verification without decryption	Preserves data privacy during audits
Bilinear Pairing (Boneh et al., 2001)	Bilinear maps for constructing proofs	Enables verifiable proof generation in public-key settings	Efficient and secure cryptographic protocol design
Provable Data Possession (PDP) (Ateniese et al., 2007)	Spot checking and probabilistic proofs	Verify possession of data without full download	Lightweight with low overhead
Proof of Retrievability (PoR) (Juels & Kaliski, 2007)	Spot checking + error-correcting codes	Ensure full file retrievability	Stronger guarantees than PDP
Blockchain-Integrated Auditing (Zhang et al., 2018)	Smart contracts + immutable logs	Decentralized, transparent audit logging	Tamper-resistant, trustless auditing
AI-Driven Anomaly Detection (Wang et al., 2021)	Machine learning-based behavior analysis	Detect anomalies in access or data manipulation	Dynamic, intelligent auditing
Lightweight Auditing for IoT (Chen et al., 2020)	Resource-optimized cryptographic protocols	Auditing on edge/IoT devices	Feasible on constrained devices
Quantum-Resistant Auditing (Almazrouei et al., 2021)	Post-quantum cryptographic primitives	Future-proof auditing systems	Secure against quantum attacks
Zero-Knowledge Proofs (ZKPs) (Xu et al., 2022)	ZKPs for privacy-preserving verification	Verify data integrity without revealing data	Strong privacy even with semi-trusted auditors
Certificateless Auditing for CPS (Adouth & Rajagopal, 2023)	Blockchain + certificateless cryptography	Privacy-focused auditing in cyber-physical systems	Eliminates key-escrow problem; ensures audit authenticity
Entangled Merkle Forest (Bappy et al., 2023)	Merkle Hash Tree-based dynamic auditing	Version control + data integrity in centralized clouds	Blockchain-like immutability without full decentralization
MoniLog – AI Anomaly Detection (Vervaet, 2023)	Log-based ML anomaly detection	Detect irregular cloud behavior via logs	Real-time detection; improves cloud observability
Group Shared Data Auditing (Qi et al., 2023)	Smart contracts + group-based privacy	Privacy-preserving audits for multi-user data	Ensures shared data confidentiality; decentralized control
IIoT Key-Exposure Resistant Auditing (Yang & Ren, 2024)	Blockchain + exposure-resistant key management	Secure IIoT auditing against key compromise	Robust even with exposed keys; designed for industrial settings

V. CHALLENGES

Despite advancements, several challenges remain:

1) *Efficiency vs. Privacy Trade-offs:* Achieving a balance between high computational efficiency and robust privacy protection is challenging. Many privacy-preserving techniques (e.g., encryption, zero-knowledge proofs) increase processing overhead, making it harder to scale.
2) *Audit Log Integrity:* Audit logs must be immutable and verifiable to ensure trust in the auditing process. If these logs can be altered, the entire audit trail becomes unreliable. Techniques like blockchain are being explored to secure audit trails.
3) *Dynamic Data Support:* Supporting secure, real-time updates—such as insertions, deletions, and modifications—of cloud-stored data without requiring complete re-audits remains a work in progress, especially for large and frequently changing datasets.
4) *TPA Trustworthiness:* Trusting a third-party auditor (TPA) introduces a potential risk if the auditor is compromised or colludes with a cloud provider. Emerging solutions involve distributed or blockchain-based auditing to reduce reliance on a single trusted entity.
5) *Scalability in Multi-User Settings:* When dealing with numerous users and massive volumes of data, maintaining efficient and secure auditing becomes complex. Solutions must address the challenge of batch auditing and parallel processing without sacrificing performance or data integrity.

VI. FUTURE DIRECTIONS

Future research in public auditing should focus on:

1) *Fully Decentralized Auditing Systems:* Future systems should explore combining blockchain with federated learning to eliminate reliance on a single trusted auditor, enabling collaborative, privacy-preserving, and tamper-proof auditing across distributed environments.
2) *Standardization and Interoperability:* There is a pressing need for unified frameworks, protocols, and APIs that promote seamless interoperability among diverse Cloud Service Providers (CSPs), enhancing cross-platform auditability and compliance.
3) *Audit-as-a-Service (AaaS):* AaaS can evolve into a cloud-native, modular service offering flexible, on-demand auditing with customizable settings for privacy, frequency, and performance—making robust auditing accessible to all users.
4) *Integrating Confidential Computing:* Leveraging Trusted Execution Environments (TEEs) like Intel SGX, future audit solutions can securely perform verifications within isolated hardware environments, ensuring confidentiality and trust even inside untrusted cloud infrastructures.

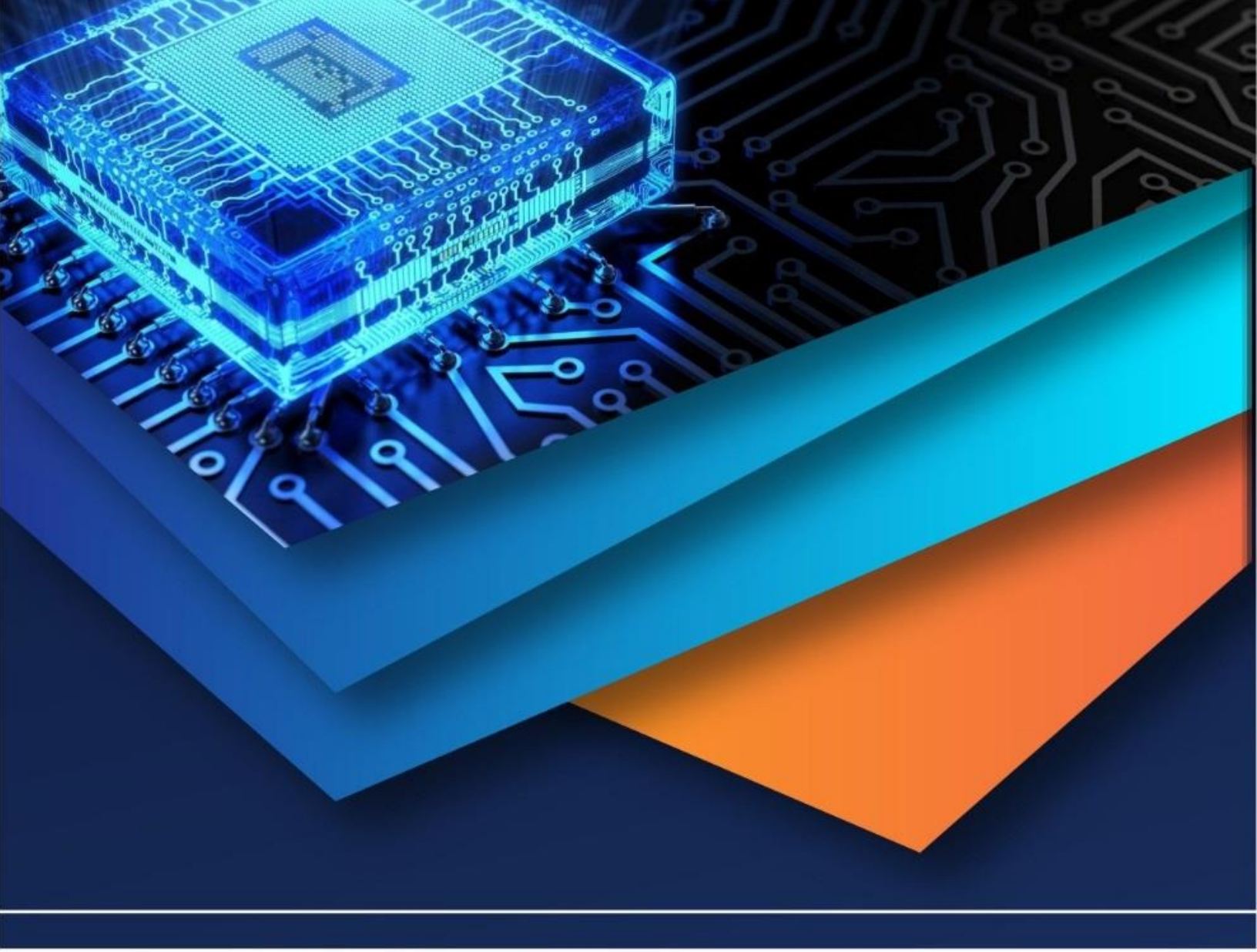
VII. CONCLUSION

Public auditing is vital for maintaining trust, integrity, and transparency in cloud computing environments. With growing adoption of cloud services, the need for robust, privacy-preserving, and efficient auditing mechanisms has become increasingly important. Through advanced cryptographic techniques, integration with emerging technologies like blockchain and AI, and continued research into lightweight and scalable solutions, public auditing is evolving into a cornerstone of secure cloud computing. However, significant challenges remain, particularly in balancing privacy, performance, and security in large-scale, multi-user environments. Continued innovation and standardization will be key to ensuring trust and security in future cloud ecosystems.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010
[2] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Gener. Comput. Syst., vol. 28, no. 3, pp. 583– 592, Mar. 2012.
[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 598–609.
[4] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in Proc. 14th Eur. Symp. Res. Comput. Secur. (ESORICS), 2010, pp. 355–370.
[5] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Privacy-preserving public auditing for secure cloud storage,” IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013
[6] A. Juels and B. S. Kaliski Jr., “PORs: Proofs of retrievability for large files,” in Proc. ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 584–597
[7] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, “Dynamic audit services for integrity verification of outsourced storages in clouds,” IEEE Trans. Serv. Comput., vol. 6, no. 2, pp. 227–238, Apr.–Jun. 2013

[8] C. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. ACM Conf. Comput. Commun. Secur. (CCS), 2009, pp. 213–222.
[9] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. ASIACRYPT, vol. 5350, Springer, 2008, pp. 90–107.
[10] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in Proc. Int. Conf. Theory Appl. Cryptogr. Tech. (EUROCRYPT), 2001, pp. 514–532.
[11] Y. Zhang, X. Chen, J. Li, D. Wong, H. Li, and I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 484–497, Apr.–Jun. 2018.
[12] C. Wang, J. Zhang, and Y. Ren, "AI-driven data integrity auditing in cloud storage," IEEE Access, vol. 9, pp. 76312–76322, 2021.
[13] X. Chen, Y. Zhang, Z. Qin, J. Li, and K. Ren, "Efficient and privacy-preserving data integrity verification for edge-assisted IoT," IEEE Internet Things J., vol. 7, no. 2, pp. 1305–1316, Feb. 2020.
[14] M. Almazrouei, A. Abuzneid, and A. Mahmood, "Post-quantum cryptography for cloud data auditing," IEEE Access, vol. 9, pp. 130291–130305, 2021.
[15] Y. Xu, Z. Zhang, and C. Li, "Zero-knowledge proof-based public auditing for secure cloud storage," IEEE Trans. Cloud Comput., early access, 2022.
[16] R. Adouth and K. Rajagopal, "Blockchain-based certificateless public auditing for cyber-physical cloud systems," in Proc. IEEE Int. Conf. Blockchain, 2023, pp. 1–8.
[17] M. Bappy, M. Rahman, and A. Anwar, "Entangled Merkle Forest: Efficient public auditing and version control in centralized cloud storage," in Proc. IEEE Int. Conf. Cloud Comput., 2023, pp. 1–7.
[18] D. Vervaet, "MoniLog: AI-based log analysis for anomaly detection in cloud infrastructure," in Proc. IEEE Int. Conf. Big Data, 2023, pp. 1–6.
[19] J. Qi, Y. Zhou, and L. Yang, "Blockchain-based privacy-preserving public auditing for group shared data in cloud," IEEE Trans. Dependable Secure Comput., early access, 2023.
[20] Y. Yang and K. Ren, "Key-exposure resistant public auditing for industrial IoT using blockchain," IEEE Internet Things J., early access, 2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY