Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Blockchain Enabled Public Auditing for Cloud Data Integrity with Federated Learning and AI Integration

Abu Salim
Department of Computer Science
College of Engineering and Computer Science
Jazan University
Jazan, Saudi Arabia

Syed Ghyasuddin Hashmi
Department of Computer Science
College of Engineering and Computer Science
Jazan University
Jazan, Saudi Arabia

Ziauddin Syed
Department of Computer Science
College of Engineering and Computer Science
Jazan University
Jazan, Saudi Arabia

Mohammad Haseebuddin
Department of Computer Science
College of Engineering and Computer Science
Jazan University
Jazan, Saudi Arabia

Jorair Ahmad
Department of Computer Science
College of Engineering and Computer Science
Jazan University
Jazan, Saudi Arabia

Shams Tabrez Siddiqui
Department of Computer Science,
College of Engineering and Computer Science,
Jazan University,
Jazan, Saudi Arabia,

***Abstract*— Cloud computing has transformed data storage and service provision by offering scalable, on-demand access to computational resources. However outsourcing data to third-party cloud servers poses significant security and privacy issues, especially concerning data integrity, confidentiality, and trust. Public auditing has become an essential tool that allows third-party auditors (TPAs) to validate the integrity of cloud-stored data without accessing the actual content. Despite its effectiveness, conventional public auditing schemes often suffer from issues such as significant computation cost, centralized trust dependency, and vulnerability to single points of failure. To address these limitation, Blockchain technology provides a decentralised, transparent, and tamper-resistant framework that can significantly enhance the reliability and efficacy of cloud auditing [1].**

This paper offers an extensive analysis of blockchain-based public auditing techniques in cloud computing and evaluates current auditing frameworks, identifies significant security and privacy concerns, and examines the combined potential of blockchain, artificial intelligence (AI), and federated learning to enhance audit reliability and ,additionally, a unique blockchain-enabled auditing architecture is developed to guarantee immutable audit logs, distributed verification, and privacy-preserving validation.

Keywords— Cloud computing, public auditing, blockchain, data integrity, federated learning, security, transparency.

I. INTRODUCTION

Cloud computing has become a prevailing model in the digital age, allowing organisations and individuals to access extensive computational resources, storage, and services via the internet on a pay-per-use basis. It has transformed information technology by enhancing flexibility, scalability, and cost efficiency across various sectors, including schools, hospitals, financial services, and government. Industry statistics indicate that the worldwide cloud services market is experiencing significant growth, as organisations increasingly transition their applications and data to cloud platforms to improve productivity and save operational expenses [2].

In spite of these benefits, outsourcing data and processing to external cloud servers presents considerable security and privacy problems. A critical concern is the verification of data integrity, ensuring that user data saved in the cloud stays unmodified and accessible over time. Conventional cryptographic techniques, including hash-based integrity checks, frequently prove inadequate in extensive cloud systems due to users' loss of direct control over their data once it is kept remotely [3]. To address this issue, scholars have suggested public auditing techniques that enable third entities, referred to as Third Party Auditors (TPAs), to regularly validate the accuracy of cloud-stored data without obtaining the complete dataset.

However, traditional public auditing frameworks have numerous constraints. The majority of these depend on a centralised Third-Party Administrator, creating a singular point of trust and potential failure. If compromised, the TPA may conspire with the cloud service provider (CSP) to fabricate audit results, so compromising the system's integrity. Moreover, these systems frequently include considerable computing overhead and communication expenses, rendering them inappropriate for large-scale or resource-constrained settings [4].

The advent of blockchain technology presents a viable solution to these difficulties. The intrinsic characteristics of blockchain like decentralization, transparency, immutability, and distributed consensus can eradicate reliance on a singular trusted auditor and guarantee verifiable audit records [5]. Blockchain-based public auditing solutions can augment trust among users, auditors, and service providers by documenting audit evidence and verification outcomes on a tamper-proof ledger. Furthermore, smart contracts provide automatic and self-executing audit procedures, minimising human involvement and the risk of manipulation.

Moreover, nascent technologies like artificial intelligence (AI) and federated learning (FL) can enhance public auditing systems. Artificial intelligence can enhance anomaly

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

detection and performance analysis, whereas federated learning enables privacy-preserving sharing of audit data among dispersed entities without disclosing private data [6].

This article focusses on incorporating blockchain technology into public auditing frameworks for cloud computing. It conducts a thorough examination of existing auditing systems, addresses critical security and privacy concerns, and presents an enhanced blockchain-enabled auditing framework. The proposed framework tries to enable transparent, efficient, and privacy-preserving audits while remaining scalable and robust.

The rest of the paper is organised as follows: Section II: Literature Review, provides an overview of existing research on cloud auditing and blockchain integration. Section III: Security and Privacy Challenges in Public Auditing Systems examines the primary challenges, vulnerabilities, and limits of both traditional and blockchain-based systems. Section IV: Proposed Blockchain-Based Auditing Framework describes the architecture, workflow, and important characteristics of the proposed framework. Section V: Future Research challenges identify open issues, technical obstacles, and new research directions. Section VI: Conclusion, summarises the key findings, contributions, and implications of the study.

II. Literature Review

Public auditing mechanism in cloud computing are intended to ensure the integrity and availability of outsourced data without requiring users to download whole files. These processes can generally be categorised into four major categories: Provable Data Possession (PDP), Proof of Retrievability (PoR), Third Party Auditing (TPA) schemes, and Blockchain-integrated audit frameworks.

A. Provable Data Possession (PDP)

The Provable Data Possession model, introduced by Ateniese et al., was among the initial formalisations addressing the data integrity verification issue [7]. In PDP, data owner preprocesses their file by creating metadata before to transmitting it to the cloud. During an audit, the auditor issues a challenge to the cloud, which then generates a proof utilising a limited subset of data blocks and their associated tags. The verifier assesses the proof's validity without accessing the complete data file.

The primary benefit of PDP is the reduction of communication and processing expenses while facilitating probabilistic verification. However, the original PDP paradigm implies private auditing, wherein only the data owner possesses the capability to check integrity. It also lacks native support for data dynamics like insertion, deletion, and updating, constraining its utility in real-time cloud systems.

B. Proof of Retrievability (PoR)

The Proof of Retrievability method, proposed by Juels and Kaliski [8], guarantees both the integrity of data and the complete recoverability of the file upon request. Proof of Retrievability (PoR) systems utilize error-correcting codes and cryptographic spot-checking to ensure the detection of any data loss or corruption. Shacham and Waters subsequently introduced a publicly verifiable Proof of Retrievability (PoR) utilizing BLS signatures, enabling any third party to authenticate integrity proofs while preserving secrecy [9].

Proof of Retrievability (PoR) systems offer more robust assurances than Provable Data Possession (PDP) but generally incur greater storage and computational expenses due to redundancy and coding requirements. Furthermore, PoR models are more appropriate for static data, as dynamic updates may jeopardise proof consistency.

C. Third Party Auditing (TPA) Models

To enhance user convenience and alleviate resource limitations, academics have developed public auditing techniques that incorporate a Third-Party Auditor (TPA). In these arrangements, a semi-trusted Third-Party Auditor (TPA) conducts verification on the client's behalf. An exemplary case is the privacy-preserving auditing framework by Wang et al., which integrates homomorphic linear authenticators and random masking to safeguard data privacy during audits [10]. The TPA can authenticate integrity without accessing data content.

The primary benefits of TPA-based schemes encompass less client-side processing and the capacity to facilitate batch auditing for several users concurrently. Nonetheless, these systems are significantly dependent on the reliability of the TPA. If the Third-Party Auditor (TPA) conspire with the Cloud Service Provider (CSP) or engage in malicious conduct, the audit outcomes may be fabricated. Moreover, TPA-centric systems create a single point of failure, undermining decentralisation and resilience.

D. Blockchain Integrated Auditing Mechanisms

Blockchain technology is currently gaining popularity as a revolutionary answer to the trust issues inherent in third-party audits [11]. A public auditing system that integrates blockchain utilises distributed ledger technology (DLT) to transparently record and verify audit transactions across numerous nodes. Every audit outcome, challenge, or evidence can be preserved as a tamper-evident record on the blockchain, obviating the necessity for a centralised auditor.

Smart contracts, implemented on blockchain systems like Ethereum or Hyperledger Fabric, can automate the auditing process by issuing challenges, verifying proofs, and rewarding honest players through incentive mechanisms [12]. This automation diminishes human involvement and improves fairness.

Besides transparency, blockchain integration enhances accountability: each audit event is traceable, and audit history cannot be modified retroactively. Various systems, like BPDS (Blockchain-based Public Data Auditing System) and DecAudit, have illustrated the viability of decentralised auditing with minimal trust requirements [13], [14].

However, blockchain-based systems encounter significant hurdles. The on-chain storage of substantial proofs is costly and inefficient because of restricted block size and elevated

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

transaction fees. Hybrid methodologies have been devised to address this issue, wherein only audit summaries or hashes are kept on-chain, while comprehensive proofs are maintained off-chain. Moreover, scalability, consensus latency, and privacy breaches (attributable to public ledger transparency) remain as unresolved issues.

Table 1 summarizes and compares the main public auditing mechanisms for cloud data. PDP and PoR focus on data integrity verification with limited support for dynamic updates and rely on private or public trust models, but lack decentralization. TPA-based schemes improve usability through third-party verification but introduce centralized trust, while blockchain-based approaches provide decentralized, public verifiability and support data dynamics, albeit with higher costs and latency.

TABLE 1: COMPARISON OF PUBLIC AUDITING MECHANISMS

Mechanism	Trust Model	Verifiability	Data Dynamics	Decentralization	Major Limitation
PDP	Private	Probabilistic	Limited	No	Private verification only
PoR	Public	Deterministic	Limited	No	High redundancy cost
TPA BASED	Semi trusted	Public	Supported	No	Centralized auditor
BLOCKCHAIN BASED	Trusted	Public	Supported	Yes	High cost, latency

III. SECURITY AND PRIVACY CHALLENGES IN PUBLIC AUDITING SYSTEMS

The security and privacy of outsourced data in cloud computing is a paramount concern. While public auditing systems facilitate external verification of data integrity, they may also provide additional attack surfaces and privacy issues. This section rigorously analyses the core security and privacy problems inherent in both traditional and blockchain-based public auditing techniques.

A. Ensuring Data Integrity and Authenticity

The principal aim of public auditing is to ascertain if cloud-stored data is preserved, unmodified, and genuine. In traditional systems, a malicious Cloud Service Provider (CSP) may eliminate rarely visited data or manipulate stored files without the owner's awareness. Methods include homomorphic authenticators, hash chains, and Merkle trees are utilised to identify integrity issues. However, if an auditor's verification keys are obtained, adversaries can fabricate seemingly legitimate proofs, so compromising the auditing process [15].

In blockchain architectures, distributed verification among numerous independent nodes provides integrity assurance. Each evidence and its associated verification outcome, once recorded on the blockchain, become immutable and visible, hence removing the possibility of retroactive modification. However, this same immutability can provide challenges, incorrect or malevolent information cannot be altered or removed, leading to issues about data governance and legal compliance.

B. Auditor Reliability and Collusion Risks

Traditional auditing systems depend on a Third-Party Auditor (TPA), presumed to be semi-trustworthy. This assumption is frequently tenuous, as a compromised or malicious TPA may conspire with the CSP to obscure integrity breaches or fabricate audit results [16]. This collaboration significantly erodes the trustworthiness and accountability of the system.

Blockchain-based auditing frameworks alleviate these vulnerabilities via decentralisation and consensus procedures. Numerous auditor nodes autonomously validate audit proofs, and outcomes are conclusive only upon attaining a majority consensus. This eradicates single failure points and centralised trust dependencies.

Nonetheless, consensus algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) are susceptible to majority (51%) and Sybil attacks, wherein adversaries dominate a substantial segment of the network to distort verification outcomes.

C. Preventing Privacy Leakage During Auditing

Public auditing facilitates integrity verification without complete data access; nevertheless, it may still expose information or usage patterns. Auditors may deduce information such as the frequency of file modifications, data volume, or access patterns from audit requests [17]. Despite employing measures such as random masking, side channel information continues to pose a possible privacy threat [18].

In blockchain-based systems, this problem is exacerbated due to the public visibility of audit records and transaction hashes on the ledger. Adversaries observing the blockchain can associate timestamps and transaction flows to infer user activity or audit frequency.

In response, researchers have suggested privacy-preserving auditing systems utilising zero-knowledge proofs (ZKPs), ring signatures, and secret transactions, which obscure audit specifics while maintaining verifiability.

D. *Key Lifecycle Management and Revocation*

Efficient cryptographic key management is essential for preserving system integrity. Users and auditors depend on private keys for generating proofs and verifying signatures. The compromise or leakage of these keys may allow attackers to fabricate audit evidence or impersonate authorised companies. Current systems frequently presume static key pairs, rendering key revocation and renewal arduous when credentials are hacked or users are substituted [19].

The integration of decentralised identity (DID) systems with smart contract-based key rotation methods can facilitate the automation of key revocation and replacement within

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

blockchain frameworks. However, maintaining backward compatibility, ensuring that previous audit records remain verifiable following important updates remains a research problem.

E. nership, Accountability, and Legal Compliance

In shared cloud environments, delineating data ownership and accountability becomes intricate, particularly when numerous clients utilise the same infrastructure. Conventional auditing methods frequently inadequately designate responsibility in cases of data corruption or loss. Blockchain provides a public and immutable audit trail, establishing a verifiable chain of ownership and acts that promotes accountability [20].

However, the immutable nature of blockchain records creates regulatory challenges, especially concerning data protection legislation like the General Data Protection Regulation (GDPR), which mandates the "right to be forgotten." Reconciling blockchain's immutability with advancing data privacy mandates continues to be an unresolved compliance challenge [21].

F. Balan ng Scalability and Performance Efficiency

While blockchain integration improves audit transparency and trust, it presents problems related to latency, scalability, and cost. Consensus mechanisms increase processing delays, while high transaction fees—particularly in public blockchains—limit the practicality of frequent audits. Furthermore, the direct storage of audit logs or proofs on-chain may result in blockchain bloat and diminished performance [22].

To resolve these challenges, off-chain storage alternatives like the Interplanetary File System (IPFS) and Layer 2 sidechains are being progressively utilised. These provide the efficient off-chain storage of extensive evidence files, with only cryptographic references anchored on-chain. Attaining an ideal equilibrium of security, privacy, and scalability continues to be a pivotal study focus, with hybrid frameworks anticipated to prevail in forthcoming designs.

Table 2 provides a comparative overview of significant security and privacy challenges in traditional and blockchain-based public auditing systems.

Table 2 Comparative summary of key security and privacy challenges

Issue	Description	Challenges in Traditional Auditing	Improvements with Blockchain-Based Auditing
Data Integrity & Authenticity	Ensuring that outsourced cloud data remains unaltered and genuine.	CSP may delete or modify files; integrity proofs rely on a single auditor's key, which can be compromised.	Distributed verification and immutable on-chain records prevent tampering and falsified proofs.
Auditor Trust & Collusion	Ensuring honest behavior from the Third-Party Auditor (TPA).	Single TPA can collude with CSP to falsify or hide audit failures.	Decentralized verification via consensus reduces reliance on a single entity.
Privacy Leakage During Auditing	Preventing exposure of sensitive metadata or audit patterns.	Auditors can infer data usage, access frequency, or modification patterns.	Zero-knowledge proofs (ZKPs), ring signatures, and confidential transactions help conceal audit details.
Key Management & Revocation	Secure handling of cryptographic keys for users and auditors.	Static key sets make revocation or renewal difficult when credentials are compromised.	Smart contracts enable automated key rotation and revocation using decentralized identity (DID).
Data Ownership & Accountability	Establishing responsibility in multi-tenant cloud environments.	Ownership boundaries are unclear; disputes arise over data loss or tampering.	Immutable blockchain audit trails enhance accountability and traceability.

IV. Proposed Blockchain Based Auditing Framework

We propose a hybrid, blockchain-enabled public auditing framework for cloud computing, based on a comparative study and the strengths of emerging technologies. The framework is intended to be decentralised, intelligent, and privacy-preserving.

A. Framework Architecture

The proposed architecture has five fundamental components:

1) *Data Owner Layer:* The data owner preprocess files prior to their upload to the CSP. This entails producing homomorphic tags or authenticators for data blocks and establishing a distinct file identifier. The data owner additionally implements and configures the smart contract that regulates the audit process.

2) *Cloud Service Provider (CSP) Layer:* The CSP retains the user's data together with its associated metadata. It is accountable for addressing audit issues by producing evidence of data possession and retrievability through the utilization of stored data blocks and tags.

3) *Blockchain Layer (Consortium Blockchain):* A permissioned blockchain functions as the trust anchor. It operates the Audit Smart Contract (ASC), which automates the complete audit lifecycle. The blockchain exclusively retains immutable audit receipts, cryptographic hashes of audit proofs, timestamps, and verification outcomes, while substantial proof material is held off-chain.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

4) *Auditor Network:* A decentralized network of nodes, which may comprise other Cloud Service Providers (CSPs), dedicated auditing nodes, or data owners, functions as the verifier. The ASC randomly selects a subset of these nodes to authenticate the proof submitted by the CSP. Their unanimous conclusion, obtained by an on-chain consensus mechanism, is conclusive.

5) *Off Chain Storage & AI/FL Engine:* Extensive audit evidence are preserved in a decentralized off-chain storage system such as IPFS, with their hashes secured on the blockchain. An AI/FL engine, orchestrated by the blockchain, executes distributed anomaly detection. Local AI models are trained on node-specific audit logs through Federated Learning, with only model updates being shared and documented on the blockchain for transparency.

B. *Process Flow of Decentralized Public Auditing in Cloud Environments*

The operational procedure of the suggested framework is as follows:

Step 1 (Initiation): The ASC initiates an audit by dispatching a challenge to the CSP, depending on a predetermined timeline or an AI-generated risk score.

Step 2 (Proof Generation): The CSP produces an integrity proof for the contested data blocks and uploads it to off-chain storage (e.g., IPFS), obtaining a content identifier (CID).

Step 3 (On Chain Submission): The CSP presents the CID of the proof to the ASC on the blockchain.

Step 4 (Distributed Verification): The ASC randomly selects a committee of auditing nodes. These nodes retrieve the proof from IPFS utilizing the CID, independently validate it, then send their votes (Valid/Invalid) to the ASC.

Step 5 (Consensus & Recording): The ASC counts the votes. Upon reaching a consensus (e.g., >2/3 majority) affirming the validity of the proof, a "Pass" audit receipt is documented on the blockchain. Alternatively, a "Fail" receipt is documented, potentially activating penalty provisions within the smart contract.

Step 6 (Continuous Learning): The local AI models at each auditor node are revised according to the audit results through Federated Learning. The consolidated global model progressively enhances, increasing the precision of anomaly detection and risk forecasting for forthcoming audits.

V. Key Features and Advantages

The proposed hybrid framework has numerous essential aspects that collectively improve the security, scalability, and intelligence of public auditing in cloud systems. These features aim to address the constraints of conventional centralized auditing approaches by utilizing blockchain, federated learning, and intelligent audit scheduling.

1) *Decentralized Trust:* The framework replaces centralized third-party auditors with a decentralized auditing committee regulated by a consortium blockchain. Every audit transaction is authenticated by a distributed consensus process, guaranteeing that no individual entity may alter or fabricate audit outcomes. This method eradicates single points of failure and allocates trust across autonomous nodes, markedly enhancing reliability and accountability.

2) *Immutability and Transparency:* All audit results, verification evidence, and consensus resolutions are permanently inscribed on the blockchain ledger. The immutable characteristics of blockchain guarantee that upon the completion of an audit, neither the Cloud Service Provider (CSP) nor any auditor may alter or erase records. This transparent audit trail enhances traceability and facilitates reliable verification for users and regulatory bodies.

3) *Cost Efficiency and scalability:* The hybrid approach, employing off-chain proof storage (such as IPFS) and streamlined on-chain references, markedly alleviates blockchain congestion and transaction costs. Audit outcomes are encapsulated as concise cryptographic commitments, reducing on-chain data while maintaining integrity. This architectural decision improves scalability, rendering the framework suitable for extensive, multi-user cloud systems.

4) *Intelligent and Adaptive Auditing:* An integrated AI auditing agent utilizes federated models to analyze historical audit results, continuously modifying audit frequency and emphasis according to real-time risk assessments. This adaptive strategy guarantees efficient resource utilization, prioritizing high-risk data segments and enhancing the system's reaction to incoming threats.

5) Interoperability and Extensibility: The framework's modular architecture facilitates seamless integration with various cloud service providers and blockchain networks. Standardized APIs facilitate effortless deployment in diverse cloud environments, accommodating both public and private cloud infrastructures.

VI. Security Analysis

This section provides a thorough examination of the security attributes provided by the proposed blockchain-based auditing framework.

1) *Data Integrity Assurance:* The framework guarantees the detection of any unauthorized

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

alteration, deletion, or substitution of data during the auditing process. Every data block is labeled with a homomorphic authenticator that facilitates aggregate verification. During an audit, the Cloud Service Provider (CSP) produces a proof of ownership that is verified by the auditing committee in a public manner. Any modification to a single block renders the proof invalid, therefore ensuring integrity based on conventional cryptographic assumptions.

2) *Public Verifiability and Accountability:* All audit evidence and verification outcomes are secured on the blockchain via tamper-proof records. The signature and decision of each committee member are permanently recorded, precluding any denial or modification of audit results. This guarantees non-repudiation and traceability, hence enhancing accountability among all involved parties, including Cloud Service Providers and auditors.

3) *Resistance to Common Attacks:* The suggested system is designed to withstand certain categories of security threats:

Replay Attacks: Timestamped blockchain records inhibit the reutilization of obsolete proofs.

Collusion Attacks: The decentralized committee and consensus voting process inhibit any group of nodes from distorting outcomes.

Forgery Attacks: Homomorphic authenticators and digital signatures render it computationally impractical to generate valid proofs without private keys.

Denial-of-Service (DoS): Off-chain proof generation alleviates the computational load on the blockchain, hence diminishing vulnerability to DoS attacks.

Data Leakage: Federated Learning-based distributed training enables audit models to discern trends without direct access to raw data, hence reducing leakage risks.

VII. Future Research Challenges

Despite the potential benefits of blockchain-based auditing, some obstacles necessitate additional examination:

1) *Scalability and Throughput:* Attaining increased transaction throughput to facilitate regular audits for millions of users continues to pose a hurdle. Investigating more efficient consensus methods (e.g., versions of Proof of Authority) and Layer 2 scaling solutions is essential.

2) *Interoperability:* Establishing common APIs and data formats for interaction among various CSPs, blockchain networks, and auditing systems is essential for broad adoption.

3) *Regulatory Compliance:* Reconciling the immutable nature of blockchain with data protection legislation, such as GDPR's "right to be forgotten," remains an unresolved issue. Methods like chameleon hashes or zero-knowledge proofs may provide avenues for compliant yet verifiable audits.

4) *Energy Efficiency:* Shifting from energy-intensive consensus techniques, like as Proof of Work, to more environmentally friendly alternatives, such Proof of Stake or Proof of Authority, is crucial for sustainable implementation.

5) *Security of Smart Contracts:* Smart contracts are susceptible to vulnerabilities and bugs. Formal verification and sophisticated security auditing methods are essential to guarantee their reliability.

VIII. Conclusion

In this study, we looked at public auditing for cloud data integrity in great detail, focusing on how blockchain technology can positively change things. We looked at traditional accounting methods like PDP and PoR and pointed out their problems with trust and centralization. When blockchain is added, it changes everything. It makes audit records decentralized, clear, and impossible to change. Additionally, the mix of blockchain, AI, and Federated Learning works well together, which makes it possible for smart, flexible, and privacy preserving auditing systems.

The proposed hybrid framework shows how these tools can work together to build a strong auditing ecosystem. There are still problems with scalability, control, and energy use, but progress is being made in distributed systems and cryptography, which makes it clear how to move forward. As cloud computing changes, public auditing that is made easier by blockchain will be necessary to create a secure, trustworthy, and accountable digital infrastructure.

References

[1] M J. Li, J. Wu, G. Jiang, and T. Srikanthan, "Blockchain-based public auditing for big data in cloud storage," *Information Processing & Management*, vol. 57, no. 6, p. 102382, Nov. 2020.

[2] Gartner, "Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023," Gartner Press Release, Apr. 19, 2023. [Online]. https://www.gartner.com/en/newsroom/press-releases/2023-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023. [Accessed: Oct. 17, 2025].

[3] P. Pradhan, "Distributed Data Verification Protocols in Cloud Computing," *arXiv preprint* arXiv:2004.07079, Apr. 2020.

[4] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," Proc. ESORICS, pp. 355–370, 2009.

[5] X. Liang, S. Shetty, D. Bowden, et al., "Towards data assurance and resilience in IoT using blockchain," Proc. IEEE MILCOM, pp. 261–266, 2017.

[6] T. Li, A. S. K. Pathirana, and Q. Wang, "Federated learning for privacy-preserving data analytics: A survey," IEEE Trans. Neural Netw. Learn. Syst., vol. 32, no. 5, pp. 1810–1829, 2021.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

[7] G. Ateniese, R. Burns, R. Curtmola, et al., “Provable data possession at untrusted stores,” Proc. ACM CCS, pp. 598–609, 2007.

[8] A. Juels and B. S. Kaliski Jr., “PORs: Proofs of retrievability for large files,” Proc. ACM CCS, pp. 584–597, 2007.

[9] H. Shacham and B. Waters, “Compact proofs of retrievability,” Proc. ASIACRYPT, pp. 90–107, 2008.

[10] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” Proc. IEEE INFOCOM, pp. 1–9, 2010.

[11] M. Samaniego and R. Deters, “Blockchain as a Service for IoT,” Proc. IEEE iThings and IEEE GreenCom, pp. 433–436, 2016.

[12] L. Zhou, D. Huang, and Z. Wang, “Efficient and privacy-preserving blockchain-based public auditing for cloud storage,” IEEE Access, vol. 7, pp. 5323–5336, 2019.

[13] J. Li, H. Yan, and Y. Zhang, “Blockchain-based public data auditing scheme for cloud storage,” IEEE Access, vol. 7, pp. 46924–46935, 2019.

[14] Y. Zhu, Q. Wang, and Z. Hu, “DecAudit: Decentralized public auditing for cloud storage,” Future Generation Computer Systems, vol. 129, pp. 1–12, 2022.

[15] Y. Ren, J. Shen, and J. Wang, “Mutual verifiable provable data auditing in public cloud storage,” IEEE Trans. Cloud Comput., vol. 5, no. 4, pp. 614–626, 2017.

[16] N. Z. Aitzhan and D. Svetinovic, “Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,” IEEE Trans. Dependable Secure Comput., vol. 15, no. 5, pp. 840–852, 2018.

[17] C. Liu, J. Chen, L. T. Yang, et al., “Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 9, pp. 2234–2244, 2014.

[18] L. Zhang, R. Wang, and J. Liu, “Blockchain-based privacy-preserving data auditing for cloud storage,” IEEE Access, vol. 8, pp. 8345–8357, 2020.

[19] W. Zhao, Y. Zhang, and S. Yu, “Blockchain-based identity management systems: A review,” Journal of Network and Computer Applications, vol. 150, p. 102504, 2020.

[20] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond bitcoin,” Applied Innovation Review, vol. 2, pp. 6–10, 2016.

[21] P. Voigt and A. von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer, 2017.

[22] D. Xu, X. Zhang, and W. Zhang, “Efficient blockchain-based public auditing with decentralized off-chain storage,” IEEE Trans. Cloud Comput., 2023 (early access).