iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 14 **Issue:** VIII **Month of publication:** August 2026

**DOI:** https://doi.org/10.22214/ijraset.2026.84677

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 14 Issue VIII Aug 2026- Available at www.ijraset.com*

# Cloud-Based Auditing System with Efficient Ownership Management for Group Data Transaction: A Literature Survey

Sanjay G P[1], Shashank Gowda T K[2], Srujangouda Malipatil[3], Yashwanth Gowda D K[4]
*Department of Information Science and Engineering, Global Academy of Technology (GAT), Bengaluru, India*

***Abstract:*** ***Cloud computing has become the default medium for storing and sharing large, AI-relevant datasets among organisations, employees, and third-party data consumers. As data ownership increasingly moves between multiple stakeholders rather than a single custodian, existing cloud auditing techniques—largely built around Provable Data Possession (PDP) and Proof of Retrievability (POR)—struggle to provide secure, efficient, and scalable ownership management for group-based data transactions.***

***This paper surveys recent literature (2020-2025) on cloud data auditing, public and privacy-preserving auditing, dynamic data auditing, blockchain-assisted auditing, and ownership transfer mechanisms, with particular emphasis on the recently published scalable cloud auditing protocol with efficient ownership transfer for group transactions. Sixteen representative works are reviewed and compared across technique, advantages, and limitations, revealing recurring weaknesses: quadratic computational overhead when handling dynamic group membership, secret-key exposure during ownership transfer that enables collusion attacks, dependence on fully trusted third parties, and poor support for partial ownership transfer within a shared group. Building on these findings, this paper outlines a research direction for a Cloud-Based Auditing System with Efficient Ownership Management that employs BLS aggregate signatures with hash-bound key pairs, random-mask-protected index keys, and a Third-Party Auditor (TPA) model involving a Sale Group (SG) and a Buy Group (BG) to achieve linear-time ownership modification, resistance to rogue-key and collusion attacks, and low-cost partial or full ownership transfer, without full reliance on a trusted authority.***

***Keywords:*** ***cloud data auditing; provable data possession; ownership transfer; group data sharing; third-party auditor; BLS signatures; privacy-preserving auditing; blockchain-based auditing.***

## I. INTRODUCTION

The rapid expansion of cloud storage, driven by the growing demand for artificial-intelligence datasets, has made outsourced data transactions an everyday business activity. Platforms such as Kaggle and Zenodo distribute large AI-related datasets whose ownership is frequently transferred between employees, research groups, or purchasing organisations through digital signatures . Because verifying the integrity of remotely stored data by downloading it in full is impractical in terms of bandwidth and computation, Provable Data Possession (PDP) and Proof of Retrievability (POR) techniques were introduced to allow integrity verification without full data retrieval.

However, most classical PDP/POR-based auditing schemes were designed for a single data owner. As soon as a dataset is shared and owned jointly by a group—and as that group evolves through member addition, revocation, or complete transfer to another group—existing schemes either fail to preserve secure multi-ownership confirmation, or, when they do address multi-ownership, they fail to scale efficiently because every membership change is treated as an independent group-to-group transfer. Worse, several schemes expose secret keys to untrusted parties during ownership transfer, opening the door to collusion attacks between a dishonest owner and the cloud storage provider.

This paper presents a structured literature survey of cloud auditing, ownership management, and secure group data transfer research published largely between 2020 and 2025. The objective is to (i) understand the evolution of PDP/POR-based auditing, (ii) identify how recent works have attempted to solve multi-owner and ownership-transfer problems, (iii) tabulate the advantages and limitations of each approach, and (iv) motivate a proposed direction—based on BLS aggregate signatures, hash-bound public keys, and random index masking—for a scalable, collusion-resistant, group-oriented cloud auditing and ownership-management system.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com*

## II. BACKGROUND

Cloud auditing research can broadly be organised into four generations of work.

### *A. Provable Data Possession and Proof of Retrievability*

Ateniese et al. introduced the PDP model in 2007, in which the data owner pre-computes homomorphic verifiable tags for file blocks so that a verifier can probabilistically confirm possession of the outsourced data without retrieving it. In the same year, Juels and Kaliski proposed the POR model, which additionally guarantees recoverability of data through erasure codes, although the original POR scheme is state-based and cannot continue auditing once secret information is exposed. Shacham and Waters later introduced Compact POR, which achieves constant-overhead public auditing using BLS-based linear homomorphic tags.

### *B. Dynamic and Privacy-Preserving Auditing*

As cloud data began to change over time, dynamic PDP schemes emerged, supporting insertion, deletion, and modification of stored blocks using structures such as Merkle hash trees, skip lists, and index hash tables. In parallel, privacy-preserving auditing became a priority: random masking, ring signatures, and identity-based/certificateless cryptography were introduced so that a Third-Party Auditor (TPA) could verify integrity without learning the data content or the identity of the specific owner who produced a block.

### *C. Data Possession with Ownership Transfer (DT-PDP)*

The DT-PDP line of work represents data ownership as a signed cryptographic "miniature" of the data, transferable through an Ownership Dynamic Token (ODT) generated via proxy re-signature or random-mask techniques. Wang et al. first proposed DT-PDP for single-owner transfer, after which several works attempted to extend the idea to multiple owners sharing the same file.

### *D. Blockchain-Assisted Auditing*

More recently,blockchain has been combined with cloud auditing to provide immutable revocation records and transparent accountability for multi-ownership transfer, though at the cost of additional consensus-related latency and storage.

## III. LITERATURE SURVEY

This section reviews sixteen representative papers relevant to cloud data auditing, ownership management, and secure group data transfer.

*1)* Wu, You and Huang (2025)

Objective: Enable scalable ownership transfer for group transactions while resisting rogue-key and collusion attacks.

Methodology: BLS aggregate signatures bound to owner identity via a hash function ($\sigma j = (H0(j)u\text{^}mj)\text{^}\{sk \cdot H1(pk)\}$), with random index masks aggregated into public verification parameters; ownership managed through Sale Group (SG) and Buy Group (BG) entities and a semi-trusted Cloud Storage Provider (CSP).

Advantages: O(s) computational overhead for key generation versus $O(s^2)$ in prior work; supports partial ownership transfer without disturbing remaining group members; provably resists collusion and rogue-key attacks under the CDH assumption.

Limitations: Random-mask bookkeeping accumulates with every ownership change; pairing-based operations remain relatively expensive for very large groups.

*2)* Xu, He, Vijayakumar, Gupta and Shen (2023)

Objective: Provide certificateless public auditing with data privacy and dynamics for a group-user model in cloud-assisted medical WSNs.

Methodology: Certificateless cryptography combined with a hash-table index structure maintained by the TPA to support dynamic data operations.

Advantages: Removes certificate-management overhead; supports both dynamic data and dynamic group users in a sensitive healthcare context.

Limitations: Reliance on a hash-table index kept by the TPA reintroduces a semi-trusted third party into the trust model.

*3)* Shen, Gai, Yu and Su (2024)
Objective: Support keyword-based, on-demand remote data-integrity auditing with full data dynamics.
Methodology: Keyword indexing layered on top of homomorphic verifiable tags, allowing an owner to audit only selected data segments.
Advantages: Reduces unnecessary auditing overhead by allowing selective verification; supports full insert/delete/modify operations. Limitations: Additional keyword-index setup cost; the scheme still depends heavily on a TPA for verification.

*4)* Yu and Shen (2024)
Objective: Combine secure cloud storage auditing with data deduplication and efficient data transfer.
Methodology: Deduplication-aware tag generation integrated with a DT-PDP-style transfer mechanism.
Advantages: Reduces storage redundancy while preserving auditability across transferred data.
Limitations: Ownership tracking across deduplicated copies introduces additional indexing complexity.

*5)* Peng, Shen, Yang and Zhang (2025)
Objective: Achieve secure deduplication and cloud storage auditing with efficient dynamic ownership management.
Methodology: Combines deduplication indices with a dynamic ownership-management module supporting owner addition/revocation. Advantages: Supports efficient storage utilisation together with flexible dynamic ownership.
Limitations: Multiple indexing and management structures increase implementation and metadata overhead.

*6)* Qi, Luo, Huang and Li (2023)
Objective: Provide blockchain-based, privacy-preserving group data auditing with secure user revocation.
Methodology: On-chain storage of revocation and ownership records combined with privacy-preserving group signatures.
Advantages: Immutable and transparent revocation history; strong accountability for group membership changes.
Limitations: Blockchain consensus introduces communication latency and additional storage overhead.

*7)* Rabaninejad, Attari, Asaar and Aref (2022)
Objective: Deliver a lightweight auditing service for shared data with secure user revocation.
Methodology: Efficient re-signing of shared-data tags upon revocation, avoiding full re-computation over all data blocks.
Advantages: Low computational cost, well suited to resource-constrained shared-data environments.
Limitations: Primarily addresses single-group revocation; does not fully address group-to-group ownership transfer.

*8)* Zhang, Liu, Liu, Zhang and Xue (2025)
Objective: Support dynamic certificateless outsourced data auditing with multi-ownership transfer via blockchain systems.
Methodology: Certificateless signatures combined with smart-contract-based ownership records.
Advantages: Decentralised trust removes the need for a central ownership authority; supports multi-ownership transfer.
Limitations: On-chain transaction/consensus cost scales with the number of users and transfers.

*9)* Zhang, Yu, Hao, Wang and Ren (2020)
Objective: Enable efficient user revocation in identity-based cloud storage auditing for shared big data.
Methodology: Identity-based cryptography with key-update-based revocation for shared datasets.
Advantages: Simplifies key management; efficient revocation suited to large, shared datasets.
Limitations: Still depends on a trusted Private Key Generator (PKG) and TPA.

*10)* Li, Yan and Zhang (2022)
Objective: Verify multiple copies of data stored across multi-cloud storage using identity-based cryptography.
Methodology: Identity-based homomorphic tags applied to each replica of the data across clouds.
Advantages: Reduces certificate-management overhead relative to PKI-based schemes.
Limitations: Computation and storage costs grow with the number of stored copies.

*11)* Li, Yan and Zhang (2021)
Objective: Provide identity-based, privacy-preserving remote data-integrity checking for cloud storage.
Methodology: Homomorphic tags combined with random masking to hide file-block content and owner identity during audits.
Advantages: Strong privacy preservation for both index and data content.
Limitations: Expensive bilinear-pairing operations limit scalability to very large datasets.

*12)* Gai, Shen, Yang and Yu (2023) — PPADT
Objective: Support privacy-preserving identity-based public auditing with efficient data transfer for cloud-based IoT data.
Methodology: Pseudonym-based identity protection combined with lightweight data-transfer tokens for IoT-generated data.
Advantages: Efficient and privacy-aware auditing suited to resource-constrained IoT devices.
Limitations: Large-scale deployment and key distribution across many IoT nodes remain challenging.

*13)* Kavitha, Basha, Madonna, Sireesha, Tufail and Odeh (2024)
Objective: Provide experimental evaluation of secure and verifiable data-control access using a dynamic cryptographic strategy.
Methodology: Combination of CP-ABE, deniable encryption, and NTRU cryptography for access control.
Advantages: Strong confidentiality and resistance to coercion-based attacks on access credentials.
Limitations: Combining three distinct cryptosystems significantly raises system complexity and processing latency.

*14)* Joshi, Dumka, Raturi, Singh and Kumar (2022)
Objective: Survey and compare cloud data security and privacy measures against common attacks.
Methodology: Comparative review of AES, RSA, ECC, homomorphic encryption, and steganography-based protection.
Advantages: Provides a broad reference point for selecting cryptographic building blocks.
Limitations: A survey rather than a concrete protocol; offers no scalable ownership-management mechanism of its own.

*15)* Siva Kumar, Jagruthi, Vasantha, Pavithra, Siroshini and Supriya (2023)
Objective: Achieve secure and proficient provable data procurity with privacy protection in cloud storage.
Methodology: Privacy-preserving TPA-based auditing with batch verification across multiple data owners.
Advantages: Improves privacy protection and supports simultaneous verification for several owners.
Limitations: High computational cost remains for very large multi-owner batches.

*16)* Wu, Cao, Shen, Chen, Tan and Han (2025)
Objective: Design a lightweight cloud auditing scheme for static data in healthcare information systems.
Methodology: Static-data homomorphic tagging tailored to the performance constraints of healthcare storage systems.
Advantages: Demonstrates that integrity auditing is practical even in sensitive, regulation-heavy environments.
Limitations: Designed only for static data; does not support dynamic ownership or group-based transfer.

## IV. COMPARATIVE ANALYSIS OF EXISTING RESEARCH

Table I summarises the technique, advantages, and limitations of the sixteen surveyed works. The comparison shows a clear trend: schemes that strengthen privacy or add functionality (deduplication, keyword search, blockchain logging, ABE-based access control) tend to do so at the cost of additional computational or communication overhead, while schemes that keep overhead low (e.g., lightweight revocation) tend to sacrifice generality, typically supporting only single-owner or single-group scenarios rather than true group-to-group ownership transfer.

A second observation is that dependence on a fully trusted party—a PKG, a dealer, or a TPA that maintains auxiliary indices—recurs across nearly two-thirds of the surveyed works, which is at odds with the semi-trusted or untrusted cloud-server assumption that motivated PDP research in the first place. Only the blockchain-based and BLS-aggregate-signature-based works reviewed here (references [1], [6], [8]) attempt to reduce this dependence, and even they introduce new costs (consensus latency, mask bookkeeping) in exchange.

TABLE I. Comparative Summary of Surveyed Literature

| Ref. | Author(s) / Year | Technique Used | Advantages | Limitations |
|---|---|---|---|---|
| [1] | Wu, You & Huang (2025) | BLS aggregate signatures, hash-bound key pairs, random index masking | Scalable O(s) group ownership management; resists rogue-key and collusion attacks; supports partial transfer | Random-mask bookkeeping grows with each ownership change; pairing operations still costly for very large s |
| [2] | Xu et al. (2023) | Certificateless auditing with hash-table index maintained by TPA | Removes certificate management overhead; supports dynamic auditing and data transfer for medical WSNs | Depends on a hash-table index kept by TPA, reintroducing a semi-trusted party |
| [3] | Shen, Gai, Yu & Su (2024) | Keyword-based remote integrity auditing with full data dynamics | Enables selective, on-demand verification of specific data segments; reduces unnecessary auditing overhead | Additional keyword-index setup cost; still relies heavily on a TPA |
| [4] | Yu & Shen (2024) | Secure cloud auditing integrated with data deduplication | Reduces storage redundancy while preserving auditability; efficient data transfer support | Deduplication logic adds indexing complexity; ownership tracking across duplicate copies is non-trivial |
| [5] | Peng, Shen, Yang & Zhang (2025) | Deduplication + dynamic ownership management with data-dynamics support | Combines storage efficiency with flexible owner addition/revocation | Multiple indexing structures increase implementation complexity and metadata overhead |
| [6] | Qi, Luo, Huang & Li (2023) | Blockchain-based privacy-preserving group auditing with secure revocation | Immutable, transparent revocation records; strong accountability | Blockchain consensus adds communication latency and storage overhead |
| [7] | Rabaninejad et al. (2022) | Lightweight auditing with secure user revocation for shared data | Low computational cost revocation suited for resource-constrained settings | Limited support for true multi-owner (group-to-group) transfer scenarios |
| [8] | Zhang, Liu, Liu, Zhang & Xue (2025) | Dynamic certificateless auditing with blockchain-assisted ownership transfer | Decentralised trust; supports multi-ownership transfer without a central authority | On-chain operations increase transaction latency; gas/consensus cost scales with users |
| [9] | Zhang, Yu, Hao, Wang & Ren (2020) | Identity-based auditing with efficient key-update revocation | Simplifies key management for shared big data; efficient revocation | Still relies on a trusted Private Key Generator (PKG) and TPA |
| [10] | Li, Yan & Zhang (2022) | Identity-based provable multi-copy possession using homomorphic tags | Reduces certificate overhead; verifies multiple replicas across multi-cloud storage | High computation and storage cost as number of copies grows |
| [11] | Li, Yan & Zhang (2021) | Identity-based privacy-preserving remote integrity checking with random masking | Strong privacy preservation of index/data during auditing | Expensive bilinear pairing operations limit scalability |
| [12] | Gai, Shen, Yang & Yu (2023) — PPADT | Privacy-preserving identity-based auditing with efficient data transfer for IoT | Pseudonym-based privacy; efficient for constrained IoT cloud data | Large-scale deployment and key-distribution remain challenging |
| [13] | Kavitha et al. (2024) | CP-ABE, deniable encryption and NTRU-based access control | Enhances confidentiality and resists coercion-based attacks | High system complexity and latency from combining multiple cryptosystems |
| [14] | Joshi et al. (2022) | Survey of AES, RSA, ECC, homomorphic encryption & steganography for cloud data | Broad comparative view of cryptographic security options | Survey-level; does not propose a concrete scalable auditing/ownership protocol |
| [15] | Dr. C. Siva Kumar et al. (2023) | Privacy-preserving TPA auditing with batch verification for multiple owners | Improves privacy and supports batch verification across owners | High computational cost persists for large-scale multi-owner batches |
| [16] | Wu, Cao, Shen, Chen, Tan & Han (2025) | Lightweight static-data cloud auditing for healthcare systems | Demonstrates practical auditing in sensitive, regulated environments | Designed for static data; lacks dynamic ownership/group-transfer support |

## V. RESEARCH GAP

From the survey and the comparative analysis, it has been found that there are several important research gaps in current cloud auditing and ownership-management methods. A major drawback is poor ownership management, since most of the existing methods assume that ownership is fixed and do not handle the efficient addition or removal of data owners over time. Scalability is also a major issue, as a number of multi-owner auditing schemes—especially those that use public-key aggregation authenticators—suffer from computational complexity that increases quadratically ($O(s^2)$) as the number of owners grows, which means they are not suitable for use in large-scale settings. Key management is another area of concern because some Dynamic Transferable Provable Data Possession (DT-PDP) schemes necessitate the transfer or disclosure of index secret keys when ownership is being transferred, thus compromising the confidentiality of data that has not yet been transferred. Even though identity-based and certificateless cryptographic methods reduce the burden of certificate management, they usually do not protect owner privacy since they reveal the identity of the tag generator or depend on expensive pairing operations. The existing systems also have shortcomings in dynamic user management, as the process of adding or removing owners is typically carried out by transferring all the ownership between separate groups rather than by making an efficient in-place update, which causes unaffected members of the group to have to participate again and carry out recomputations. Moreover, the integration of advanced cryptographic techniques such as Ciphertext-Policy Attribute-Based Encryption (CP-ABE), NTRU encryption, deniable encryption, and blockchain consensus mechanisms greatly increases the computational overhead, resulting in higher latency and greater resource usage. Auditing efficiency is also a problem, as a number of schemes require the Third-Party Auditor (TPA) or the Cloud Service Provider (CSP) to keep large auxiliary index structures, such as hash tables and Merkle trees, and the amount of storage needed increases with the size of the files, thus raising the total cost of auditing. Lastly, secure ownership transfer is not well addressed, with very few of the existing solutions providing both partial ownership transfer without impacting the other members of the group and full group-to-group ownership transfer at the same time while also being resistant to collusion and rogue-key attacks. These limitations show that there is a need for a more efficient, scalable, privacy-preserving, and secure cloud auditing framework with strong ownership management capabilities.

## VI. PROPOSED SYSTEM

The Cloud-Based Auditing System with Efficient Ownership Management has been designed to overcome the research gaps found in current cloud auditing and ownership management schemes by building on the BLS aggregate signature approach suggested by Wu et al. and by introducing a multi-entity architecture made up of the Sale Group (SG), Buy Group (BG), Cloud Service Provider (CSP), and Third-Party Auditor (TPA). In order to achieve efficient ownership management, the system creates file tags using the equation $\sigma j = (H_0(j)u\text{^}mj)\text{^}(sk_i \cdot H_1(pk_i))$, which allows the signatures of multiple owners to be aggregated. This reduces the key generation complexity from $O(s^2)$ to (s) and means that owners can be added to or removed from the group by updating the tags in place, rather than having to carry out complete transfers between groups. Secure key management is achieved by linking each owner's public and secret keys via the hash function $H_1(pk_i)$, which stops attackers from producing fake aggregate signatures using just the public keys and thus makes the system resistant to rogue-key attacks without the need for costly proof-of-possession protocols. The system also supports public auditing via a Third-Party Auditor, who checks data integrity by asking the Cloud Service Provider to provide a randomly chosen subset of data blocks and then verifying a compact aggregate proof, thus avoiding the necessity of downloading the whole dataset while at the same time keeping data confidentiality. To enhance privacy protection, a random index-secret mask is included in each file tag and then combined into the public verification parameter, so that even if the index secret key is revealed during an ownership transfer, it cannot be used to forge tags for data that has not been transferred. Moreover, the proposed model includes a secure group-to-group ownership transfer mechanism in which the Sale Group and Buy Group swap Ownership Dynamic Tokens (ODTs) that allow the Cloud Service Provider to recompute the file tags securely, thereby enabling both partial ownership transfers within a group and complete ownership transfers between different groups. Data integrity is checked using a challenge-response auditing method based on homomorphic verifiable tags, so that verification can be carried out with only a small, fixed-size proof no matter how large the file is. The system also provides better scalability since the cost of modifying ownership depends only on the number of owners being added or removed rather than on the total number of owners, and the cost of updating the tags depends only on the data blocks that are affected, resulting in linear rather than quadratic growth as the group size increases. Furthermore, computational and communication overhead are greatly reduced by means of batch auditing and BLS signature aggregation, which combine several block-level proofs into a single pairing-based verification operation. In summary, the proposed framework effectively tackles the main limitations present in existing cloud auditing schemes by offering efficient ownership management, secure key handling, privacy-preserving public auditing, secure ownership transfer, scalable performance, and reduced computational cost while still maintaining the standard semi-trusted Cloud Service Provider and independent Third-Party Auditor trust model that is used in cloud auditing systems.

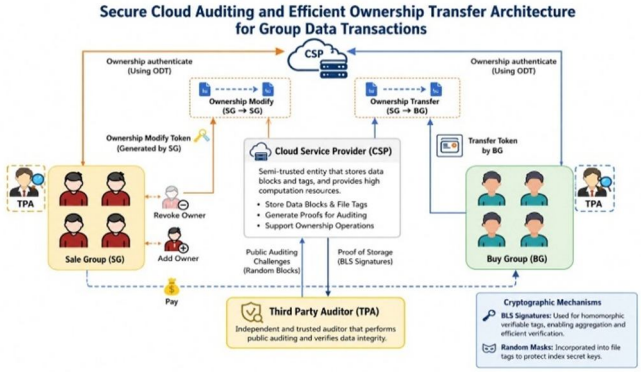


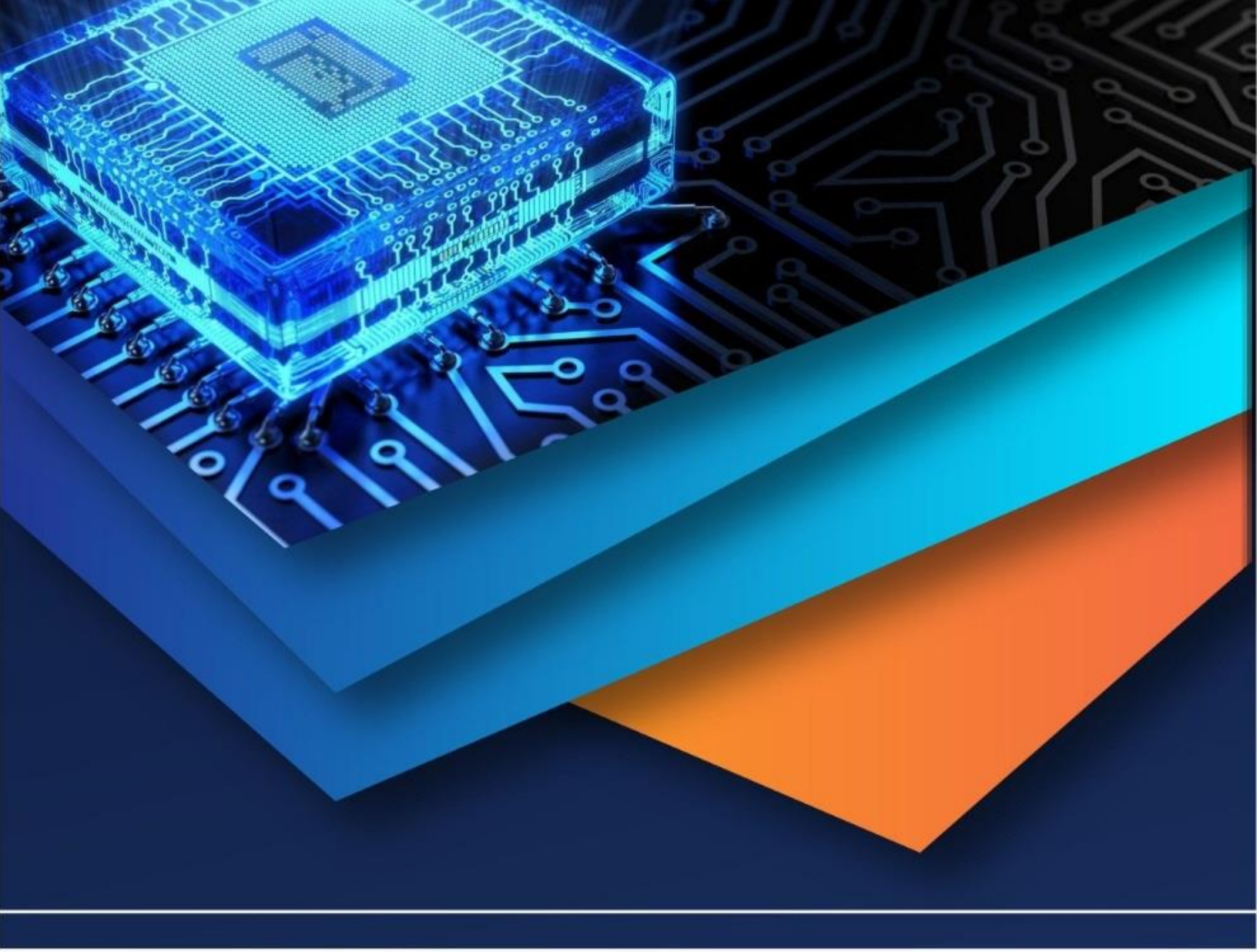

Figure 1: System Architecture

## VII. CONCLUSION

This survey reviewed sixteen representative works spanning classical PDP/POR auditing, dynamic and privacy-preserving auditing, identity-based and certificateless schemes, deduplication-aware auditing, blockchain-assisted ownership management, and the recent scalable BLS-based ownership-transfer protocol for group transactions. The comparative analysis shows that, despite substantial progress in data-integrity verification, existing systems continue to struggle with three intertwined problems: scalable multi-owner key management, secure ownership transfer without key leakage, and reduced dependence on fully trusted parties. The proposed direction—built around hash-bound BLS aggregate signatures, random index masking, and an SG/BG/CSP/TPA system model—offers a concrete path toward a cloud auditing system that supports dynamic, group-oriented data ownership with linear scalability and resistance to collusion and rogue-key attacks. Future work will focus on implementing and experimentally validating this design against the computational and communication benchmarks established in the surveyed literature.

## REFERENCES

[1] C. Wu, W. You, and X. Huang, "Scalable Cloud Auditing With Efficient Ownership Transfer for Group Transactions," IEEE Trans. Inf. Forensics Security, vol. 20, pp. 12665-12679, 2025, doi: 10.1109/TIFS.2025.3636056.
[2] Z. Xu, D. He, P. Vijayakumar, B. B. Gupta, and J. Shen, "Certificateless public auditing scheme with data privacy and dynamics in group user model of cloud-assisted medical WSNs," IEEE J. Biomed. Health Informat., vol. 27, no. 5, pp. 2334-2344, May 2023.
[3] W. Shen, C. Gai, J. Yu, and Y. Su, "Keyword-based remote data integrity auditing supporting full data dynamics," IEEE Trans. Services Comput., vol. 17, no. 5, pp. 2516-2529, Sep. 2024.
[4] J. Yu and W. Shen, "Secure cloud storage auditing with deduplication and efficient data transfer," Cluster Comput., vol. 27, no. 2, pp. 2203-2215, Apr. 2024.
[5] X. Peng, W. Shen, Y. Yang, and X. Zhang, "Secure deduplication and cloud storage auditing with efficient dynamic ownership management and data dynamics," IEEE Trans. Netw. Service Manage., vol. 22, no. 4, pp. 3463-3479, Aug. 2025.
[6] Y. Qi, Y. Luo, Y. Huang, and X. Li, "Blockchain-based privacy-preserving group data auditing with secure user revocation," Comput. Syst. Sci. Eng., vol. 45, no. 1, pp. 183-199, 2023.
[7] R. Rabaninejad, M. A. Attari, M. R. Asaar, and M. R. Aref, "A lightweight auditing service for shared data with secure user revocation in cloud storage," IEEE Trans. Services Comput., vol. 15, no. 1, pp. 1-15, Jan. 2022.
[8] X. Zhang, Q. Liu, B. Liu, Y. Zhang, and J. Xue, "Dynamic certificateless outsourced data auditing mechanism supporting multi-ownership transfer via blockchain systems," IEEE Trans. Netw. Service Manage., vol. 22, no. 2, pp. 2017-2030, Apr. 2025.
[9] Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren, "Enabling efficient user revocation in identity-based cloud storage auditing for shared big data," IEEE Trans. Dependable Secure Comput., vol. 17, no. 3, pp. 608-619, May 2020.
[10] J. Li, H. Yan, and Y. Zhang, "Efficient identity-based provable multi-copy data possession in multi-cloud storage," IEEE Trans. Cloud Comput., vol. 10, no. 1, pp. 356-365, Jan. 2022.
[11] J. Li, H. Yan, and Y. Zhang, "Identity-based privacy preserving remote data integrity checking for cloud storage," IEEE Syst. J., vol. 15, no. 1, pp. 577-585, Mar. 2021.
[12] C. Gai, W. Shen, M. Yang, and J. Yu, "PPADT: Privacy-preserving identity-based public auditing with efficient data transfer for cloud-based IoT data," IEEE Internet Things J., vol. 10, no. 22, pp. 20065-20079, Nov. 2023.
[13] T. Kavitha, Sk. H. Basha, K. W. Madonna, K. Sireesha, Tufail M. S., and M. Odeh, "Experimental evaluation of secure and verifiable data control access over cloud storage environment using dynamic cryptographic strategy," in Proc. ICSES, 2024, doi: 10.1109/ICSES63760.2024.10910755.
[14] A. Joshi, A. Dumka, A. Raturi, D. P. Singh, and S. Kumar, "Improved security and privacy in cloud data security and privacy: Measures and attacks," in Proc. ICFIRTP, 2022, doi: 10.1109/ICFIRTP56122.2022.10063186.
[15] C. Siva Kumar, P. Jagruthi, L. Vasantha, N. Pavithra, P. Siroshini, and T. Supriya, "Secure and proficient provable data procurity with privacy protection in cloud storage," in Proc. ICCCI, 2023, doi: 10.1109/ICCCI56745.2023.10128477.
[16] G. Wu, L. Cao, H. Shen, L. Chen, X. Tan, and J. Han, "Cloud auditing for outsourced storage service in healthcare systems with static data transfer," Electron. Res. Arch., vol. 33, no. 4, pp. 2577-2600, 2022



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY