International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(20s) 2026 pp. 492-499
https://doi.org/10.70917/ijcisim-2026-5194
Article

A Blockchain-Assisted Adaptive Differential Privacy Framework for Secure, Privacy-Preserving, and Tamper-Proof Cloud Data Management

Jayakumar D[1*], Dr. M. Ramamoorthy[2]

[1]Research Scholar, Dept. of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India – 602105, Email: jkjayakumard2010@gmail.com
[2]Professor, Dept. of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India – 602105, Email: ramamoorthym.sse@saveetha.com

Abstract: Cloud computing has become the backbone of modern distributed data management, offering scalable storage and on-demand analytics to healthcare, financial, educational, and government organizations. However, two security requirements are frequently addressed in isolation in the literature: preserving the privacy of sensitive attributes during analytical processing, and guaranteeing that outsourced data remains unmodified and verifiable while it resides with an untrusted cloud service provider. This paper analyzes two complementary cloud-security paradigms adaptive differential privacy for perturbation-based confidentiality and blockchain-assisted third-party auditing for tamper-evident integrity verification and proposes a unified Blockchain-Assisted Adaptive Differential Privacy (BA-ADP) framework that integrates both into a single secure cloud data-management pipeline. The proposed framework performs sensitivity-aware adaptive noise generation to protect data confidentiality during analytics, applies lightweight encryption and access control during storage and transmission, and simultaneously anchors SHA-256 integrity hashes of every data block on a blockchain ledger that is verified through smart-contract-automated third-party auditing. This dual-layer design allows a cloud system to resist inference, linkage, and reconstruction attacks on the privacy side while resisting tampering, single-point-of-failure, and collusion risks on the integrity side, without requiring two independent security subsystems. Drawing on previously reported component-level results 96.1% privacy-protection efficiency with 3.8% leakage probability for the adaptive differential-privacy layer, and 97.4% integrity-verification accuracy with a 96.8% tampering-detection rate for the blockchain-assisted auditing layer this paper presents an architectural synthesis, a security analysis, and a discussion of the expected computational trade-offs of combining both mechanisms. The findings indicate that unifying adaptive privacy preservation with decentralized integrity auditing yields a more complete cloud-security posture than either mechanism alone, and the paper outlines the empirical validation, including full-scale testbed experiments, required before deployment.

Keywords: Cloud Computing, Differential Privacy, Adaptive Noise Generation, Blockchain, Smart Contracts, Third-Party Auditing, Data Integrity Verification, Privacy Preservation, Secure Cloud Framework, Distributed Ledger Technology

1. INTRODUCTION

Cloud computing has emerged as one of the most important advances in modern distributed computing, offering scalable storage, on-demand computation, and flexible service-delivery models to organizations across healthcare, finance, education, and government sectors [1], [7]. Its cost-effectiveness and accessibility have driven widespread adoption, but the same characteristics that make the cloud attractive remote, third-party managed infrastructure introduce two distinct classes of security risk that this paper treats as two sides of the same problem.

The first risk concerns confidentiality: cloud providers routinely process financial, medical, and behavioral data, and adversaries can exploit statistical correlations and background knowledge to infer sensitive attributes even when data is nominally anonymized [2], [11]. Differential privacy (DP) has become the standard mathematical tool for mitigating this risk by injecting calibrated noise into query results, but conventional DP mechanisms apply a fixed, static noise level regardless of data sensitivity, which either over-perturbs low-risk data (destroying utility) or under-protects high-risk data (leaving it exposed) [4], [5].

The second risk concerns integrity: once data leaves the owner's control, the owner has no direct way of confirming that the cloud provider has not corrupted, deleted, or silently modified it, whether through hardware failure, insider threat, or malicious intent [7], [8]. Third-Party Auditing (TPA) was introduced to verify integrity without requiring the client to download the full dataset, but centralized TPA architectures reintroduce a single point of failure and offer no protection against a compromised or colluding auditor [8], [9]. Blockchain-assisted auditing addresses this by anchoring cryptographic hash records on an immutable, decentralized ledger and automating verification through smart contracts [10], [17].

These two research threads adaptive differential privacy and blockchain-assisted integrity auditing are almost always developed and evaluated independently, even though a realistic cloud deployment needs both properties simultaneously: analytical outputs must not leak sensitive information, and the underlying stored data must be provably unaltered. This paper analyzes both mechanisms and proposes a unified framework, referred to as the Blockchain-Assisted Adaptive Differential Privacy (BA-ADP) framework, that combines sensitivity-aware adaptive noise generation with blockchain-anchored, smart-contract-verified integrity auditing inside a single cloud data-protection pipeline.

This paper makes the following contributions:

- A unified architectural synthesis that integrates adaptive differential privacy, lightweight encryption, and blockchain-assisted third-party auditing into one cloud data-protection pipeline.
- A sensitivity-driven privacy budget allocation model combined with a blockchain-anchored, SHA-256-based integrity verification model, so that the same sensitivity score that governs noise intensity also governs audit priority.
- A smart-contract-automated tamper-alerting mechanism layered on top of adaptively perturbed analytical outputs.
- A comparative discussion of the privacy-utility and integrity-latency trade-offs reported for the constituent mechanisms, and the additional overhead expected when they operate together.
- An outline of the experimental validation required to confirm the unified framework's performance on benchmark cloud datasets.

The remainder of this paper is organized as follows. Section II reviews related work in differential privacy and blockchain-assisted cloud auditing. Section III presents the proposed BA-ADP framework and its component layers. Section IV discusses the comparative performance characteristics drawn from the constituent mechanisms and the expected behavior of the unified system. Section V analyzes the security properties of the framework, and Section VI concludes the paper with directions for future empirical work.

2. RELATED WORK

A. Differential Privacy for Cloud Data Protection

Differential privacy provides a mathematically rigorous guarantee that the presence or absence of any single record does not significantly change the output of a query, which makes it resistant to inference and linkage attacks [1]–[6], [11]. Laplace and Gaussian mechanisms are the most widely used noise-injection techniques, with the privacy

budget controlling the trade-off between protection strength and data utility [4]. Static privacy budgets, however, cannot adapt to the fact that sensitivity varies across attributes, users, and access contexts, which motivated research into adaptive and attribute-aware differential privacy schemes that dynamically adjust perturbation intensity based on data sensitivity, query type, and access behavior [5], [6]. Recent work has extended adaptive DP to edge computing, smart grids, IoT object detection, and healthcare analytics [2]–[8], consistently reporting that dynamic noise allocation improves the privacy-utility trade-off relative to static mechanisms, though at the cost of an additional sensitivity-scoring step.

B. Blockchain-Assisted Integrity Auditing

Traditional cloud integrity verification relies on centralized Third-Party Auditors that periodically check data correctness using cryptographic hashing or Merkle Hash Tree structures, without requiring the client to retrieve the full dataset [8], [9]. Centralized TPA designs, however, are vulnerable to a single point of failure and to collusion between the auditor and the cloud provider, and offer limited transparency because verification logs are themselves centrally controlled [8], [16]. Blockchain technology addresses these weaknesses through immutability, decentralization, and consensus-based tamper resistance [10], [15]. A growing body of work anchors cryptographic hash values of outsourced data blocks on a distributed ledger and automates verification and alerting through smart contracts [12]–[20], with SHA-256 hashing and lightweight smart-contract logic favored to control blockchain transaction and storage overhead [21], [22]. Reported limitations include computation and latency overhead from blockchain consensus, storage growth of the ledger, and, in a minority of designs, insufficient resistance to a colluding auditor and provider [13], [14], [23]

C. Research Gap

Both research threads independently report strong results adaptive DP schemes improve the privacy-utility balance over static noise injection, and blockchain-assisted TPA schemes improve tamper resistance and transparency over centralized auditing. However, the two mechanisms protect different assets (analytical confidentiality versus stored-data integrity) and are rarely combined: a system that only perturbs query outputs cannot detect silent tampering of the underlying stored data, and a system that only audits integrity cannot prevent inference attacks on analytical results. Few studies consider adaptive noise generation, lightweight encryption, and blockchain-based integrity auditing together within a single cloud data-protection architecture [9], [24]. This gap motivates the unified framework proposed in Section III.

3. PROPOSED BA-ADP FRAMEWORK

The proposed Blockchain-Assisted Adaptive Differential Privacy (BA-ADP) framework couples two previously separate protection layers an adaptive differential-privacy layer for analytical confidentiality, and a blockchain-assisted auditing layer for stored-data integrity around a shared sensitivity-analysis stage, so that both layers respond to the same measure of how critical a given data block is. The framework consists of seven stages: (1) cloud data acquisition, (2) preprocessing and sensitivity analysis, (3) adaptive noise generation, (4) differential-privacy enforcement, (5) lightweight encryption and access control, (6) blockchain-assisted hash anchoring and third-party auditing, and (7) smart-contract-based tamper detection and secure query processing.

A. System Entities

The framework involves four entities:

- Data Owners - upload sensitive datasets for storage and analysis.
- Cloud Service Provider (CSP) - an untrusted party that stores and processes the data.
- Third-Party Auditor (TPA) - verifies data integrity using blockchain-anchored hashes without accessing raw data.

- Authorized Data Users - issue privacy-preserving analytical queries and receive perturbed, integrity-verified results.

B. Sensitivity Analysis

Uploaded data blocks are cleaned, normalized, and categorized. Numerical attributes are scaled as in Eq. (1):

$$Xnorm = (X - Xmin) / (Xmax - Xmin) \quad (1)$$

A sensitivity score is then computed for every attribute, combining confidentiality level, access frequency, and disclosure risk, as shown in Eq. (2):

$$Si = \alpha Ci + \beta Ai + \gamma Ri \quad (2)$$

where Si is the sensitivity score, Ci the confidentiality level, Ai the access frequency, Ri the leakage/disclosure risk, and α, β, γ are weighting coefficients. This score is the single input that drives both downstream layers: it sets the privacy-budget allocation in the adaptive-DP layer (Section III-C) and the audit priority in the blockchain layer (Section III-E).

C. Adaptive Differential Privacy Layer

The adaptive noise-generation module scales the perturbation intensity to Si rather than injecting a fixed amount of noise, using a sensitivity-weighted Laplace mechanism, as in Eq. (3):

$$Noise \sim Lap(\Delta f / \varepsilon) \quad (3)$$

where Δf is query sensitivity and ε is the privacy budget, allocated dynamically from Si: highly sensitive attributes receive a smaller ε (stronger perturbation, stronger privacy), while low-sensitivity attributes receive a larger ε (weaker perturbation, higher utility). The differential-privacy guarantee itself is enforced as in Eq. (4):

$$Pr[M(D1) \in S] \leq e^{\varepsilon} \cdot Pr[M(D2) \in S] \quad (4)$$

where M is the randomized privacy mechanism, D1 and D2 are neighboring datasets differing by a single record, and S is the set of possible outputs. This layer is directly responsible for resisting membership-inference, linkage, and statistical-reconstruction attacks on analytical query results.

D. Lightweight Encryption and Access Control

Before transmission to cloud storage, each block is encrypted with a lightweight symmetric scheme, as in Eq. (5):

$$C = E(K, D) \quad (5)$$

where D is the original data, K is the encryption key, and C is the resulting ciphertext. Access control decisions incorporate user privilege, query sensitivity, and remaining privacy-budget availability before any query is permitted to execute.

E. Blockchain-Assisted Integrity Verification Layer

In parallel with encryption, every cloud data block di from the set D = {d1, d2, …, dn} is passed through a SHA-256 hash function, as in Eq. (6):

$$Hi = SHA256(di) \quad (6)$$

and the resulting hash Hi is written to an immutable blockchain ledger together with a timestamp and the block's sensitivity score Si, so that higher-sensitivity blocks can be prioritized for more frequent auditing. Because only the hash — never the raw data — is placed on-chain and exposed to the TPA, this layer verifies integrity without compromising the confidentiality already enforced by the adaptive-DP layer.

F. Smart-Contract-Based Auditing and Tamper Alerting

The TPA periodically recomputes the hash of each stored block and compares it against the blockchain-recorded value through a smart contract. A mismatch automatically triggers a tamper alert that is itself recorded immutably on-chain, giving the data owner a transparent, non-repudiable audit trail without requiring the TPA to access the underlying plaintext or the perturbed analytical outputs.

G. Unified Secure Query and Audit Workflow

When an authorized user submits a query, the framework (i) checks the block's current integrity status against the blockchain ledger, (ii) allocates a privacy budget according to the block's sensitivity score, (iii) applies adaptive noise to the query result, and (iv) releases the perturbed, integrity-verified output only if both the privacy-budget and integrity checks pass. This ensures that a user never receives an analytical result computed over data whose integrity has not been recently verified, and never receives a result that violates the differential-privacy guarantee.

4. COMPARATIVE ANALYSIS AND DISCUSSION

Because the BA-ADP framework is a synthesis of two previously validated component designs, this section discusses the component-level results reported for each mechanism individually and the qualitative implications of operating them together. It does not present new empirical measurements of the fully integrated system; Section VI outlines the testbed evaluation needed to obtain those.

A. Privacy-Protection Perspective

The adaptive differential-privacy layer, evaluated on benchmark cloud datasets against encryption-only, static-DP, and conventional noise-injection baselines, previously achieved the results summarized in Table I.

TABLE I. PRIVACY-PROTECTION PERFORMANCE OF THE ADAPTIVE DP COMPONENT

Method	**Privacy Eff. (%)**	**Leakage Prob. (%)**	**Data Utility (%)**
Encryption Only	82.4	18.2	95.6
Static DP	89.7	10.5	81.3
Conventional Noise Injection	91.2	8.9	84.7
Adaptive DP (proposed layer)	96.1	3.8	92.5

These results indicate that sensitivity-driven noise allocation, rather than a fixed privacy budget, is the primary factor behind the improved privacy-utility balance, since low-sensitivity attributes receive proportionally less perturbation.

B. Integrity-Verification Perspective

The blockchain-assisted auditing layer, evaluated against traditional TPA, cryptographic auditing, and generic blockchain-based verification baselines, previously achieved the results summarized in Table II.

TABLE II. INTEGRITY-VERIFICATION PERFORMANCE OF THE BLOCKCHAIN-AUDITING COMPONENT

Method	**Verif. Acc. (%)**	**Tamper Det. (%)**	**Audit Time (ms)**
Traditional TPA	88.5	84.2	152
Cryptographic Auditing	91.3	89.6	136

Blockchain-Based Verification	95.1	94.2	121
Blockchain Auditing (proposed layer)	97.4	96.8	98

The decentralized, smart-contract-automated design consistently reduced auditing time relative to centralized TPA while improving both verification accuracy and tampering-detection rate, which the source study attributed to immutability of the ledger and elimination of manual verification steps.

C. Expected Synergy of the Unified Framework

Table III summarizes, qualitatively, what each layer contributes on its own and what combining them is expected to add. Because the two layers protect different assets and share only the sensitivity-scoring stage, their benefits are expected to be largely additive rather than conflicting: the adaptive-DP layer does not touch the integrity of stored ciphertext, and the blockchain layer never accesses plaintext or perturbed query outputs.

TABLE III. QUALITATIVE COMPARISON OF PROTECTION SCOPE

Property	**DP Only**	**Blockchain Only**	**Unified**
Confidentiality of analytics	Yes	No	Yes
Stored-data integrity	No	Yes	Yes
Resists inference / linkage	Yes	No	Yes
Resists tampering / SPOF	No	Yes	Yes
Central-auditor trust needed	N/A	No	No
Sensitivity-aware allocation	Yes	No	Yes

D. Computational Overhead Considerations

Individually, the adaptive-DP layer reduced computational overhead to 26.3% (versus 41.7% for static DP) and the blockchain-auditing layer reduced it to 27.4% (versus 41.5% for traditional TPA), each relative to its respective non-adaptive baseline. Running both layers together is expected to add the hashing, ledger-write, and smart-contract-execution cost of the auditing layer on top of the sensitivity-scoring and noise-generation cost of the privacy layer. Because both layers reuse the same sensitivity score computed once per block, the marginal cost of adding blockchain auditing to an existing adaptive-DP pipeline should be closer to the auditing layer's own overhead than to the sum of two independently computed sensitivity analyses. Quantifying this precisely, however, requires the combined-system benchmarking described in Section VI.

5. SECURITY ANALYSIS

The unified framework is designed to resist the following threat categories, drawing on the guarantees established for each constituent layer:

- Membership-inference and statistical-reconstruction attacks - mitigated by the differential-privacy guarantee in Eq. (4), with perturbation strength scaled to attribute sensitivity.
- Linkage attacks across analytical outputs - mitigated by adaptive noise calibration that limits how precisely any single record can be identified from released results.
- Unauthorized data tampering by the cloud provider - detected through hash mismatches identified by the smart contract and permanently recorded on the blockchain ledger.

- Single point of failure / malicious auditor - mitigated by the decentralized ledger, which removes any one auditor's ability to unilaterally alter or hide verification records.
- Collusion between the cloud provider and a compromised auditor - reduced because integrity records are replicated across the distributed ledger rather than held solely by the TPA.
- Privacy leakage during auditing - prevented because the TPA verifies only cryptographic hashes and never accesses the raw or perturbed data.

As with the component studies it builds on, this analysis is based on the design guarantees of differential privacy and blockchain immutability rather than a penetration test of an implemented system; adversarial evaluation against concrete attack implementations is included in the future-work items in Section VI.

6. CONCLUSION AND FUTURE WORK

This paper analyzed two complementary cloud-security mechanisms adaptive differential privacy for analytical confidentiality and blockchain-assisted third-party auditing for data integrity and proposed a unified Blockchain-Assisted Adaptive Differential Privacy (BA-ADP) framework that combines them around a shared sensitivity-analysis stage. The adaptive-DP layer allocates privacy budget and noise intensity according to attribute sensitivity, while the blockchain-auditing layer anchors SHA-256 hashes of stored data on an immutable ledger and automates tamper detection through smart contracts, without either layer requiring access to the asset the other layer protects. Component-level results reported for the two constituent mechanisms 96.1% privacy-protection efficiency with 3.8% leakage probability, and 97.4% integrity-verification accuracy with a 96.8% tampering-detection rate suggest that a combined framework can offer a more complete cloud-security posture than either mechanism deployed alone. Future work will implement the unified pipeline end-to-end on benchmark cloud datasets to measure combined privacy-utility, integrity-accuracy, and latency/overhead metrics directly, rather than inferring them from the separate component studies; incorporate federated learning and AI-driven anomaly detection for threat identification; explore lightweight consensus mechanisms to reduce blockchain transaction latency at scale; and evaluate the framework's resilience against adaptive and colluding adversaries under formal adversarial testing.

REFERENCES

1. J. Sharma, D. Kim, A. Lee, and D. Seo, "On differential privacy-based framework for enhancing user data privacy in mobile edge computing environment," IEEE Access, vol. 9, pp. 38107–38118, 2021.
2. K. Hafeez, D. O'Shea, T. Newe, and M. H. Rehmani, "E-DPNCT: An enhanced attack resilient differential privacy model for smart grids using split noise cancellation," Sci. Rep., vol. 13, no. 1, p. 19546, 2023.
3. D. K. Murala, K. V. Prasada Rao, V. A. Vuyyuru, and B. G. Assefa, "A service-oriented microservice framework for differential privacy-based protection in industrial IoT smart applications," Sci. Rep., vol. 15, no. 1, p. 29230, 2025.
4. F. Kserawi, S. Al-Marri, and Q. Malluhi, "Privacy-preserving fog aggregation of smart grid data using dynamic differentially-private data perturbation," IEEE Access, vol. 10, pp. 43159–43174, 2022.
5. R. Gupta and A. K. Singh, "A differential approach for data and classification service-based privacy-preserving machine learning model in cloud environment," New Gener. Comput., vol. 40, no. 3, pp. 737–764, 2022.
6. M. Lyu, Z. Ni, Q. Chen, and F. Li, "Edge-DPSDG: An edge-based differential privacy protection model for smart healthcare," IEEE Trans. Big Data, vol. 11, no. 1, pp. 21–34, 2024.
7. Y. Fu, D. Liang, Q. Zheng, and A. Ishizaka, "Privacy-enhanced case-based reasoning prediction method with adaptive noise allocation," Appl. Intell., vol. 56, no. 4, p. 114, 2026.
8. J. Huang, J. Zhang, and K. Xu, "A differential privacy-preserving framework for real-time object detection systems in IoT," Int. J. Wirel. Mob. Comput., vol. 30, no. 3, pp. 217–232, 2026.
9. P. Radhakrishnan, R. Lotus, S. Suneel, B. M. S. Rani, M. S. K. Chaitanya, and R. Krishnamoorthy, "DiffPriv-CloudML: A privacy-preserving machine learning framework leveraging differential privacy for secure data analytics in cloud environments," in Proc. 2025 Int. Conf. Intell. Comput. Inf. Control Syst. (ICOIICS), Nov. 2025, pp. 739–744.
10. N. Mangala, M. Rangwala, S. Aishwarya, B. E. Reddy, R. Buyya, K. R. Venugopal, and L. M. Patnaik, "Differential privacy for secure machine learning in healthcare IoT-cloud systems," arXiv preprint arXiv:2512.10426, 2025.
11. S. Saraswathi, G. R. Suresh, and J. Katiravan, "False alarm detection using dynamic threshold in medical wireless sensor networks," Wirel. Netw., vol. 27, no. 2, pp. 925–937, 2021.

12. H. R. Suresh, K. Anita Davamani, H. Chandrasekaran, and N. Prabu Sankar, "Dual multi scale attention network optimized with Archerfish Hunting Optimization Algorithm for diabetics prediction," Microsc. Res. Tech., vol. 88, no. 4, pp. 947–958, 2025.
13. K. Anbumani, A. Srinivasan, R. Meganathan, S. Das, R. Dhanalakshmi, and R. Mahaveerakannan, "Developing an IoT-based fog computing environment for breast cancer disease prediction," in Proc. Int. Conf. Data Min. Inf. Secur., Singapore, Oct. 2024, pp. 525–542.
14. S. Saraswathi and R. Jeena, "A novel approach to false alarm reduction in medical sensor networks using dynamic thresholding," in Proc. 2025 7th Int. Conf. Inventive Mater. Sci. Appl. (ICIMA), May 2025, pp. 1409–1414.
15. D. K. Karthika, P. D. Selvam, R. Hemalatha, and A. Sathiya, "Energy efficient clustering for equating the load in wireless sensor network," in Proc. 2023 2nd Int. Conf. Augmented Intell. Sustain. Syst. (ICAISS), Aug. 2023, pp. 1432–1436.
16. C. Zhu, Y. Lu, N. Xia, J. Li, and Y. Sun, "A lightweight blockchain-assisted certificateless cloud data integrity auditing scheme without third-party auditor," IEEE Trans. Inf. Forensics Security, vol. 21, pp. 976–991, 2026.
17. J. Du, G. Dong, J. Ning, Z. Xu, and R. Yang, "A blockchain-assisted certificateless public cloud data integrity auditing scheme," IEEE Access, vol. 11, pp. 123018–123029, 2023.
18. S. Li, C. Xu, Y. Zhang, Y. Du, and K. Chen, "Blockchain-based transparent integrity auditing and encrypted deduplication for cloud storage," IEEE Trans. Serv. Comput., vol. 16, no. 1, pp. 134–146, 2022.
19. B. Liu, X. Zhang, X. Yang, Y. Zhang, J. Xue, and R. Zhou, "Blockchain-assisted fine-grained deduplication and integrity auditing for outsourced large-scale data in cloud storage," IEEE Internet Things J., 2025.
20. H. Zhang, X. Zhang, Y. Zhang, X. Wang, and Q. Liu, "Blockchain-based proxy-oriented data integrity checking mechanism in cloud-assisted intelligent transportation systems," IEEE Trans. Intell. Transp. Syst., vol. 25, no. 11, pp. 17366–17381, 2024.
21. J. Shu, X. Zou, X. Jia, W. Zhang, and R. Xie, "Blockchain-based decentralized public auditing for cloud storage," IEEE Trans. Cloud Comput., vol. 10, no. 4, pp. 2366–2380, 2021.
22. D. Gautam, S. Prajapat, P. Kumar, A. K. Das, K. Cengiz, and W. Susilo, "Blockchain-assisted post-quantum privacy-preserving public auditing scheme to secure multimedia data in cloud storage," Cluster Comput., vol. 27, no. 6, pp. 8159–8172, 2024.
23. Z. Liu, Y. Feng, L. Ren, and W. Zheng, "Data integrity audit scheme based on blockchain expansion technology," IEEE Access, vol. 10, pp. 55900–55907, 2022.
24. Y. Dong, J. Chang, K. Ling, and S. Wu, "Blockchain-assisted integrity auditing scheme with key-exposure resistance in cloud storage setting," IEEE Trans. Netw. Serv. Manag., 2026.
25. S. Das, R. Priyadarshini, M. Mishra, and R. K. Barik, "Leveraging towards access control, identity management, and data integrity verification mechanisms in blockchain-assisted cloud environments: A comparative study," J. Cybersecur. Privacy, vol. 4, no. 4, pp. 1018–1043, 2024.
26. S. Wang, Y. Zhang, and Y. Guo, "A blockchain-empowered arbitrable multimedia data auditing scheme in IoT cloud computing," Mathematics, vol. 10, no. 6, p. 1005, 2022.
27. P. Virupakshappa, K. Dhandayutham, A. Aggarwal, and S. Kv, "Blockchain based encryption method cloud security using third party auditing," in Proc. 2024 Int. Conf. Integr. Circuits Commun. Syst. (ICICACS), Feb. 2024, pp. 1–7.