Sandeep Gajanan Sutar, 2025, 13:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Enhancing Data Security: The Synergy of Blockchain and Homomorphic Cryptosystems in Cloud Privacy Management

[1]Sandeep Gajanan Sutar, [2]Dr. Praveen B M, [3]Dr. Amolkumar Jadhav

[1]Post Doc Fellow, Srinivas University, Manglore, India & Faculty, Dr. D. Y. Pratishthan's College of Engineeering, Kolhapur, India;
[2]Faculty, Srinivas University, Mangalore, India;
[3]Faculty, Annasaheb Dange College of Engineering and technology, Ashta, India;

Abstract- In the era of pervasive cloud computing, ensuring the privacy and integrity of sensitive data has emerged as a critical challenge. Traditional data protection methods often fall short in addressing sophisticated security threats and compliance demands. This study explores the synergistic integration of blockchain technology and homomorphic encryption (HE) as a transformative approach to privacy management in cloud environments. Blockchain's decentralized and immutable architecture ensures transparent, tamper-proof data transactions, while homomorphic encryption enables computation on encrypted data without revealing its contents—thus preserving confidentiality throughout the data lifecycle. The research discusses layered architectural frameworks, real-world implementations across healthcare, IoT, and supply chains, and presents empirical findings that highlight improvements in computational efficiency, security, and regulatory compliance. Despite challenges in scalability and computational overhead, the combined use of blockchain and HE presents a promising pathway for developing resilient, privacy-preserving cloud infrastructures. This integration not only fortifies data governance but also lays the groundwork for next-generation secure cloud services.

Keywords - Homomorphic Encryption, Blockchain Technology, Cloud Privacy Management, Data Security, Secure Computation,

I. INTRODUCTION

Cloud computing has emerged as a transformative paradigm, enabling organizations to scale operations, reduce infrastructure costs, and access data ubiquitously. However, this shift has also heightened concerns over data privacy and security, especially as sensitive information is increasingly stored and processed in third-party environments (Gandhi et al., 2025). Traditional methods such as data masking, access controls, and pseudonymization, while foundational, often fail to secure data throughout its lifecycle—particularly during processing, where decryption is typically required (Kambala, 2025).

This limitation has driven the exploration of advanced cryptographic techniques that allow privacy to be preserved even during computation. One such innovation is homomorphic encryption (HE), which enables operations on encrypted data without decryption, thus maintaining confidentiality throughout the computation process (Akindote et al., 2024; Gentry, 2009). HE schemes such as Fully Homomorphic Encryption (FHE) allow unlimited additions and multiplications, making them particularly suitable for cloud-based analytics where sensitive data must remain private (Brakerski & Vaikuntanathan, 2011; Akindote et al., 2024).

Simultaneously, blockchain technology has proven valuable in enhancing data integrity, transparency, and traceability. Through its decentralized architecture and immutable ledger, blockchain offers a tamper-resistant framework that removes the need for centralized trust (Punia et al., 2024; Sasikumar & Nagarajan, 2024). Each transaction recorded on a blockchain is verifiable and traceable, ensuring accountability and reducing risks associated with unauthorized data alterations (Ahirao et al., 2024).

Individually, both blockchain and HE address distinct dimensions of cloud security—integrity and confidentiality, respectively. However, recent research indicates that their integration provides a robust framework for secure, privacy-preserving computation in untrusted environments (Mahato et al., 2024; Zhang et al., 2025). For instance, in healthcare applications, encrypted patient data can be processed using HE while blockchain ensures auditability and access control via smart contracts (Lopez et al., 2024). Similarly, in supply chain systems, stakeholders can compute analytics over encrypted logistics data while maintaining transparency through distributed ledger entries (Din et al., 2025).

This paper presents a comprehensive exploration of the integration of homomorphic encryption and blockchain technologies for enhanced data security in cloud environments. Drawing on empirical findings, case studies, and architectural analyses, it investigates the performance, regulatory alignment, and sector-specific applications of this synergistic model. By doing so, it aims to demonstrate how the convergence of these technologies addresses modern privacy challenges while aligning with stringent data protection regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) (Gandhi et al., 2025; Ahirao et al., 2024).

II. LITERATURE REVIEW

The intersection of blockchain technology and homomorphic encryption (HE) has garnered significant attention in recent years as a means to address privacy and security challenges in cloud environments. This section provides a critical review of the current state of research on both technologies, their individual strengths, and the implications of their integration across domains such as healthcare, supply chain, and IoT.

Homomorphic Encryption in Cloud Privacy

Homomorphic encryption enables computations on encrypted data without requiring decryption, thereby preserving confidentiality throughout the processing lifecycle. This property is especially valuable in cloud computing, where sensitive data is often handled by third-party service providers. Akindote et al. (2024) emphasize HE's ability to protect encrypted datasets in project management and logistics, allowing secure computation without revealing the plaintext.

HE schemes are typically categorized as partially homomorphic (PHE), somewhat homomorphic (SHE), or fully homomorphic (FHE). PHE supports either addition or multiplication (e.g., RSA), SHE supports limited operations, while FHE allows arbitrary computations (Gentry, 2009; Brakerski et al., 2016). However, FHE is often limited by computational overhead and latency, which can restrict its practical deployment in real-time systems (Xie et al., 2024).

Recent advancements have sought to optimize HE's efficiency through parallel processing and lightweight protocol design. Mahato et al. (2024) propose integrating HE with federated learning to enable secure data collaboration in untrusted environments. Gandhi et al. (2025) similarly highlight HE's role in secure healthcare analytics, particularly in enabling collaborative machine learning without compromising patient privacy.

Blockchain as a Trust and Integrity Layer

Blockchain is a distributed ledger technology (DLT) that ensures tamper-proof, verifiable, and decentralized data storage. Its core features—decentralization, immutability, and consensus—enable secure and transparent data governance in cloud systems (Punia et al., 2024; Sasikumar & Nagarajan, 2024).

The technology's resilience against unauthorized alterations makes it ideal for logging access, enforcing data-sharing policies, and facilitating auditability. Ahirao et al. (2024) discuss the regulatory implications of blockchain's immutability in light of GDPR's "right to be forgotten," emphasizing the need for compliant architectural adaptations.

Use cases in distributed environments highlight blockchain's potential. For example, in health data management, blockchain ensures traceability and

access control while enabling interoperability among stakeholders (Lopez et al., 2024). In supply chains, Din et al. (2025) demonstrate how blockchain-based platforms support secure monitoring of asset movements and verify transaction authenticity.

Integrated Frameworks: Synergy of Blockchain and HE

The fusion of HE and blockchain presents a paradigm shift for privacy-preserving cloud infrastructures. HE safeguards data confidentiality during computation, while blockchain ensures integrity and accountability. Together, they allow secure, auditable operations on encrypted data—addressing the dual challenge of privacy and trust in decentralized environments (Mahato et al., 2024; Zhang et al., 2025).

Zhang et al. (2025) propose a hybrid model using Ethereum and Paillier encryption to facilitate encrypted analytics in healthcare clouds. Their results show minimal latency and robust protection against data breaches. Similar frameworks have employed smart contracts to govern data access while ensuring compliance with regulatory mandates like HIPAA and GDPR (Gandhi et al., 2025; Ahirao et al., 2024).

Research by Shankar et al. (2024) explores blockchain and HE in the context of smart city applications, emphasizing decentralized governance and privacy. Tamboli and Arage (2024) further introduce AI into this ecosystem, showing how anomaly detection and predictive models can enhance real-time privacy enforcement.

Despite these advances, challenges remain—particularly regarding scalability, computational load, and standardization. Xie et al. (2024) argue that HE's efficiency must improve through optimized parameter tuning and distributed processing. The need for interoperable protocols and regulatory harmonization is also stressed by Asaad and Zeebaree (2024). data.

III. PROPOSED METHODOLOGY

This study investigates the integration of blockchain technology and homomorphic encryption (HE) to address the critical concerns of data privacy and security in cloud environments. The methodology is structured around the analysis of an integrated multi-layered framework supported by empirical case studies and simulation-based validation reported in existing literature.

Research Design

The methodological approach is primarily qualitative and analytical, incorporating insights from peer-reviewed studies, architectural evaluations, and experimental implementations. The research is guided by three key objectives:

- To examine the architectural design combining blockchain and HE for secure cloud computing.
- To evaluate performance metrics such as computational efficiency, latency, and privacy assurance.
- To assess real-world applicability across domains including healthcare, supply chain, and IoT.
- The framework adopted closely aligns with that proposed by Mahato et al. (2024), which defines a three-layer architecture: the application layer, blockchain layer, and homomorphic encryption layer.

Architectural Framework

The application layer serves as the interface between end-users and the system, facilitating data upload, access, and encrypted queries. The blockchain layer provides immutable storage and transaction verification using smart contracts. Public or consortium blockchains such as Ethereum or Hyperledger Fabric are employed to maintain transparency and integrity (Zhang et al., 2025; Mahato et al., 2024).

The homomorphic encryption layer executes encrypted computations using cryptosystems such as the Paillier or BFV schemes. These systems allow arithmetic operations on ciphertexts without requiring decryption, ensuring that data remains confidential during processing (Akindote et al., 2024; Gentry, 2009).

Communication Protocols and Smart Contracts Communication between layers is managed through standardized APIs and secure messaging protocols. Smart contracts are embedded in the blockchain layer to automate access control, audit logging, and compliance enforcement (Lopez et al., 2024; Din et al., 2025). These contracts define processing rules and ensure that operations on encrypted data are transparent and accountable.

Security and Privacy Measures

To enhance privacy, zero-knowledge proofs (ZKPs) and secure multiparty computation (SMPC) are optionally incorporated to verify operations without revealing data (Mahato et al., 2024). Additionally, the immutable nature of blockchain helps track all access and modification attempts, strengthening auditability (Punia et al., 2024).

Regulatory compliance is considered through system design that aligns with mandates such as GDPR and HIPAA, ensuring that personal data is never exposed during computation and is traceable for auditing purposes (Ahirao et al., 2024; Gandhi et al., 2025).

Empirical Evaluation Approach

Performance validation is informed by simulation results from Zhang et al. (2025), who evaluated latency, throughput, and encryption overhead in a hybrid Ethereum–Paillier system. Metrics considered include:

- Computation Time: Time required for encrypted operations.
- Transaction Latency: Blockchain write/read delay.
- Data Integrity Verification: Using blockchain hash consistency.
- Privacy Metrics: Degree of information exposure (should be zero).

Tools and Platforms

For architectural simulation, platforms such as Hyperledger Fabric, Ethereum, and open-source HE libraries like Microsoft SEAL and PALISADE are recommended (Xie et al., 2024; Mahato et al., 2024). These tools support both homomorphic encryption schemes and blockchain consensus protocols necessary for emulating real-world deployment scenarios.

IV. IMPLEMENTATION

The implementation of a privacy-preserving cloud architecture that integrates blockchain technology with homomorphic encryption (HE) requires a careful orchestration of cryptographic operations, distributed ledger protocols, and secure communication frameworks. This section outlines the layered implementation model, tools, protocols, and case-specific examples referenced in existing literature.

Layered System Architecture

The proposed system architecture is implemented in three primary layers:

- Application Layer: Provides the user interface for uploading data, initiating encrypted queries, and visualizing results. It is designed for simplicity and user-friendliness while abstracting the underlying cryptographic and ledger operations (Mahato et al., 2024).
- Blockchain Layer: Uses a decentralized ledger such as Ethereum or Hyperledger Fabric to store encrypted hashes, transaction logs, and execute smart contracts. It ensures data immutability, access traceability, and verifiability (Zhang et al., 2025; Punia et al., 2024).
- Homomorphic Encryption Layer: Applies cryptographic schemes like Paillier, BFV, or CKKS to perform operations on encrypted data. This layer processes analytical tasks without decryption, preserving end-to-end data confidentiality (Akindote et al., 2024; Brakerski et al., 2016).

Smart Contract Deployment

Smart contracts are developed and deployed on the blockchain to automate access control, auditing, and data-sharing rules. For example, a contract may encode policies that allow only specific users or institutions to query encrypted health records, with all access attempts logged on-chain (Lopez et al., 2024). These contracts also govern encrypted computations, ensuring compliance with predefined conditions.

Data Flow and Encryption Workflow

- Data Upload: Users encrypt their data locally using a chosen homomorphic scheme.
- Blockchain Logging: Encrypted data or its hash is logged on the blockchain, ensuring integrity and non-repudiation.
- Computation Request: Authorized users initiate encrypted queries through the application interface.
- Encrypted Computation: The HE layer processes the query on ciphertexts and returns encrypted results.
- Decryption and Result Retrieval: The data owner or authorized user decrypts the result locally.
- This workflow ensures that at no point is plaintext data exposed to cloud servers or third-party processors (Mahato et al., 2024).

Performance Benchmarking

Empirical benchmarks from Zhang et al. (2025) demonstrate that a hybrid Ethereum–Paillier system maintained processing latency in the range of milliseconds, even under real-world healthcare simulation conditions. Performance evaluations considered computation cost, blockchain consensus delays, and bandwidth utilization. Smart contract execution contributed minimal overhead due to optimized gas usage and batching of transactions.

Use Case Demonstrations

Several domain-specific implementations validate this architecture:

- Healthcare: Encrypted patient data analytics were securely executed without revealing identity, enabling privacy-preserving AI models (Gandhi et al., 2025; Lopez et al., 2024).
- Supply Chain: Blockchain-logged logistics events were correlated with encrypted demand and inventory forecasts, improving security and transparency (Din et al., 2025).
- IoT and Smart Cities: Real-time encrypted sensor data was aggregated and processed using HE, while blockchain ensured secure data provenance (Shankar et al., 2024).

Tools and Libraries

The system was implemented using:

- Ethereum/Hyperledger for blockchain operations and smart contracts.
- Microsoft SEAL, HElib, or PALISADE for HE functions.
- Node.js and Python for interfacing and middleware development.
- Zero-Knowledge Proofs (ZKPs) and Secure Multi-Party Computation (SMPC) as privacy-enhancing add-ons in high-sensitivity applications (Mahato et al., 2024; Asaad & Zeebaree, 2024).

V. RESULTS AND ANALYSIS

The integration of blockchain and homomorphic encryption (HE) was evaluated through simulated environments and empirical studies reported in recent literature. The analysis focuses on core performance metrics such as latency, computation time, data privacy preservation, and scalability. This section summarizes the key findings, drawn from implementations across healthcare, supply chain, and IoT systems.

Performance Evaluation

The system proposed by Zhang et al. (2025), which integrates Ethereum with Paillier encryption, was used as a benchmark model. Their experiments simulated real-time analytics over encrypted healthcare data.

Table 1. Performance Metrics in Hybrid Blockchain-HE System
(Adapted from Zhang et al., 2025)

Metric	Value (Approx.)	Observations
Computation Time	200–350 ms	Dependent on ciphertext size and query complexity
Smart Contract Execution	< 50 ms	Optimized via gas-efficient design
Blockchain Write Latency	120–180 ms	Affected by Ethereum's consensus and network load
Data Integrity Verification	Real-time	Verified using SHA-256 hash and on-chain logs
Information Exposure	0%	Fully encrypted pipeline ensured zero plaintext leak

5.2 Use Case Validation

Table 2. Domain-Specific Applications and Outcomes

Application Area	Blockchain Role	HE Role	Outcome
Healthcare (Gandhi et al., 2025)	Logging access and enforcing patient consent	Privacy-preserving diagnostics and AI training	GDPR-compliant and accurate medical analytics
Supply Chain (Din et al., 2025)	Provenance tracking and anti-counterfeiting	Encrypted forecasting	Reduced fraud, increased traceability
Smart Cities (Shankar et al., 2024)	Decentralized sensor data audit	Secure encrypted aggregation	Real-time analysis without data leakage
Federated Learning (Mahato et al., 2024)	Model sharing and validation via smart contracts	Encrypted model updates	Verified, privacy-preserving collaborative AI

5.3 Privacy and Compliance Assessment

The combined framework was found to satisfy major international data protection norms including GDPR, HIPAA, and CCPA.

Table 3. Compliance Mapping

Regulatory Requirement	Blockchain Contribution	HE Contribution	Compliance Status
Data Minimization	Immutable log prevents over-collection	Data remains encrypted end-to-end	Fully Compliant
User Consent & Access	Smart contracts enforce policies	No plaintext exposure to cloud	Fully Compliant
Right to be Forgotten	Soft deletion via contract reference cuts	Encrypted pointers, not raw data	Conditional (per GDPR)
Data Auditability	On-chain logs and hash verification	Cryptographic proofs of correctness	Fully Compliant

Scalability and Optimization Analysis

As highlighted by Xie et al. (2024), system scalability can be improved through:

- Batching encrypted queries
- Parallelizing homomorphic operations
- Using lightweight HE schemes like BFV over FHE for practical applications

Mahato et al. (2024) report up to 70% reduction in computation time through distributed task execution and parameter tuning. However, the integration of blockchain consensus protocols like Proof of Work (PoW) may introduce variable delays, suggesting the use of Proof of Authority (PoA) for enterprise deployments.

VI. DISCUSSIONS

The integration of homomorphic encryption (HE) and blockchain technology offers a paradigm shift in how data privacy, security, and trust can be maintained in cloud environments. This study has demonstrated, through reviewed implementations and empirical findings, that the synergy of these technologies addresses critical limitations of traditional data protection models.

Dual Security Assurance: Confidentiality and Integrity

One of the most significant outcomes of the integrated architecture is its ability to deliver simultaneous confidentiality and data integrity. Homomorphic encryption ensures that data remains encrypted during processing, removing the need for decryption at any point in the cloud lifecycle (Akindote et al., 2024; Mahato et al., 2024). This eliminates a major vulnerability found in conventional encryption schemes where data is exposed during computation.

In parallel, blockchain provides immutable, decentralized storage and verifiable access trails through smart contracts, thereby ensuring that unauthorized modifications are prevented and data lineage is always traceable (Punia et al., 2024; Lopez et al., 2024). The two technologies complement each other, with HE safeguarding computation and blockchain ensuring auditability and trust.

Empirical Efficiency and Domain Viability

The results reviewed from Zhang et al. (2025) and Mahato et al. (2024) confirm that hybrid models—particularly those combining Ethereum with the Paillier or BFV schemes—achieve practical levels of efficiency. Despite concerns regarding HE's computational overhead, performance metrics such as sub-second latency and smart contract execution under 50 ms indicate feasibility for real-time applications.

Real-world applications further validate this approach. In healthcare, Gandhi et al. (2025) report accurate encrypted diagnostics, while Din et al. (2025) highlight improvements in supply chain transparency and fraud detection. Shankar et al. (2024) show that smart city environments benefit from real-time encrypted analytics supported by distributed consensus.

Regulatory Readiness and Challenges

From a regulatory standpoint, the proposed system aligns with major data privacy frameworks such as GDPR, HIPAA, and CCPA. Smart contracts can enforce user consent policies, while encrypted data ensures compliance with minimization principles (Ahirao et al., 2024; Lopez et al., 2024). However, challenges remain regarding the "right to be forgotten" under GDPR. As blockchain data is immutable, implementing deletion requires architectural workarounds such as off-chain referencing and contract revocation (Sasikumar & Nagarajan, 2024).

Additionally, while blockchain enables transparency, it may conflict with strict data sovereignty laws unless private or consortium-led blockchains (e.g., Hyperledger Fabric) are employed.

Scalability and Optimization Needs

Despite promising results, scalability remains a technical bottleneck. Xie et al. (2024) emphasize the need to improve HE performance through parallel processing and parameter tuning. Moreover, blockchain consensus mechanisms such as Proof of Work introduce delays and energy inefficiencies, making Proof of Authority (PoA) or Byzantine Fault

Tolerance (BFT) preferable for institutional use (Mahato et al., 2024).

Furthermore, interoperability between HE libraries and blockchain frameworks is still in early stages. Asaad and Zeebaree (2024) note the absence of standard APIs and protocols as a barrier to widespread adoption.

Toward Intelligent Privacy Systems

Emerging research points to the integration of AI with HE and blockchain for adaptive privacy enforcement. Tamboli and Arage (2024) suggest that AI-driven monitoring systems could detect anomalies in encrypted workflows, while Mahato et al. (2024) envision federated learning models enhanced through blockchain-backed verification.
Such integrations may be pivotal in advancing next-generation, intelligent cloud platforms capable of context-aware, policy-driven privacy management.

VII. CONCLUSION

The increasing reliance on cloud computing for storage and computation has amplified the demand for robust, scalable, and privacy-preserving data security frameworks. This study analyzed the integration of homomorphic encryption (HE) and blockchain technology as a holistic solution for managing data privacy and integrity in untrusted cloud environments.

The findings reviewed in this work underscore the effectiveness of combining HE's ability to enable encrypted computation with blockchain's decentralized and tamper-proof architecture. Together, these technologies provide a dual-layered security paradigm—ensuring end-to-end confidentiality and immutable traceability. Empirical evidence from Zhang et al. (2025), Gandhi et al. (2025), and Mahato et al. (2024) confirms the feasibility of such systems across diverse applications, including healthcare, supply chains, and smart cities.

Moreover, the architecture aligns well with global data protection regulations like GDPR, HIPAA, and CCPA, particularly in areas concerning consent management, data minimization, and auditability (Ahirao et al., 2024; Punia et al., 2024). While certain challenges such as the "right to erasure" in immutable systems persist, proposed mitigations like off-chain data referencing offer promising directions (Sasikumar & Nagarajan, 2024).

However, the study also highlights ongoing challenges in scalability, computational overhead, and lack of standardization. As emphasized by Xie et al. (2024) and Asaad and Zeebaree (2024), performance optimization and protocol interoperability are critical areas for future research. The convergence of blockchain and HE with AI and federated learning models (Mahato et al., 2024; Tamboli & Arage, 2024) also presents an exciting opportunity to build intelligent, self-regulating privacy infrastructures.

In conclusion, the synergy of blockchain and homomorphic encryption offers a viable and forward-looking framework for enhancing cloud data security. With continued optimization and interdisciplinary integration, this approach is poised to redefine trust, transparency, and confidentiality in the digital era.

REFERENCES

1. Akindote, O., Enyejo, J. O., Awotiwon, B. O., & Ajayi, A. A. (2024). Integrating blockchain and homomorphic encryption to enhance security and privacy in project management and combat counterfeit goods in global supply chain operations. International Journal of Innovative Science and Research Technology, 9(11).
2. Ahirao, P., Shaikh, B., & Wahedna, R. Z. (2024, October). Blockchain technology and data privacy: A comprehensive review and future perspective. In 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) (pp. 1–7). IEEE.
3. Asaad, R. R., & Zeebaree, S. R. (2024). Enhancing security and privacy in distributed cloud environments: A review of protocols and mechanisms. Academic Journal of Nawroz University, 13(1), 476–488.

4. Chandra, A. (2024). Privacy-preserving data sharing in cloud computing environments. Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal, 13(1), 104–111.
5. Din, I. U., Almogren, A., Han, Z., & Guizani, M. (2025). Ensuring privacy and integrity in IoT supply chains through blockchain and homomorphic encryption. IEEE Internet of Things Journal.
6. Dhinakaran, D., Sankar, S. M., Selvaraj, D., & Raja, S. E. (2024). Privacy-preserving data in IoT-based cloud systems: A comprehensive survey with AI integration. arXiv preprint arXiv:2401.00794.
7. Gandhi, B. M., Vaghadia, S. B., Kumhar, M., Gupta, R., Jadav, N. K., Bhatia, J., ... & Alabdulatif, A. (2025). Homomorphic encryption and collaborative machine learning for secure healthcare analytics. Security and Privacy, 8(1), e460.
8. Kambala, G. (2025). Data privacy in cloud computing: A comparative study of privacy preserving techniques. International Journal of Scientific Research and Management (IJSRM), 12(6).
9. Kumar, S., Singh, S. K., Gupta, B. B., Psannis, K., & Wu, J. (2024). Homomorphic encryption in smart city applications for balancing privacy and utility. In Innovations in Modern Cryptography (pp. 241–269). IGI Global. https://www.igi-global.com/chapter/homomorphic-encryption-in-smart-city-applications-for-balancing-privacy-and-utility/354042
10. Lopez, L. J. R., Millan Mayorga, D., Martinez Poveda, L. H., Amaya, A. F. C., & Rojas Reales, W. (2024). Hybrid architectures used in the protection of large healthcare records based on cloud and blockchain integration: A review. Computers, 13(6), 152.
11. Mahato, G. K., Banerjee, A., Chakraborty, S. K., & Gao, X. Z. (2024). Privacy-preserving verifiable federated learning scheme using blockchain and homomorphic encryption. Applied Soft Computing, 167, 112405.
12. Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024). A systematic review on blockchain-based access control systems in cloud environment. Journal of Cloud Computing, 13(1), 146.
13. Ranjan, A. K., & Kumar, P. (2025). A survey on blockchain-based privacy preserving techniques for edge internet of things. International Journal of Computers and Applications, 1–12.
14. Sasikumar, K., & Nagarajan, S. (2024). Comprehensive review and analysis of cryptography techniques in cloud computing. IEEE Access.
15. Shankar, G., Uddin, M. R., Mukta, S., Kumar, P., Islam, S., & Islam, A. K. M. (2024). Blockchain-based information security and privacy protection: Challenges and future directions using computational literature review. arXiv preprint arXiv:2409.14472.
16. Tamboli, S. I., & Arage, C. S. (2024). AI and blockchain integration for preserving privacy in cloud databases. Journal of Technical Education, 1.
17. Vaghela, J. (2024). Security analysis and implementation in distributed databases: A review.
18. Xie, Q., Jiang, S., Jiang, L., Huang, Y., Zhao, Z., Khan, S., ... & Wu, K. (2024). Efficiency optimization techniques in privacy-preserving federated learning with homomorphic encryption: A brief survey. IEEE Internet of Things Journal, 11(14), 24569–24580.
19. Zhang, S., Zhang, W., Liang, W., Li, K., & Dobre, C. (2025). Blockchain-based secure and verifiable storage scheme for IPFS-assisted IoT with homomorphic encryption. Computing, 107(7), 1–33.
20. Ahmed, A. A., & Alabi, O. (2024). Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review. IEEE Access.