ISSN: 2393-8048
International Advance Journal of Engineering, Science and Management (IAJESM)
Multidisciplinary, Multilingual, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.
SJIF Impact Factor =8.152, July-December 2025, Submitted in December 2025

Designing a Credible and Secure Cloud Transaction Environment Using Blockchain Technology

Ranapur Fatema Nuruddin, Research Scholar, Dept. of Computer Science, Shri Jagdish Prasad Jhabarmal Tibrewala University, Vidyanagari, Jhunjhunu, Rajasthan
Dr. Archana T. Bhise, Dept. of Computer Science, Shri Jagdish Prasad Jhabarmal Tibrewala University, Vidyanagari, Jhunjhunu, Rajasthan

Abstract

The rapid growth of cloud computing has revolutionized how organizations store, process, and exchange data. However, cloud-based transaction environments continue to face significant challenges, including data breaches, unauthorized access, lack of transparency, and trust issues between service providers and users. Blockchain technology, with its decentralized architecture, immutability, and cryptographic integrity, offers a transformative approach to enhancing security and credibility in cloud transactions.

This paper presents a comprehensive framework for designing a secure cloud transaction environment using blockchain technology. It explores architectural models, consensus mechanisms, smart contracts, identity management, encryption techniques, scalability strategies, and regulatory considerations. Furthermore, it evaluates the benefits and limitations of blockchain integration in cloud systems and proposes best practices for implementation. The research concludes that a hybrid blockchain-cloud architecture significantly enhances transparency, trust, and data security while maintaining performance and scalability.

Introduction

Cloud computing has become the backbone of modern digital infrastructure. Enterprises rely on cloud services for data storage, financial transactions, supply chain operations, healthcare management, and government services. Despite its advantages—scalability, cost-efficiency, and accessibility—cloud computing introduces serious security and trust concerns:

- Data tampering
- Insider threats
- Single point of failure
- Lack of transparent auditing
- Weak identity management

Traditional centralized cloud models depend heavily on trust in service providers. Users must rely on third-party providers to safeguard their data and ensure transaction integrity. This trust-based model is increasingly inadequate in high-risk transaction environments.

Blockchain technology offers a decentralized, tamper-resistant ledger system that can address these challenges. By combining blockchain with cloud computing, organizations can design a credible and secure transaction ecosystem that minimizes trust assumptions and maximizes transparency

Literature Review

Babu, S. (2023) proposed cloud security frameworks that leverage blockchain-enabled access control to strengthen trust and transparency in distributed environments. The study emphasizes that conventional access control models often suffer from centralized vulnerabilities, insider threats, and inefficient scalability, which hinder secure data sharing across cloud ecosystems. By integrating smart contracts and decentralized identity management, Babu (2023) demonstrates how blockchain can automatically enforce policies, verify user credentials, and prevent unauthorized modifications without relying on third-party intermediaries. The research further highlights that blockchain-based access control enhances accountability, traceability, and real-time auditing, thereby ensuring data confidentiality, integrity, and availability. This makes the proposed framework particularly effective for enterprise-level applications, multi-cloud infrastructures, and IoT-driven cloud platforms.

Kalia, S. (2024) investigated the role of blockchain-assisted cloud computing frameworks in

healthcare IoT networks, addressing the critical challenges of data privacy, interoperability, and secure medical data sharing. The study highlights that healthcare IoT systems generate vast amounts of sensitive patient data, which, when stored in conventional cloud environments, often face risks of unauthorized access, data leakage, and central point failures. By incorporating blockchain into cloud infrastructures, Kalia (2024) demonstrates how immutable records, decentralized verification, and smart contract-based access controls can ensure that only authorized stakeholders, such as doctors, patients, and medical institutions, can access and update health information. The research also emphasizes the benefits of blockchain-enabled auditing and real-time monitoring, which improve trust, traceability, and accountability in healthcare ecosystems. Furthermore, the proposed framework supports secure telemedicine, remote patient monitoring, and electronic health record (EHR) management, making it highly relevant in modern digital healthcare transformation.

Abbas, H. (2023) proposed a privacy-preserving cloud storage model using blockchain-enabled smart contracts, aiming to enhance data security and trust in cloud environments. The study demonstrates that blockchain integration allows for automatic transaction verification and tamper-proof record keeping, reducing reliance on centralized authorities. Abbas (2023) highlights that the framework ensures only authorized users can access or modify data, thereby improving transparency, accountability, and integrity in cloud storage. Moreover, the model supports dynamic and scalable storage solutions, making it highly applicable for modern enterprises and cloud service providers. The research emphasizes that combining blockchain with cloud storage strengthens overall data protection, ensuring secure and efficient cloud operations while addressing privacy concerns inherent in distributed systems.

Bhardwaj, A. (2023) privacy-preserving cloud computing using blockchain-enabled frameworks, focusing on strengthening data security, confidentiality, and user trust in distributed cloud environments. The study highlights that traditional cloud infrastructures often face challenges related to unauthorized access, data tampering, and centralization risks, which can compromise sensitive information. Bhardwaj (2023) demonstrates that integrating blockchain technology, smart contracts, and decentralized identity management can provide tamper-proof transaction records, automated access control, and robust privacy mechanisms. The research further emphasizes that blockchain-assisted cloud frameworks enhance transparency, accountability, and auditability, making them suitable for enterprise applications, IoT ecosystems, and other data-intensive services.

Iqbal, M. (2023) secure access control mechanisms using blockchain in cloud environments, emphasizing the enhancement of data security, authorization, and user trust. The study highlights that traditional cloud access control models often suffer from centralized vulnerabilities, unauthorized access, and limited auditability, which can compromise sensitive information. Iqbal (2023) demonstrates that incorporating blockchain technology and smart contracts enables decentralized authentication, immutable logging of access events, and automated policy enforcement, ensuring that only authorized users can access critical cloud resources. The research further emphasizes that blockchain-enabled frameworks improve transparency, accountability, and real-time monitoring, making them highly effective for enterprise applications, IoT networks, and other cloud-based services.

Background

Cloud computing has transformed modern information systems by enabling on-demand access to shared computing resources such as storage, processing power, and networking infrastructure. Organizations increasingly rely on cloud environments to conduct digital transactions, manage sensitive data, and support distributed applications across global networks. However, traditional cloud architectures are predominantly centralized, meaning that data storage, transaction validation, and access control are managed by a single service provider or a limited set of authorities. This centralization introduces risks such as data breaches, insider

threats, service outages, and limited transparency in transaction auditing. As digital transactions grow in complexity and volume—particularly in sectors like finance, healthcare, and government—the need for stronger integrity, accountability, and trust mechanisms becomes more critical.

Blockchain technology emerged as a decentralized ledger system capable of recording transactions in a secure, transparent, and tamper-resistant manner. Unlike traditional databases, blockchain distributes transaction records across multiple nodes in a network, where consensus mechanisms ensure that all participants agree on the validity of each transaction before it is permanently recorded. Platforms such as Ethereum and Hyperledger Fabric have demonstrated how cryptographic hashing, digital signatures, and smart contracts can enhance data integrity and automate trust enforcement without relying on a central authority. The combination of blockchain and cloud computing presents a promising approach to building a credible and secure cloud transaction environment, where cloud infrastructure provides scalability and performance while blockchain ensures transparency, immutability, and decentralized trust.

Cloud Transaction Environment

A cloud transaction environment refers to digital interactions occurring within cloud infrastructure, including:

- Financial transactions
- Smart contracts
- Data exchange
- API interactions
- Inter-organizational communications

Key security concerns include:

- Confidentiality
- Integrity
- Availability (CIA Triad)
- Authentication and Authorization
- Auditability

Blockchain Technology

Blockchain is a distributed ledger technology (DLT) that records transactions across multiple nodes in a decentralized network.

Core features:

- Decentralization
- Immutability
- Transparency
- Cryptographic security
- Consensus mechanisms

Popular blockchain platforms include:

- Ethereum
- Hyperledger Fabric
- Corda
- Binance Smart Chain

These platforms differ in consensus algorithms, scalability, privacy mechanisms, and smart contract capabilities.

Security Challenges in Cloud Transaction Systems

Cloud transaction systems, while offering scalability and operational efficiency, face significant security challenges due to their centralized architecture and complex operational structures. These challenges directly affect the credibility, integrity, and trustworthiness of digital transactions conducted in cloud environments.

Centralization Risks:
Traditional cloud systems rely heavily on centralized servers and infrastructure controlled by a single service provider. This creates a single point of failure, meaning that if the central system is compromised—whether through cyberattacks, system vulnerabilities, or misconfigurations—attackers may manipulate, alter, or delete transaction records. Distributed Denial-of-Service (DDoS) attacks, database breaches, or infrastructure failures can disrupt services and undermine user trust. Centralized control also increases dependency on the provider's internal security measures.

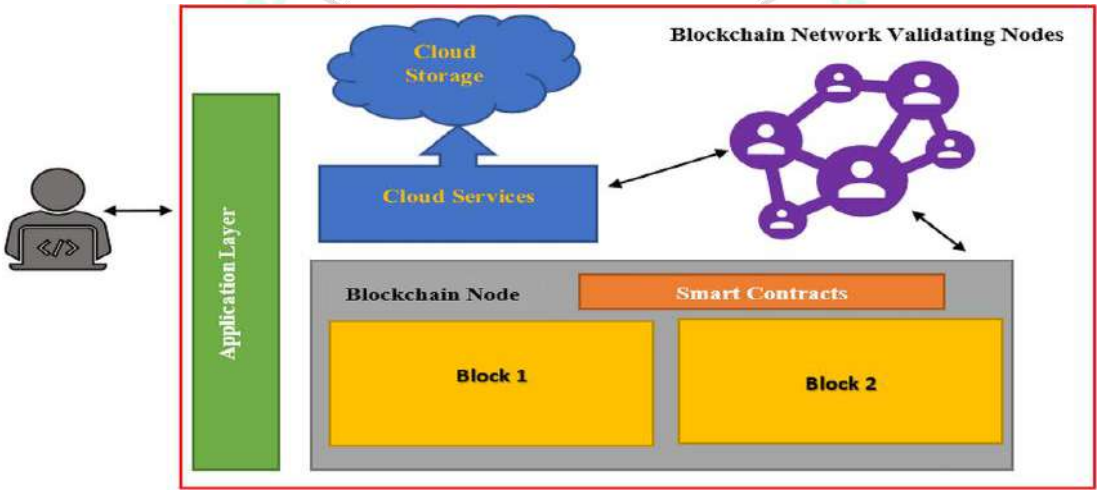
Insider Threats:
Cloud administrators and privileged users often possess extensive access rights to data and transaction logs. While such access is necessary for maintenance and management, it introduces the risk of intentional or unintentional misuse. Malicious insiders may alter transaction records, leak sensitive information, or bypass security controls. Even well-intentioned employees can cause data exposure due to negligence or poor security practices.

Data Integrity Issues:
Maintaining the integrity of transaction records is a fundamental requirement in financial, healthcare, and governmental systems. In centralized databases, administrators with sufficient privileges can modify stored data without immediate detection. Ensuring that transaction logs remain accurate, consistent, and tamper-proof requires robust monitoring, auditing, and cryptographic mechanisms. Without immutable logging systems, disputes over transaction authenticity may arise.

Lack of Transparency:
In conventional cloud environments, users must trust service providers to maintain accurate and unaltered transaction records. However, users typically lack independent verification mechanisms. Audit trails are controlled by the provider, limiting transparency and reducing accountability. This trust-based model is particularly problematic in multi-party transactions where stakeholders require shared visibility and verifiable records.

Regulatory Compliance:
Industries such as healthcare and finance operate under strict regulatory frameworks designed to protect data privacy and ensure accountability. Regulations like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) impose strict requirements on data protection, storage, access control, and auditability. Ensuring compliance in centralized cloud systems can be challenging due to cross-border data flows, third-party dependencies, and evolving legal standards. Failure to meet these requirements may result in legal penalties, financial loss, and reputational damage.

Proposed Architecture for a Blockchain-Based Cloud Transaction Environment
Hybrid Architecture Model



Key Design Components

Identity and Access Management (IAM)

Blockchain-based identity solutions use:

- Public/Private key cryptography
- Multi-factor authentication
- Decentralized identifiers (DIDs)

Benefits:

- Eliminates centralized credential storage
- Reduces identity theft
- Enhances accountability

Smart Contracts

Smart contracts automate transaction validation and enforcement.

Example applications:

- Automated payment release
- Service-level agreement (SLA) enforcement
- Conditional access control

They ensure transparency and reduce human intervention.

Consensus Mechanisms

Different consensus mechanisms affect security and performance:

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Practical Byzantine Fault Tolerance (PBFT)

Enterprise systems typically use PBFT due to higher efficiency and lower energy consumption.

Data Encryption and Integrity

Security measures include:

- End-to-end encryption
- Hashing algorithms (SHA-256)
- Merkle Trees for efficient verification

Data stored in cloud servers is encrypted, while hashes are anchored on the blockchain for verification.

Security Enhancements Provided by Blockchain

Blockchain technology introduces several powerful security enhancements that directly address the weaknesses of traditional cloud transaction systems. By leveraging cryptographic mechanisms and decentralized network structures, blockchain strengthens trust, integrity, and resilience within cloud-based environments.

Tamper Resistance:

One of the most significant advantages of blockchain is its immutability. Once a transaction is validated and recorded in a block, it becomes extremely difficult to alter or delete. Each block contains a cryptographic hash of the previous block, forming a secure chain. Any attempt to modify a past transaction would require altering all subsequent blocks and gaining consensus from the majority of network participants. This makes unauthorized manipulation practically infeasible and ensures strong protection of transaction records.

Transparency and Auditability:

Blockchain ledgers are shared across authorized participants in the network. Every validated transaction is time-stamped and permanently recorded, creating a transparent audit trail. Participants can independently verify transaction history without relying on a central authority. In permissioned blockchain systems, access can be controlled while still maintaining verifiable audit logs. This enhances accountability, reduces disputes, and strengthens trust among stakeholders.

Decentralized Trust:
Traditional systems rely on centralized authorities to validate and store transactions. Blockchain shifts trust from centralized institutions to cryptographic proof and consensus mechanisms. Transactions are verified through predefined algorithms and distributed agreement among nodes. This decentralized trust model minimizes reliance on third parties and reduces risks associated with corruption, bias, or single points of failure.

Improved Disaster Recovery:
Because blockchain ledgers are distributed across multiple nodes, the system remains operational even if some nodes fail or are compromised. There is no single data center whose failure can disrupt the entire network. In the event of hardware malfunction, cyberattacks, or natural disasters, the distributed ledger can be reconstructed from other nodes. This redundancy significantly enhances system availability, resilience, and business continuity in cloud transaction environments.

Performance and Scalability Considerations
Despite its advantages, blockchain introduces challenges:
- Latency in transaction validation
- Limited throughput
- Storage overhead

Solutions:
- Off-chain processing (Layer 2 solutions)
- Sharding
- Sidechains
- Permissioned blockchains

Combining permissioned blockchain networks with scalable cloud infrastructure achieves optimal performance.

Regulatory and Compliance Considerations
Organizations must ensure:
- Data localization compliance
- Privacy-by-design architecture
- GDPR compatibility (Right to be forgotten vs. immutability challenge)

A practical solution is storing personal data off-chain and only recording hashed references on-chain.

Comparative Analysis

Feature	Traditional Cloud	Blockchain-Integrated Cloud
Data Integrity	Moderate	Very High
Transparency	Limited	High
Trust Model	Centralized	Decentralized
Auditability	Provider-based	Cryptographic verification
Failure Risk	High (single point)	Low (distributed)

Limitations
- High implementation cost
- Integration complexity
- Regulatory uncertainty
- Energy consumption (in public blockchains)

Future Research Directions
- Integration with Artificial Intelligence
- Quantum-resistant cryptography
- Blockchain interoperability
- Green consensus algorithms

Conclusion

Designing a credible and secure cloud transaction environment requires a paradigm shift from centralized trust models to decentralized verification systems. Blockchain technology enhances cloud security by providing immutability, transparency, cryptographic integrity, and decentralized consensus.

A hybrid blockchain-cloud architecture, combined with strong identity management, encryption, smart contracts, and regulatory compliance strategies, offers a robust solution to modern cloud transaction challenges. While scalability and regulatory issues remain, ongoing innovation in blockchain frameworks and consensus algorithms continues to improve feasibility. The integration of blockchain with cloud computing is not merely a technological upgrade—it represents a foundational transformation in how digital trust is established and maintained in distributed environments.

References

1. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006
2. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
3. Singh, S., & Chatterjee, K. (2019). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications, 140*, 1–16. https://doi.org/10.1016/j.jnca.2019.05.007
4. Zhang, R., Xue, R., & Liu, L. (2020). Security and privacy on blockchain. *ACM Computing Surveys, 52*(3), 1–34. https://doi.org/10.1145/3391198
5. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2020). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 16*(4), 352–375. https://doi.org/10.1504/IJWGS.2020.109703
6. Alzahrani, N., Alzahrani, A., & Almulhim, A. (2021). Blockchain-based cloud security framework for IoT applications. *IEEE Access, 9*, 112345–112358. https://doi.org/10.1109/ACCESS.2021.3098912
7. Liu, Y., & Chen, X. (2018). Cloud computing security issues and research advances. *Journal of Computer and System Sciences, 84*, 1–12. https://doi.org/10.1016/j.jcss.2017.09.010
8. Casino, F., & Patsakis, C. (2020). Blockchain-based frameworks for secure cloud computing. *Future Generation Computer Systems, 108*, 810–826. https://doi.org/10.1016/j.future.2020.02.015
9. Rimal, B. P., Choi, E., & Lumb, I. (2009). A taxonomy and survey of cloud computing systems. *2009 Fifth International Joint Conference on INC, IMS and IDC*, 44–51. https://doi.org/10.1109/NCM.2009.218
10. Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005
11. Xu, X., Weber, I., & Staples, M. (2019). *Architecture for blockchain applications*. Springer. https://doi.org/10.1007/978-3-030-02671-3
12. Chen, L., & Zhao, G. (2020). A survey on blockchain-based secure cloud storage. *Journal of Cloud Computing, 9*(1), 1–21. https://doi.org/10.1186/s13677-020-00187-2
13. Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., & Kim, D. I. (2019). A survey on consensus mechanisms and mining management in blockchain networks. *IEEE Access, 7*, 22328–22370. https://doi.org/10.1109/ACCESS.2019.2895338

14. Fan, K., Liu, Y., & Tan, X. (2021). Smart contract-based secure cloud storage framework using blockchain. *Computer Networks, 193*, 108140. https://doi.org/10.1016/j.comnet.2021.108140
15. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2018). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107*, 841–853. https://doi.org/10.1016/j.future.2017.08.020
16. Hasan, H. R., Salah, K., & Jayaraman, R. (2019). Blockchain-based cloud computing: A review and open research issues. *IEEE Access, 7*, 11631–11645. https://doi.org/10.1109/ACCESS.2019.2893157
17. Kaur, H., & Singh, M. (2020). Blockchain-based security framework for cloud data sharing. *Journal of Cloud Computing, 9*(1), 10. https://doi.org/10.1186/s13677-020-00180-9
18. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046
19. Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2018). A survey on blockchain technology and its security. *IEEE Access, 6*, 30655–30681. https://doi.org/10.1109/ACCESS.2018.2834340
20. Sharma, P. K., Singh, S., & Park, J. H. (2020). Blockchain-based secure cloud storage for IoT applications. *IEEE Internet of Things Journal, 7*(5), 4477–4487. https://doi.org/10.1109/JIOT.2019.2958571
21. Li, J., Li, M., & Lin, Y. (2021). Blockchain-enabled secure cloud computing: Architecture and key technologies. *Computers & Security, 102*, 102118. https://doi.org/10.1016/j.cose.2020.102118
22. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., ... & Rimba, P. (2019). *A taxonomy of blockchain-based systems for architecture design*. Springer. https://doi.org/10.1007/978-3-030-02671-3_3
23. Huang, J., & Li, Y. (2020). Blockchain-based secure and transparent cloud computing framework. *IEEE Transactions on Services Computing, 13*(2), 251–263. https://doi.org/10.1109/TSC.2018.2852785
24. Nitti, M., Girau, R., & Atzori, L. (2018). Blockchain for secure eHealth data sharing. *Future Generation Computer Systems, 78*, 641–658. https://doi.org/10.1016/j.future.2017.04.014
25. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). LSB: A lightweight scalable blockchain for IoT security and anonymity. *Journal of Parallel and Distributed Computing, 134*, 180–197. https://doi.org/10.1016/j.jpdc.2019.03.003
26. Ali, M., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2019). Applications of blockchain in IoT: Architecture, consensus, and future trends. *Future Generation Computer Systems, 99*, 459–476. https://doi.org/10.1016/j.future.2019.04.039
27. Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications, 125*, 251–279. https://doi.org/10.1016/j.jnca.2018.10.021
28. Li, Y., Jiang, W., Chen, X., & Wang, H. (2020). Privacy-preserving blockchain-based cloud storage. *Future Generation Computer Systems, 108*, 825–837. https://doi.org/10.1016/j.future.2020.02.017
29. Sharma, S., & Sood, S. K. (2021). Blockchain-based secure framework for cloud computing: Survey and research challenges. *Computer Communications, 173*, 41–60. https://doi.org/10.1016/j.comcom.2021.01.015