www.ijarp.com ISSN 2456-9992 Page: 01-07
International Journal Advanced Research Publications
Review Article
Volume: 02
Issue: 01

# A BLOCKCHAIN DRIVEN SECURE DATA SHARING FRAMEWORK FOR CLOUD ENVIRONMENTS

***[1]Pankaj Kumar and [2]Dr. Jeetendra Singh Yadav**

[1]M.Tech Scholar , [2]Associate Professor

Department of Computer Science and Engineering, Bhabha University, Bhopal, India.

**Article Received: 17 December 2025, Article Revised: 06 January 2026, Published on: 26 January 2026**

**Corresponding Author: Pankaj Kumar**

M.Tech Scholar, Department of Computer Science and Engineering, Bhabha University, Bhopal, India.

DOI: https://doi-doi.org/101555/ijarp.2771

## ABSTRACT

Cloud computing has become a fundamental platform for data storage, processing, and information exchange across distributed environments. Despite its advantages, secure data sharing in cloud environments remains a critical challenge due to centralized control, lack of transparency, vulnerability to insider attacks, and limited user trust. Traditional cloud security mechanisms rely heavily on trusted third-party cloud service providers, which introduces single points of failure and weak accountability. To address these challenges, this paper proposes a Blockchain-Driven Secure Data Sharing Framework (BSDSF) for cloud environments. The proposed framework integrates blockchain technology with cloud infrastructure to enable decentralized, transparent, and tamper-resistant data sharing. A hybrid on-chain/off-chain architecture is adopted, where encrypted data is stored off-chain in cloud or distributed storage, while security-critical metadata, access policies, cryptographic hashes, and audit logs are maintained on the blockchain. Smart contracts are employed to automate identity management, access control enforcement, key distribution, and auditing without human intervention. To ensure reliability and fault tolerance, a Byzantine Fault Tolerant (BFT)-based consensus mechanism is utilized for transaction validation. The proposed framework enhances data confidentiality, integrity, transparency, and accountability while maintaining scalability through off-chain storage. This work demonstrates that blockchain integration provides a practical and effective solution for secure data sharing in modern cloud environments, particularly for security-sensitive applications such as healthcare, enterprise collaboration, and government information systems.

***KEYWORDS:*** *Blockchain, Cloud Computing, Secure Data Sharing, Smart Contracts, Byzantine Fault Tolerance, Decentralized Systems*

## I. INTRODUCTION

Cloud computing has become the backbone of modern information systems by providing scalable, flexible, and cost-efficient storage and computing services [1]. Organizations increasingly rely on cloud platforms to store and share sensitive data across distributed users. Despite these advantages, secure data sharing in cloud environments remains a critical challenge due to centralized control, limited transparency, and dependence on trusted third-party cloud service providers [2], [3].

Traditional cloud security mechanisms rely on encryption, authentication, and centralized access control enforced by cloud providers. Although these approaches improve confidentiality, they introduce single points of failure and remain vulnerable to insider threats and unauthorized policy manipulation [4], [5]. Once data is outsourced to the cloud, data owners lose direct control over access enforcement and auditing, which reduces trust in cloud-based data sharing systems [6].

As cloud-based data sharing becomes more collaborative and cross-organizational, the limitations of centralized security models become increasingly evident. Single points of failure, opaque auditing mechanisms, and dependency on trusted third parties reduce user confidence and hinder adoption in security-sensitive domains such as healthcare, finance, and enterprise Systems[8].

Blockchain technology has emerged as a promising solution to address trust and security issues in distributed systems [7]. Its decentralized ledger and immutable transaction records enable transparent and tamper-resistant data management without relying on centralized authorities. Smart contracts further enhance blockchain functionality by enabling automated and rule-based execution of access control and authorization policies [8], [9]. These characteristics make blockchain particularly suitable for secure data sharing in untrusted cloud environments.

However, direct integration of blockchain with cloud systems introduces scalability and performance challenges due to consensus overhead and storage limitations [10], [11]. Therefore, an effective framework is required that combines blockchain-based security with scalable cloud storage. This paper proposes a Blockchain-Driven Secure Data Sharing

Framework (BSDSF) that integrates blockchain, smart contracts, and hybrid storage architecture to ensure secure, transparent, and scalable cloud data sharing.

To address these challenges, this paper proposes a Blockchain-Driven Secure Data Sharing Framework (BSDSF) that integrates blockchain technology with cloud infrastructure using a hybrid on-chain/off-chain architecture. The framework decentralizes trust enforcement, automates access control through smart contracts, and ensures secure, transparent, and scalable cloud data sharing [10].

## II. RELATED WORK

Several studies have explored secure data sharing mechanisms in cloud environments using centralized encryption and access control techniques [4], [6]. While these methods enhance confidentiality, they depend heavily on trusted cloud providers and lack transparent auditing and user-controlled security enforcement.

Traditional cloud-based data sharing solutions primarily rely on centralized encryption, authentication, and access control mechanisms enforced by cloud service providers. While these approaches enhance confidentiality, they introduce single points of failure and remain vulnerable to insider attacks and policy manipulation [7]. Furthermore, centralized audit logs maintained by cloud providers lack transparency and can be altered without detection.

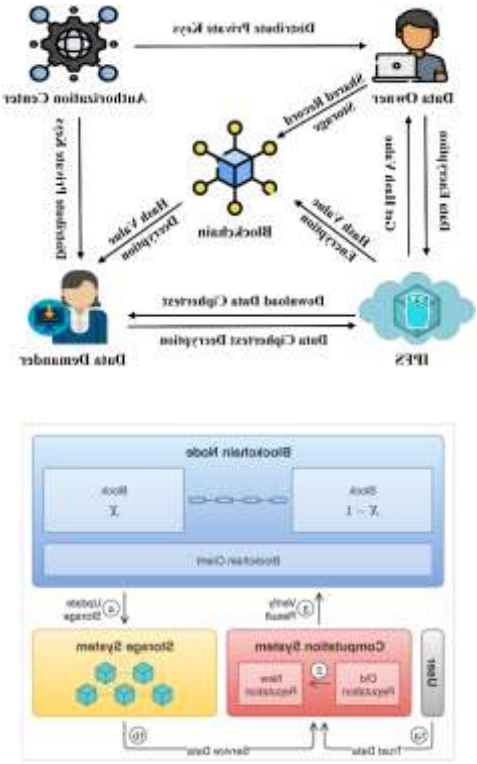
Recent research has investigated blockchain-based approaches for secure cloud data sharing [7], [8], [12]. Blockchain-enabled frameworks leverage decentralization and immutability to improve data integrity and accountability. Smart contracts have been widely used to automate access control and authorization decisions [9], [13]. Hybrid on-chain/off-chain architectures have also been proposed to reduce blockchain storage overhead [10], [14].

Despite these advancements, many existing solutions focus primarily on security enhancement while neglecting scalability, automation, or comprehensive workflow integration [11], [15]. In contrast, this paper proposes a holistic blockchain-driven framework that integrates off-chain encrypted storage, smart contract-based access control, and Byzantine fault-tolerant consensus within a unified architecture.

In contrast, this paper proposes a comprehensive blockchain-driven secure data sharing framework that integrates off-chain encrypted storage, smart contract–based access control, decentralized trust enforcement, and fault-tolerant consensus within a unified architecture [16].

## III. PROPOSED BLOCKCHAIN-DRIVEN SECURE DATA SHARING FRAMEWORK

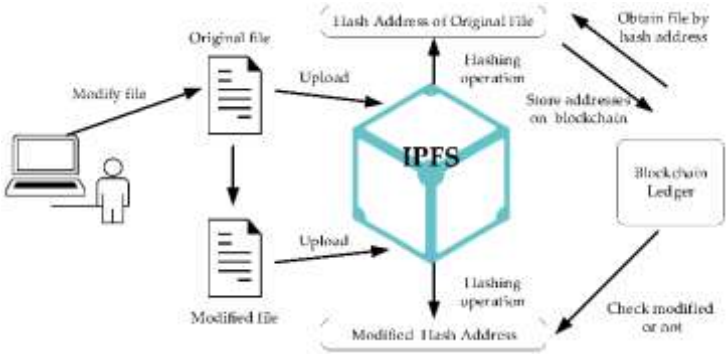
### A. Overall System Architecture



The proposed BSDSF adopts a hybrid on-chain/off-chain architecture to balance security, scalability, and performance. The system consists of four primary entities: Data Owner, Data Requester, Cloud/Distributed Storage, and Blockchain Network.

Figure 1 illustrates the overall architecture of the proposed framework. Data Owners encrypt data locally before uploading it to cloud or distributed storage. Only encrypted data is stored off-chain, while cryptographic hash values, access policies, and audit records are stored on the blockchain. The blockchain network acts as a decentralized trust layer responsible for access control enforcement and transaction validation through smart contracts.

### B. Secure Data Upload and Storage Workflow



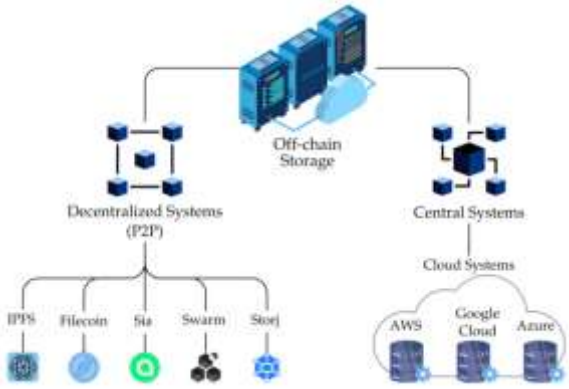



Figure 2 presents the secure data upload and storage workflow. The process begins with data encryption using a symmetric encryption algorithm. The encrypted data is uploaded to cloud or IPFS storage, while a cryptographic hash of the encrypted data is generated and recorded on the blockchain. This separation of data and metadata ensures scalability while enabling integrity verification at any time.

### C. Smart Contract–Based Access Control

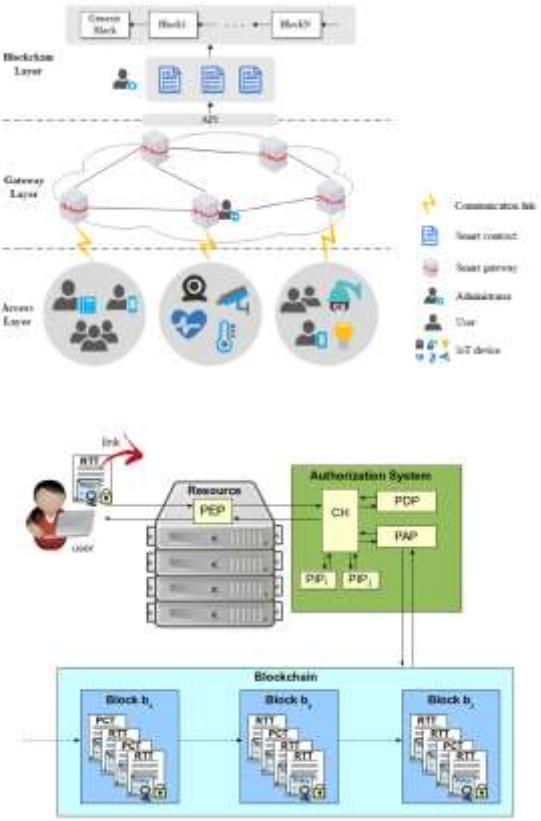



Figure 3 illustrates the smart contract–based access control process. When a Data Requester submits an access request, the smart contract verifies identity credentials and access policies.

Authorized requests are approved and logged immutably on the blockchain, while unauthorized requests are automatically rejected without human intervention.

## IV. SECURITY ANALYSIS

The proposed framework ensures data confidentiality through encryption, as only encrypted data is stored off-chain and decryption keys are shared exclusively with authorized users. Data integrity is guaranteed by recording cryptographic hash values on the blockchain, enabling immediate detection of any unauthorized modification.

Decentralized trust enforcement eliminates insider threats associated with centralized cloud control. Immutable blockchain records provide transparent and tamper-proof audit trails, ensuring accountability and traceability of all data access activities. Smart contracts ensure consistent and policy-driven access control enforcement.

## V. CONCLUSION

This paper presented a blockchain-driven secure data sharing framework for cloud environments that addresses key limitations of traditional centralized cloud security models. By integrating blockchain technology, smart contract automation, and hybrid storage architecture, the proposed framework ensures confidentiality, integrity, transparency, and accountability in cloud-based data sharing. The framework provides a practical foundation for secure and scalable data sharing in modern cloud environments.

## REFERENCES

1. P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” *NIST Special Publication 800-145*, 2022.
2. M. Ali, R. Khan, and S. Kumar, “A blockchain-based decentralized framework for secure cloud data sharing,” *IEEE Access*, vol. 13, pp. 34521–34535, 2025.
3. G. Kovács, A. Farkas, and L. Tóth, “Blockchain-enabled secure data sharing with smart contracts in cloud systems,” *IEEE Access*, vol. 13, pp. 51240–51255, 2025.
4. Y. Xu, J. Li, and H. Zhang, “Secure cross-domain cloud data sharing using blockchain and dynamic access control,” *IEEE Transactions on Cloud Computing*, early access, 2025.
5. S. Singh and R. Buyya, “Blockchain-based secure data sharing in cloud environments: A comprehensive review,” *IEEE Access*, vol. 13, pp. 28910–28930, 2025.
6. M. Zoughbi, A. Alsharif, and K. Salah, “Mitigating cloud security threats using blockchain-based audit mechanisms,” *IEEE Access*, vol. 13, pp. 40112–40128, 2025.

7. K. Li, Y. Wang, and X. Chen, "Privacy-preserving blockchain-based data sharing for cloud and healthcare systems," *IEEE Journal of Biomedical and Health Informatics*, vol. 29, no. 2, pp. 845–856, 2025.
8. A. Sharma, P. Verma, and S. Gupta, "Decentralized cloud storage and data sharing using blockchain and IPFS," *IEEE Access*, vol. 13, pp. 17892–17905, 2025.
9. R. Kumar, N. Patel, and V. Mishra, "Smart contract-based access control for secure cloud data sharing," *IEEE Systems Journal*, vol. 19, no. 1, pp. 112–123, 2025.
10. X. Gao, Y. Liu, and J. Wang, "Blockchain-enabled secure delegation and access control for cloud data sharing," *IEEE Access*, vol. 12, pp. 76540–76555, 2024.
11. H. Yi, Z. Zhou, and L. Sun, "Blockchain-based decentralized key management for cloud storage systems," *IEEE Transactions on Services Computing*, vol. 17, no. 6, pp. 3102–3114, 2024.
12. R. Punia, A. Kumar, and S. Bansal, "Blockchain-based access control mechanisms in cloud computing: A survey," *IEEE Access*, vol. 12, pp. 95410–95432, 2024.
13. J. Ma, Q. Zhang, and Y. Ren, "A security-oriented blockchain framework for cloud data sharing," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 3, pp. 1452–1464, 2024.
14. S. Sharma and M. Dave, "Blockchain-based collaborative cloud data sharing with immutable audit trails," *IEEE Access*, vol. 12, pp. 68211–68225, 2024.
15. K. Al-Zahrani, M. Alenezi, and A. Irshad, "Survey of blockchain-based access control models for cloud environments," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1342–1365, 2023.
16. Y. Wang, Z. Chen, and L. Xu, "Traceable and secure blockchain-based cloud data sharing using attribute-based encryption," *IEEE Transactions on Cloud Computing*, vol. 11, no. 4, pp. 1985–1998, 2023.
17. P. Ren, S. Guo, and H. Li, "A decentralized blockchain-based data security and sharing system for cloud platforms," *IEEE Access*, vol. 11, pp. 90210–90225, 2023.
18. X. Liu, J. Zhang, and M. Chen, "FairShare: Blockchain-enabled secure and fair data sharing for cloud and industrial IoT," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7841–7853, 2023.
19. M. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," *IEEE Distributed Systems Online*, vol. 23, no. 4, pp. 1–10, 2022.
20. K. Nguyen, T. Le, and H. Tran, "A survey of blockchain consensus mechanisms: Performance and security," *IEEE Access*, vol. 10, pp. 145233–145251, 2022.