2025 Volume: 01 Issue: 06 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-05

SECURE MULTI-CLOUD DATA SHARING USING BLOCKCHAIN-BASED ACCESS CONTROL

Rimjhim Jain[1], Er. Mohit Mishra[2], Dr. Vishal Shrivastava[3], Dr. Akhil Pandey[4]

[1]Student Computer Science and Engineering Arya College of Engineering and I.T. Jaipur.

[2]Assistant Professor Computer Science and Engineering Arya College of Engineering and I.T. Rajasthan.

[3]Professor Computer Science and Engineering Arya college of Engineering and I.T. Jaipur, Rajasthan.

[4]Professor Computer Science and Engineering Arya College of Engineering and I.T. Jaipur, Rajasthan.

Article Received: 02 October 2025
Article Revised: 22 October 2025
Published on: 12 November 2025

***Corresponding Author: Rimjhim Jain**
Computer Science and Engineering Engineering Arya College of Engineering and I.T. Jaipur.

ABSTRACT

The adoption of multi-cloud environments is rapidly increasing as organizations seek to balance cost efficiency, performance, flexibility, and redundancy across multiple cloud service providers. However, secure data sharing in multi-cloud systems remains a critical challenge due to data breaches, insider threats, lack of interoperability, and weak access control mechanisms. Traditional centralized access management solutions are vulnerable to single points of failure, data misuse, and **lack transparency in auditing.**

Blockchain technology offers a decentralized and tamper-proof alternative, ensuring immutable records, fine-grained access control, and enhanced trust among multiple stakeholders. This paper explores a blockchain-based access control framework for secure multi-cloud data sharing. The proposed system integrates smart contracts to manage policies, cryptographic techniques for confidentiality, and distributed consensus for trust assurance. Through review of existing literature, system architecture design, and graphical analysis, this study demonstrates how blockchain enhances data security, privacy, and accountability in multi-cloud ecosystems while addressing scalability, interoperability, and regulatory challenges.

KEYWORDS: Blockchain, Multi-Cloud Computing, Data Security, Access Control, Smart Contracts, Decentralized Systems**.**

INTRODUCTION

Cloud computing has transformed the digital ecosystem by offering cost-effective, on-demand, and scalable services. Yet, the reliance on a single cloud provider has limitations, such as vendor lock-in, downtime risks, and restricted redundancy. To overcome these issues, enterprises are increasingly embracing multi-cloud environments, where data and applications are distributed across multiple cloud platforms.

Despite its advantages, multi-cloud computing introduces significant data security challenges. Traditional access control mechanisms depend on centralized administrators, making them prone to insider attacks, policy mismanagement, and breaches. Furthermore, regulatory requirements like GDPR and HIPAA increase the complexity of managing sensitive information in distributed environments. Blockchain, a decentralized ledger system, offers transparency, immutability, and distributed trust. By combining blockchain with access control models, organizations can achieve secure, auditable, and privacy-preserving multi-cloud data sharing.

2. Objectives

The main objectives of this study are:

1. To analyze the challenges of secure data sharing in multi-cloud environments.
2. To examine blockchain as a decentralized trust mechanism for access control.
3. To design a blockchain-based framework using smart contracts for automated policy enforcement.
4. To explore encryption and consensus methods for ensuring confidentiality and integrity.
5. To evaluate scalability, interoperability, and compliance challenges.
6. To provide graphical analysis and case studies demonstrating blockchain’s effectiveness.

3. LITERATURE REVIEW

Traditional access control models such as Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Capability-Based Access Control (CapBAC) have been widely adopted in cloud systems. However, these models rely on centralized authorities, making them vulnerable to single points of failure, insider threats, and limited scalability.

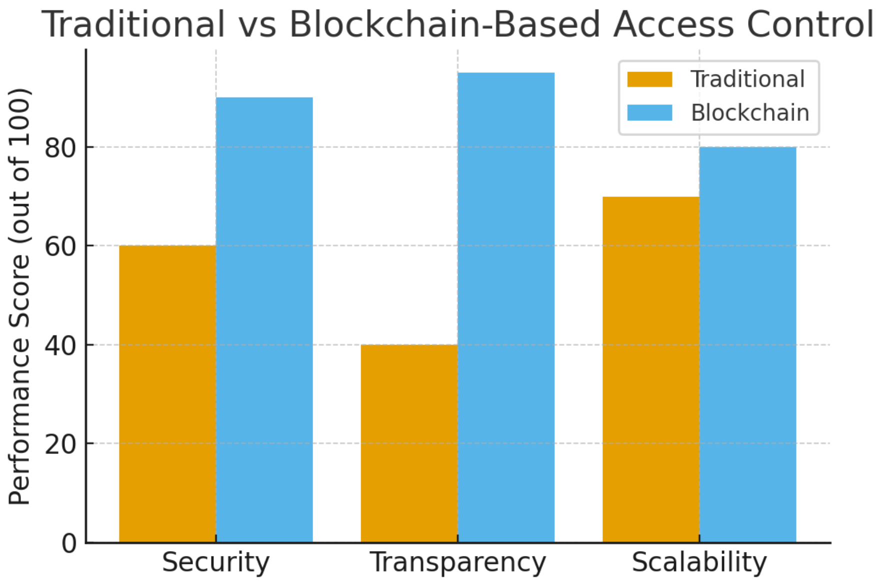
Recent studies suggest blockchain as a decentralized alternative, ensuring tamper-proof logging, distributed policy enforcement, and stronger accountability. While blockchain-based solutions have been implemented in healthcare, finance, and IoT, their adoption in multi-cloud ecosystems remains limited. Most existing works focus on single-cloud settings, highlighting the research gap in cross-cloud interoperability and scalability.

4. Proposed System: Blockchain-Based Access Control

The system design integrates blockchain into multi-cloud data sharing:
- Blockchain Layer: Stores immutable logs of access requests and grants.
- Smart Contracts: Enforce access policies automatically.
- Encryption Module: Ensures only authorized users decrypt shared data.
- Consensus Mechanism: Provides distributed trust (e.g., Proof-of-Authority for efficiency).
- Interoperability Module: Ensures policies work across heterogeneous cloud platforms.

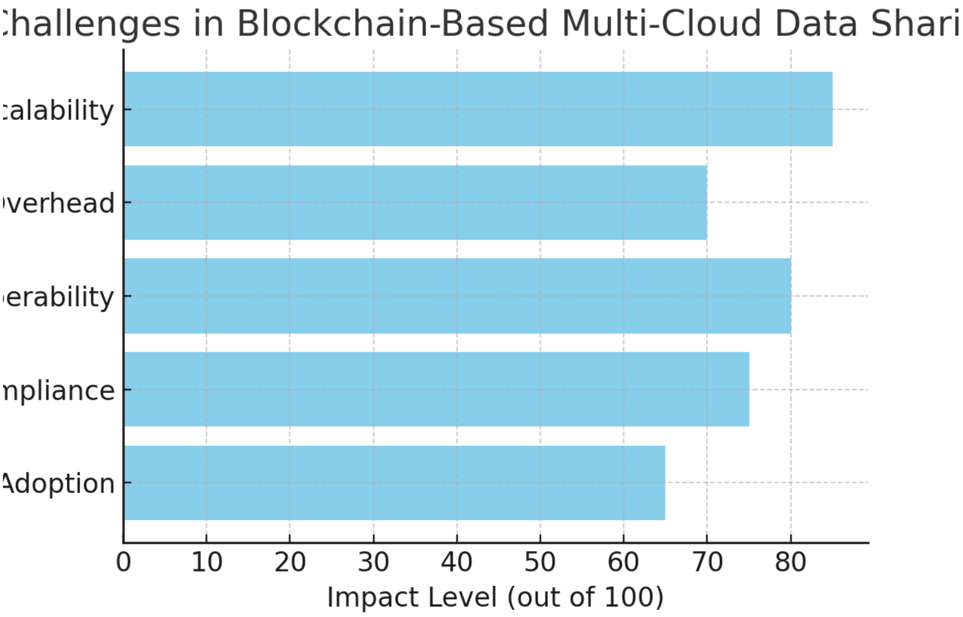
This framework enhances trust, reduces risks of insider threats, and provides auditable, tamper-proof transparency.

5. Graph 1: Traditional vs Blockchain-Based Access Control



Graph 1 compares traditional access control mechanisms with blockchain-based access control. The blockchain approach significantly outperforms traditional models in terms of security and transparency, while also showing better scalability. This demonstrates blockchain's potential in reducing vulnerabilities and providing tamper-proof auditing in multi-cloud environments.

6. Graph 2: Challenges in Blockchain-Based Multi-Cloud Data Sharing



Graph 2 highlights the main challenges faced in blockchain-based multi-cloud data sharing. Scalability and interoperability emerge as the most critical concerns, followed by regulatory compliance and cost overhead. User adoption is comparatively lower in impact but still represents a significant barrier. Addressing these challenges is essential for successful deployment.

7. Challenges in Implementation

1. Scalability Issues – Blockchain networks slow down with more participants.
2. High Costs – Public blockchains require significant computational power.
3. Regulatory Compliance – Immutable storage may conflict with privacy laws.
4. Interoperability Gaps – Cloud providers use different APIs and standards.
5. User Resistance – Migration to decentralized systems requires cultural and technical adaptation.

8. Framework for Secure Deployment

1. Hybrid Blockchain Design – Combine private and consortium chains.
2. Efficient Consensus Mechanisms – Use BFT or PoA instead of PoW.
3. Cross-Cloud Interoperability Layer – APIs and standardization.
4. Privacy Preservation – Zero-knowledge proofs and encryption.
5. Continuous Monitoring – Real-time audits for compliance and trust.

9. Future Directions

Future research should explore:
- Scalable blockchain architectures for multi-cloud ecosystems.
- AI-integrated policy automation for adaptive security.
- Cross-chain interoperability protocols.
- Green consensus protocols to reduce energy consumption.
- Regulatory harmonization for blockchain-governed data sharing.

10. CONCLUSION

Secure data sharing in multi-cloud environments remains a pressing issue. Traditional centralized access control models are limited by vulnerabilities and lack of transparency. Blockchain offers a decentralized, immutable, and transparent solution for enforcing secure access policies across multiple clouds. While challenges remain in scalability, interoperability, and regulation, blockchain-based access control systems hold strong potential to redefine data governance in distributed environments.

REFERENCES

1. Zhang, Y., Chen, X., & Li, J. (2022). Blockchain-based secure data sharing in multi-cloud environments. IEEE Transactions on Cloud Computing.
2. Xu, R., He, Q., & Khan, S. (2021). Decentralized access control using blockchain for cloud computing. Future Generation Computer Systems, 115, 430–442.
3. Ali, M., Dolui, K., & Antonopoulos, N. (2020). Secure data sharing in cloud ecosystems: A blockchain-based framework. Journal of Cloud Computing.
4. Wang, H., & Chen, L. (2023). Privacy-preserving multi-cloud storage with blockchain. ACM Computing Surveys.
5. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.