Proceeding International Conference Of Innovation Science, Technology, Education, Children And Health
Vol. 3 No. 2, 2023
e-ISSN : 2776-9062, page 123-126
Available online at: https://icistech.org/index.php/icistech/

Blockchain-Based Secure Data Sharing in Cloud Computing

[1*]Zahran Rayyan, [2]Rayyan Mahdi, [3]Syarifal Luthfan
[1-3] Effat University, Arab Saudi
Author's correspondence : zahranrayyan@gmail.com

Abstract Cloud computing has revolutionized data storage and management; however, security and privacy concerns remain critical challenges. This paper explores the integration of blockchain technology to enhance data security in cloud environments. A decentralized approach ensures data integrity, authentication, and tamper resistance. The proposed framework leverages smart contracts to enforce access control policies efficiently. Simulation results indicate that our model significantly improves data security without compromising system performance.

Keywords: Blockchain, Cloud Computing, Data Security, Smart Contracts, Decentralized Systems

1. INTRODUCTION

Cloud computing has emerged as a dominant paradigm for data storage, providing scalable, cost-effective, and flexible solutions for individuals and businesses. However, security concerns related to data privacy, unauthorized access, and data integrity remain unresolved. Traditional security models rely on centralized authorities, making them vulnerable to breaches and insider threats.

Blockchain technology offers a decentralized and tamper-proof alternative to traditional security mechanisms. By leveraging cryptographic techniques and distributed ledger technology, blockchain ensures data authenticity, transparency, and access control in cloud environments. This paper investigates how blockchain-based solutions enhance secure data sharing and access management in cloud computing.

2. LITERATURE REVIEW

Cloud Computing and Security Challenges

Cloud computing provides remote access to computing resources, but it faces several security risks, including unauthorized access, data leakage, and denial-of-service attacks. Centralized cloud architectures introduce single points of failure, making them attractive targets for cyberattacks.

Introduction to Blockchain Technology

Blockchain is a distributed ledger that records transactions in an immutable and transparent manner. It consists of decentralized nodes that validate transactions through consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS). Smart contracts further automate and enforce security policies without human intervention.

Received December 01, 2023; Revised December 15, 2023; Accepted December 29, 2023; Published December 31, 2023

Blockchain for Secure Data Sharing

Recent studies have explored the use of blockchain for securing cloud data. By replacing centralized authentication mechanisms with decentralized identity management, blockchain mitigates security risks while ensuring data privacy. Additionally, smart contracts can define and enforce access control policies, ensuring only authorized users can retrieve sensitive information.

3. METHODOLOGY

Framework Design

Our proposed model integrates blockchain technology into cloud environments for secure data sharing. The framework consists of the following components:

- **Decentralized Storage:** Data is stored in encrypted form and indexed on the blockchain for integrity verification.
- **Smart Contracts:** Define access control rules and automate permission management.
- **Consensus Mechanism:** Ensures transaction validation without a central authority.
- **User Authentication:** Blockchain-based identity verification reduces risks of unauthorized access.

Implementation Process

1. Users encrypt and upload data to the cloud.
2. A blockchain transaction records metadata, ensuring data authenticity.
3. Smart contracts enforce predefined access rules.
4. Authorized users retrieve data via blockchain-based authentication.

4. RESULTS

Security Enhancement

Blockchain's immutability ensures that unauthorized modifications are detected. Smart contracts prevent access breaches by automating authentication processes.

Performance Evaluation

Our simulation results indicate minimal latency overhead while significantly improving security. Compared to traditional access control models, blockchain-based authentication reduces risks of insider threats and unauthorized modifications.

User Adoption and Feasibility

Surveyed participants reported improved trust and transparency in data sharing. However, computational overhead for consensus mechanisms requires optimization for large-scale deployments.

5. DISCUSSION

Benefits of Blockchain Integration

- **Data Integrity:** Ensures immutability and verifiability of records.
- **Access Control:** Smart contracts enhance security policies.
- **Reduced Insider Threats:** Decentralized authentication removes reliance on central authorities.

Challenges and Limitations

- **Scalability:** Increased transaction volumes may impact performance.
- **Energy Consumption:** Consensus mechanisms such as PoW require substantial computational power.
- **Regulatory Concerns:** Adoption requires compliance with data protection laws.

6. CONCLUSION

Blockchain technology presents a promising solution for enhancing data security in cloud environments. By integrating decentralized authentication and smart contracts, cloud systems can achieve higher levels of security and reliability. Future research should focus on optimizing blockchain scalability and exploring hybrid cloud-blockchain architectures.

REFERENCES

Ahmed, Z., & Thomas, M. (2022). A comparative study of blockchain-based and traditional access control mechanisms. Computing Security Review, 19(1), 78-92.

Ali, M., Ahmed, F., & Khan, S. (2021). Blockchain for secure identity management in cloud computing. Journal of Information Security, 50(4), 120-136.

Johnson, L., Williams, M., & Brown, D. (2021). Decentralized cloud storage using blockchain. Journal of Cloud Computing, 9(4), 143-162.

Kim, S., Park, J., & Lee, K. (2019). Smart contracts for policy enforcement in cloud data sharing. IEEE Transactions on Information Security, 17(3), 45-67.

Li, H., Wang, X., & Zhang, J. (2020). A review of blockchain-based cloud security models. Cloud Security Journal, 15(2), 200-220.

Miller, J. (2019). The impact of blockchain on cloud security. International Cybersecurity Journal, 13(2), 87-102.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Nelson, P., Wang, X., & Liu, Y. (2020). Evaluating blockchain-based security in cloud storage. Journal of Emerging Technologies, 27(2), 99-115.

Patel, K., & Singh, R. (2020). Smart contracts for access control in cloud computing. International Journal of Computer Science, 12(1), 44-59.

Roberts, D., Green, T., & Harris, K. (2021). Next-generation blockchain solutions for cloud computing. Technology & Security Research, 30(4), 130-148.

Smith, R., & Anderson, T. (2018). Blockchain-enabled authentication in cloud systems. Security & Privacy Studies, 25(3), 66-80.

Wang, J., Zhang, L., Li, X., & Zhou, Y. (2021). Enhancing cloud security with blockchain. Journal of Digital Security, 45(3), 78-92.

White, C. (2020). Overcoming scalability issues in blockchain-integrated cloud systems. Cybersecurity Advances, 28(5), 188-204.

Yang, W., Liu, H., & Zhang, P. (2022). A hybrid cloud-blockchain framework for secure data sharing. Journal of Digital Innovation, 21(3), 55-72.

Zhao, X., Chen, Y., & Wu, Q. (2019). Secure data sharing in decentralized clouds. Cloud Computing Research, 34(2), 102-118.