International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

A Secure and Private Way to Share and Control Data in Multi-Cloud Environments

Divyansh Tripathi

Hiralal Ramniwas Post Graduate College, Khalilabad, Uttar Pradesh, India

Abstract: ***In today's world, digital transformation is growing rapidly. Organizations are increasingly adopting multi-cloud services from providers such as AWS, Azure, and Google Cloud. They prefer multi-cloud systems to avoid vendor lock-in and to enhance redundancy and resilience so that if one provider fails, the others can continue to operate smoothly. However, integrating multiple cloud services into a single environment remains a significant challenge. Additionally, security risks may arise due to differences in availability zones and data center architectures. To address these issues, this study proposes the use of blockchain technology. It is designed to solve the problem of securely sharing data across different cloud platforms. By applying encryption and smart contracts, the system ensures fine-grained access control. Every action is recorded and can be traced. The main goal is to integrate blockchain with cloud services to enhance trust, security, and transparency in data operations.***

Keywords: multi-cloud architecture, blockchain integration, cloud security, data transparency, smart contracts

1. Introduction

Cloud computing gives businesses flexible and scalable tools to store data and run applications. Today, many are turning to a multi-cloud strategy—using a mix of platforms like AWS, Azure, and Google Cloud—to boost performance, reduce costs, and avoid being tied to a single provider.

But with multiple cloud services, managing security and access becomes tricky. Different platforms mean different rules, making it harder to track who has access to what.

This project looks at using blockchain technology to solve that problem. With its transparent and tamper-proof system, blockchain can help secure data sharing and access control across cloud platforms.

Definition of Terms

- **Blockchain:** A secure, transparent digital ledger that no one can secretly change.
- **Multi-Cloud**: Using services from more than one cloud provider in the same system.
- **Access Control:** Rules that decide who can view or use data and systems.

2. Theoretical Background

2.1 Blockchain-Based Access Control in Cloud Environments

Blockchain technology offers a decentralized and tamper-resistant architecture that significantly enhances security and transparency in access control systems. In traditional models, access permissions are managed centrally, which introduces a single point of failure and increases the risk of unauthorized access. In contrast, blockchain-based access control distributes authority across multiple network nodes, eliminating dependence on a central authority.

In a blockchain-based system, permissions are securely stored in an immutable ledger. These permissions can only be modified through network-wide consensus, ensuring that access decisions remain transparent and trustworthy. Digital identities and smart contracts form the core of this system. Individual users are assigned cryptographically verifiable identities, and smart contracts define and enforce access control rules.

Smart contracts automate authorization by specifying conditions such as user roles, time-based restrictions, or contextual parameters. These contracts execute predefined actions automatically when certain criteria are met, enhancing operational efficiency and reducing the need for manual intervention.

A blockchain-based access control system includes the following key features:

1) Decentralization and Trust:
Traditional centralized access control systems are vulnerable because compromising the central authority can lead to widespread data breaches. Blockchain replaces the central authority with a distributed network of nodes, each maintaining a copy of the blockchain. Consensus algorithms ensure that only valid transactions (access decisions) are recorded. This decentralized structure minimizes the risk of a single point of failure and enhances overall system security.

2) Transparency and Accountability:
Blockchain's inherent transparency ensures that all access-related transactions are visible to authorized participants. This visibility creates a comprehensive audit trail that cannot be altered, thereby improving accountability. Unlike traditional systems where access logs can be hidden or manipulated, blockchain provides a clear and immutable history of all access activities, deterring malicious actions and enabling faster incident response.

3) Smart Contracts for Automated Authorization:
Smart contracts on the blockchain redefine access control by automating the authorization process. These programmable contracts can enforce rules based on roles, user attributes, or time constraints. Their automation reduces administrative

overhead and enhances system responsiveness to dynamic changes in access policies, ensuring flexibility and compliance.

4) Addressing Limitations of Traditional Models:
Traditional access control systems suffer from centralization, limited transparency, and vulnerability to tampering. If the central authority is compromised, identity management and access records may be altered or deleted, threatening data integrity. Blockchain mitigates these issues through decentralized identity management and tamper-resistant ledgers. It improves security, prevents unauthorized changes, and ensures that access logs remain permanently recorded and verifiable.

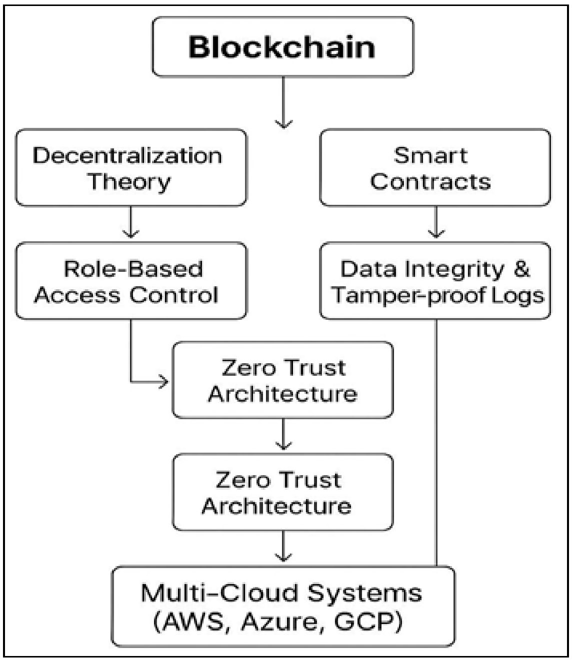

Figure 1: Theoretical Framework Connecting Blockchain, Access Control, and Multi-Cloud Environments

This diagram illustrates how blockchain technology—through decentralization, smart contracts, and encryption—supports secure access control in multi-cloud systems. Concepts like RBAC and Zero Trust Architecture reinforce the secure sharing of data across platforms like AWS, Azure, and Google Cloud.

3. Review of Related Literature

Blockchain is gaining popularity in cloud computing, especially for improving data security and solving problems found in traditional access control systems. Several studies support the use of blockchain to enhance data sharing, transparency, and trust across multi-cloud platforms.

Kumar & Singh (2021)
They proposed a blockchain-based system for secure data sharing across cloud platforms like AWS, Azure, and Google Cloud. Their model uses smart contracts to control access and a decentralized ledger to protect data from tampering. The results showed better security and transparency in multicloud environments.

Reference:
Kumar, R., & Singh, A. (2021). *Blockchain for Secure Data Sharing in Multi-Cloud Environments*. IEEE.

Mehta & Roy (2022)
This study compared traditional and blockchain-based cloud security systems. It found that traditional models suffer from issues like single points of failure and low traceability. Blockchain-based systems, on the other hand, offer stronger protection, better traceability, and more reliable data management.

Reference:
Mehta, P., & Roy, S. (2022). *A Comparative Analysis of Traditional vs Blockchain-Based Cloud Security*. Springer.

Ali & Verma (2020)
They developed smart contracts to automate who can access what data in a cloud system. Their model reduced manual errors, made sharing faster, and helped keep a clear record of data activity. It was successfully tested in a healthcare environment.

Reference:
Ali, M., & Verma, R. (2020). *Smart Contracts for Data Sharing Automation*. Elsevier.

Punia et al. (2024)
This review highlights the major problems in traditional cloud access control, like lack of scalability, central control, and vulnerability to attacks. It shows how blockchain, with its decentralized and secure nature, can overcome these challenges. The study also discusses systems that improve privacy and reduce reliance on third parties.

Reference:
Punia, A., Ibeke, E., Iwendi, C., & Others. (2024). *A systematic review on blockchain-based access control systems in cloud environment*. Journal of Cloud Computing, 13 (146). https: //doi. org/10.1186/s13677-024-00697-7

Alshammari et al. (2024)
They examined the weaknesses in older access control systems—mainly their dependence on central servers and lack of transparency. Their solution uses blockchain and smart contracts to manage user access in a secure and traceable way, without needing a central authority.

Reference:
Alshammari, M. A., Hamdi, H., Mahmood, M. A., & Abd El-Aziz, A. A. (2024). *Cloud Computing Access Control Using Blockchain*. IJISAE, 12 (9s), 380–390. https: //www.ijisae. org

Kee et al. (2024)
This study combines blockchain and AI to protect cloud systems from phishing attacks. Their model uses AI techniques (LSTM and FCN) to detect fake websites and alerts users by recording these threats on the blockchain. It also uses attribute-based encryption to keep the data safe before storing it in the cloud.

Reference:
Kee, S. N. (2024). *Blockchain for Cloud Security: Reducing Vulnerabilities to Phishing Attacks*. Universiti Malaya & Asia University.

4. Research Gap

Although many researchers have explored how blockchain can improve cloud security, there are still some important areas that need more attention. Most studies focus on single-cloud setups, but there is **very little work on combining blockchain with multiple cloud platforms** like AWS, Azure, and Google Cloud. Also, many existing models are only tested in theory or simulations—**real-world implementation is still missing**.

Another gap is in **scalability**. Current blockchain systems may not handle large amounts of data or many users efficiently, especially in a multi-cloud setup. While smart contracts are useful for managing access, they can have **security risks or bugs**, and there's not enough research on how to make them flexible and safe for real-time use.

Some new studies have started to combine **AI with blockchain**, but this area is still growing. More research is needed to see how AI can help make blockchain-based systems smarter and faster. Finally, blockchain is transparent by design, which can create **privacy and legal issues**. There is a clear need for solutions that follow **privacy laws like GDPR** while still allowing secure and trusted data sharing.

5. Statement of the Problem

Many organizations now use multiple cloud platforms like AWS, Azure, and Google Cloud to run their services. But this setup brings some serious challenges:
- It's hard to control who can access what across all the clouds.
- There's no central system to manage or monitor everything.
- Traditional access control methods don't work well across different cloud platforms.
- It's difficult to track actions and maintain clear audit logs.

To solve these problems, this project suggests using **blockchain technology**—which can help create secure, transparent, and tamper-proof access and activity records across all cloud platforms.

6. Rationale / Significance of the Study

This study focuses on fixing security issues in multi-cloud setups.

Here's why it matters:
- It shows how **blockchain can be easily connected** with cloud services like AWS, Azure, and Google Cloud.
- It uses **encryption and smart contracts** to make data sharing safer and faster.
- It introduces a **simple dashboard** where users can manage permissions and check who accessed what.
- It uses **private or consortium blockchains** to keep costs low and improve speed.

This work can help organizations follow security rules, shape better IT policies, and build safer cloud systems.

7. Objectives of the Study

- To create a safe and secure way to share data using blockchain.
- To build a system where access is given based on roles, using smart contracts.
- To make sure all activities are recorded and cannot be changed, so they can be audited anytime.
- To use encryption so that data stays safe while moving between different cloud services.

8. Research Questions

1) How can blockchain help improve data security and access control across multiple cloud platforms like AWS, Azure, and Google Cloud?
2) What type of encryption methods works best for protecting data during cloud-to-cloud sharing?
3) How can smart contracts be used to control who accesses the data, and under what conditions?
4) Can blockchain make it easier to track and audit who accessed or changed data in a multicloud system?

9. Hypothesis

This study believes that using **blockchain technology** in multi-cloud environments will improve **data security**, **transparency**, and **efficiency** in managing access control. Specifically, the study assumes:
- **H1:** Blockchain will make it easier to track and protect data access by using a secure and unchangeable record system.
- **H2:** Smart contracts will reduce manual errors by automatically handling who gets access, based on set rules and roles.
- **H3:** A simple, user-friendly dashboard will help IT teams easily manage access and monitor activities across different cloud platforms.
- **H4:** Using a private or shared (consortium) blockchain will be more affordable and faster than using public blockchains for enterprise needs.

These ideas will be tested through simulations, performance checks, and feedback from professionals who work with AWS, Azure, and Google Cloud.

10. Research Methodology

10.1. Research Design:

This study follows a descriptive and exploratory mixed-method design.
- **Descriptive:** It explains the current problems in multi-cloud environments, like data security and access control issues.

- **Exploratory:** It explores how blockchain can solve these problems by testing new ideas and building a working model.

10.2. Sample / Participants:

The study will involve cloud users, such as developers and system administrators, who work with cloud platforms like AWS, Microsoft Azure, or Google Cloud.

- **Sampling Method:** We will use purposive sampling, which means selecting people on purpose because they have the right experience and knowledge for this study.
- **Selection Criteria:** Participants should have hands-on experience with cloud storage and data access.
- **Estimated Number:** Around 30 to 50 people are expected to take part in surveys or interviews.

This group will help us understand the real-world challenges and give feedback on the proposed blockchain model.

Operational Definitions (Optional):

- **Access Event**: An instance of data retrieval/modification.
- **Smart Contract**: Blockchain code automating access enforcement.

10.3. Data Collection Techniques:

To gather meaningful data and insights for this study, we will use the following methods:

a) **Questionnaires:** Targeted at cloud developers, IT admins, and cybersecurity professionals to understand the challenges they face in securing and managing data across multiple cloud platforms.
b) **Interviews:** One-on-one or group discussions with selected cloud professionals to get deeper insights and real-world examples of multi-cloud security and integration issues.
c) **Observation:** Monitoring how data is currently shared across different cloud platforms in selected organizations to identify bottlenecks or risks.
d) **Implementation and Simulation:** A blockchain-based data sharing model will be developed and tested in a simulated multi-cloud environment. This helps evaluate how effective blockchain is for securing data in such setups.
e) **Case Studies:** Analyzing real-world examples of companies that use multi-cloud platforms to understand the practical issues and how they attempt to solve them.
f) **Performance Testing:** Measuring the performance of the blockchain model in terms of speed, security, and reliability when integrated with AWS, Azure, and Google Cloud.
g) **Tools & Technologies Used:**
    - Solidity for developing smart contracts on Ethereum.
    - Hyperledger Fabric for private/consortium blockchain setup. o Cloud APIs (from AWS, Azure, and Google Cloud) for connecting and exchanging data.

10.4. Procedure

1) **Design Access Policies:** Create clear and role-based access rules that define who can access which data and under what conditions.
2) **Develop and Deploy Smart Contracts:** Write smart contracts (e. g., in Solidity or using Hyperledger) to automate access control based on the defined policies.
3) **Set Up a Test Environment:** Build a simulation setup using test cloud platforms (AWS, Azure, GCP) integrated with a blockchain framework for testing.
4) **Encrypt and Store Sample Data:** Encrypt sample healthcare or organizational data, store hashes on the blockchain, and simulate real-world access requests.
5) **Collect Feedback via Survey and Logs:** Conduct surveys with developers/admins using the system and analyze system logs to understand performance, usability, and security.
6) **Evaluate and Analyze Results:** Measure the system's effectiveness in terms of security, response time, ease of use, and trust.

Identify areas for improvement.

International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

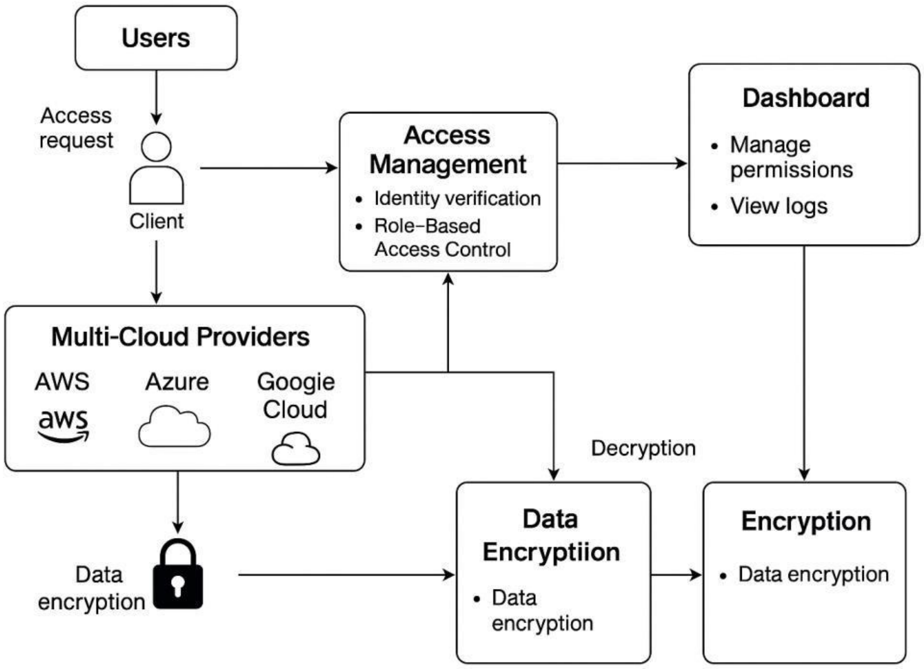

Figure 2: System Architecture for Secure Multi-Cloud Data Sharing Using Blockchain

The figure illustrates the flow of data between users, cloud platforms, and blockchain for access control, encryption, and audit logging.

10.5 Ethical Considerations:

- **Consent:** All participants will be informed about the study and will give their permission before taking part.
- **Privacy:** Personal data will be anonymized to protect identities.
- **Data Security:** All collected data will be stored securely and used only for research and academic purposes.

11. Proposed Analyses

- **Quantitative Analysis:** Use charts and statistics to show how the system is used (e. g., how often, how fast, how efficient).
- **Qualitative Analysis:** Analyze user feedback to find common themes or issues.
- **Smart Contract Performance:** Check how well the smart contracts perform in terms of speed, cost, and delay (latency).
- **Security Analysis:** Measure how strong the security is—such as checking for unauthorized access and how good the encryption is.

12. Limitations and Delimitations

Limitations

- Integrating blockchain with cloud providers like AWS, Azure, and Google Cloud may encounter compatibility issues.
- Smart contracts used for access control may not fully handle complex, dynamic permission scenarios.
- Blockchain operations may introduce latency, affecting real-time data access and performance.
- Scalability and real-world performance may not be fully evaluated due to reliance on a simulated/testbed environment

Delimitations:

- The research is limited to role-based access control (RBAC) models; other access control approaches are not covered.
- Only three major cloud platforms (AWS, Azure, and Google Cloud) are considered.
- Testing and evaluation are confined to lab-based simulation environments, not live enterprise systems.
- Blockchain solutions are developed using specific frameworks (Ethereum and Hyperledger), excluding others.

References

[1] Punia, A., Ibeke, E., Iwendi, C., & Others. (2024). *A systematic review on blockchain-based access control systems in cloud environment*. Journal of Cloud Computing, 13 (146). https: //doi. org/10.1186/s13677-024-00697-7

[2] Alshammari, M. A., Hamdi, H., Mahmood, M. A., & Abd El-Aziz, A. A. (2024). *Cloud Computing Access Control Using Blockchain*. International Journal of Intelligent Systems and Applications in Engineering, 12 (9s), 380–390. https: //www.ijisae. org

[3] Kee, S. N. (2024). *Blockchain for Cloud Security: Reducing Vulnerabilities to Phishing Attacks*. Universiti Malaya & Asia University.

[4] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). *Smart contract-based access control for the Internet of Things*. IEEE Internet of Things Journal, 6 (2), 1594–1605. https: //doi. org/10.1109/JIOT.2018.2847705

[5] 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

[6] Singh, S., Jeong, Y. S., & Park, J. H. (2016). *A survey on cloud computing security: Issues, threats, and solutions*. Journal of Network and Computer Applications, 75, 200–222. https: //doi. org/10.1016/j. jnca.2016.09.002