ISCSITR - INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN INFORMATION TECHNOLOGY (ISCSITR - IJSRIT)

Vol.2, Iss. 1, January-December, 2021, pp. 1-5.
https://iscsitr.com/index.php/ISCSITR-IJSRIT
Journal ID: 1551-1116

A Blockchain-Enabled Framework for Secure and Transparent Data Sharing in Multi-Cloud Environments with Role-Based Access Control

Anastasia Vasileiou,

Greece.

Abstract

With the proliferation of multi-cloud architectures and the rise in cross-organizational data sharing, the need for a secure, transparent, and role-aware data management system is more critical than ever. Traditional access control models often lack trust, auditability, and interoperability. This paper proposes a blockchain-enabled framework integrated with Role-Based Access Control (RBAC) to ensure secure and transparent data sharing across multi-cloud environments. Blockchain's immutability and decentralized trust model enhance accountability, while RBAC facilitates fine-grained access permissions. The proposed framework bridges critical gaps in existing architectures by combining cryptographic integrity, distributed ledger technologies, and cloud-native access control models.

Keywords: Blockchain, Role-Based Access Control (RBAC), Multi-cloud, Secure Data Sharing, Distributed Ledger, Access Management, Cloud Security, Decentralized Trust

How to cite this paper: Anastasia Vasileiou. (2021) A Blockchain-Enabled Framework for Secure and Transparent Data Sharing in Multi-Cloud Environments with Role-Based Access Control. *ISCSITR - INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN INFORMATION TECHNOLOGY (ISCSITR - IJSRIT)*, 2(1), 1–7.

URL: https://iscsitr.com/index.php/ISCSITR-IJSRIT/article/view/ISCSITR-IJSRIT_02_01_001
Published: 26th May 2021

1. Introductıon

The increasing adoption of **multi-cloud environments** by organizations has enabled scalable and efficient storage and computation. However, this flexibility comes with heightened concerns over **data security, access control, and interoperability**. In such distributed systems, the data traverses multiple administrative domains, each with distinct security policies and access rights.

Traditional access control mechanisms, including **Discretionary Access Control (DAC)** and **Mandatory Access Control (MAC)**, fall short when it comes to dynamic, fine-grained, and scalable control over distributed data access. This limitation has led to the wide adoption of **Role-Based Access Control (RBAC)** in cloud computing. RBAC allows permissions to be associated with roles rather than individuals, thus simplifying policy enforcement across dynamic user bases.

Nevertheless, existing RBAC implementations depend on centralized authorities, which may become single points of failure and are vulnerable to insider threats. Furthermore, there is limited **auditability and traceability** in these systems.

To address these challenges, **Blockchain technology** is gaining traction in the security domain due to its **immutability, decentralized trust, and tamper-proof audit trails**. Integrating blockchain with RBAC introduces a paradigm where **data access policies and operations are logged transparently**, enabling verifiable trust among cloud providers, users, and service auditors.

This paper introduces a hybrid framework that leverages **blockchain** to record all RBAC transactions, ensuring **transparent access control and secure data exchange** in a **multi-cloud environment**.

2. Problem Statement and Objectives

2.1 Problem Statement

In multi-cloud environments, existing RBAC systems are often centralized, opaque, and vulnerable to manipulation, offering no guarantees of transparency or resistance against tampering. Furthermore, traditional logging mechanisms cannot verify if access rights have been granted or revoked fairly and securely.

2.2 Objectives

- To design a **decentralized RBAC framework** using **blockchain** as a trust layer.
- To ensure **data access traceability and transparency** through immutable logging.
- To support **multi-tenancy and cross-cloud interoperability**.
- To enhance **data confidentiality, integrity, and access control** using cryptographic techniques and smart contracts.

3. Literature Review

The literature review synthesizes key contributions before 2020 concerning blockchain, RBAC, and secure multi-cloud data sharing.

3.1 Blockchain for Secure Data Sharing

Mukhopadhyay (2019) emphasized using blockchain to ensure trust and secure distributed storage across IoT platforms, which parallels cloud-based systems [1]. Fabian et al. (2015) developed a healthcare data sharing system across clouds using secret sharing and audit trails based on blockchain [2].

3.2 Role-Based Access Control (RBAC) Models

Zhou et al. (2013) proposed a trust-enhanced RBAC framework for cloud data using cryptographic role policies [3]. Yan et al. (2017) integrated trust and temporal constraints into RBAC for mobile clouds [4].

3.3 Multi-Cloud Security Challenges

Shajina and Varalakshmi (2017) introduced dual authentication protocols to secure multi-cloud user interactions [5]. Rajeswari and Kalaiselvi (2017) identified weaknesses in cloud storage security and proposed an RBAC-trust fusion model [6].

3.4 Hybrid Architectures with Blockchain and RBAC

Sharaf and Huang (2012) designed a hierarchical RBAC model for secure electronic health records (EHR) sharing in multi-clouds [7]. Sukmana et al. (2017) presented CloudRAID, emphasizing flexible access and file-level RBAC enforcement [8].

3.5 Identity and Policy Management

Suzic et al. (2015) addressed policy heterogeneity using interoperable RBAC for secure data exchange [9]. Kalra and Chaudhary (2019) introduced a formal identity management

protocol using role-based policies on a blockchain platform [10].

4. Proposed Framework

4.1 System Architecture

The proposed architecture consists of:

- **Blockchain Layer**: Stores immutable records of all RBAC transactions and role updates.
- **RBAC Policy Engine**: Assigns, revokes, and enforces access based on predefined roles.
- **Cloud Gateway**: Mediates between multiple cloud environments and ensures interoperability.
- **Smart Contracts**: Encapsulate logic for authorization, audit logging, and policy enforcement.

4.2 Workflow

1. Data Owner defines access policies via smart contracts.
2. A user requests data access through an RBAC interface.
3. Authorization is verified using smart contracts.
4. Blockchain logs the request and response for audit purposes.
5. Upon success, access is granted through cloud APIs.

5. Security and Performance Considerations

- **Confidentiality** is preserved using encryption.
- **Integrity** is guaranteed via hash-chaining of logs.
- **Non-repudiation** is achieved through blockchain's immutable ledger.
- **Scalability** is enabled by off-chain data storage and hybrid ledger solutions.
- **Interoperability** is ensured via API gateways for different cloud services.

6. Conclusion

The integration of blockchain with RBAC introduces a robust and transparent access control mechanism for multi-cloud environments. This framework enhances accountability,

ensures secure data sharing, and addresses limitations in centralized access systems. Future work will include implementing and benchmarking the prototype on Ethereum testnets and evaluating performance under various load conditions.

References

[1] Mukhopadhyay, S. (2019). *Secure Distributed Storage for the Internet of Things*. Springer.

[2] Fabian, B., Ermakova, T., & Junghanns, P. (2015). *Collaborative and Secure Sharing of Healthcare Data in Multi-Clouds*. *Information Systems*, Elsevier.

[3] Zhou, L., Varadharajan, V., & Hitchens, M. (2013). *A Trust Management Framework for Secure Cloud Data Storage Using Cryptographic RBAC*. Springer.

[4] Yan, Z., Li, X., & Kantola, R. (2017). *Heterogeneous Data Access Control Based on Trust and Reputation in Mobile Cloud Computing*. Springer.

[5] Shajina, A. R., & Varalakshmi, P. (2017). *A Novel Dual Authentication Protocol (DAP) for Multi-Owners in Cloud Computing*. *Cluster Computing*, Springer.

[6] Rajeswari, S., & Kalaiselvi, R. (2017). *Survey of Data and Storage Security in Cloud Computing*. *IEEE International Conference*.

[7] Sharaf, M., & Huang, C. T. (2012). *A Hierarchical Framework for Secure and Scalable EHR Sharing and Access Control in Multi-Cloud*. *IEEE Conf.*

[8] Sukmana, M. I. H., Torkura, K. A., & Meinel, C. (2017). *Redesign CloudRAID for Secure Enterprise File Sharing over Public Cloud*. *ACM Conf.*

[9] Suzic, B., Reiter, A., Venturi, D., & Reimair, F. (2015). *Secure Data Sharing in Heterogeneous Clouds*. *Procedia Computer Science*.

[10] Kalra, S., & Chaudhary, T. (2019). *Interoperable Identity Management for Multi-Cloud Platforms*. *IJBDI.*