International Journal of Advanced Multidisciplinary Research and Educational Development ISSN: **3107-6513**
Volume 2, Issue 3 | May – June 2026 | www.ijamred.com

Blockchain-Based Access Control for Cloud Storage

Ajay Gopal Kumawat

MCA & Modern College Of Engineering Pune

Ajay.kumawat.nanyo@gmail.com

Abstract:

This project presents a blockchain-based access control system for cloud storage designed to enhance security, transparency, and data integrity. Traditional cloud storage systems rely on centralized control, which makes them vulnerable to unauthorized access, data breaches, and lack of user trust. To overcome these issues, the proposed system integrates Blockchain for secure and tamper-proof access management and InterPlanetary File System for decentralized file storage.

The system is developed with a user-friendly interface using React, allowing users to interact efficiently. In this system, Admin and Owner can upload files, which are stored in IPFS and identified by a unique cryptographic hash (CID). Access permissions are managed through blockchain-based smart contracts, ensuring that only authorized users can view or download files.

Users with granted access can directly view files, while other users can request access, which is then approved or rejected by Admin or Owner. All activities are securely recorded, ensuring transparency and auditability. The proposed system provides a secure, decentralized, and scalable solution for modern cloud storage challenges.

Keywords: Blockchain ,InterPlanetary File System (IPFS), Decentralized Cloud Storage ,Role-Based Access Control (RBAC) ,Secure File Sharing

1.Introduction

Cloud storage has become a fundamental component of modern computing, enabling users and organizations to store, manage, and access data remotely with high scalability and flexibility. However, traditional access control mechanisms in

cloud systems are centralized, making them vulnerable to data breaches, unauthorized access, and single points of failure.

As the volume of sensitive data continues to grow, ensuring secure and transparent access control has become a critical challenge. Blockchain technology, with its

decentralized and immutable nature, offers a promising solution to address these limitations. By eliminating the need for a central authority, blockchain enhances trust, data integrity, and accountability.

Smart contracts further enable automated and fine-grained access control policies without human intervention. Integrating blockchain with cloud storage systems can significantly improve security, auditability, and user privacy. This research aims to design a decentralized access control framework that leverages blockchain to provide a robust and scalable solution for secure cloud data management.

Cloud storage is widely used for storing and accessing large amounts of data remotely.

Traditional access control systems are centralized, leading to security risks and single points of failure.

Blockchain technology provides decentralization, transparency, and tamper- proof data management.

Smart contracts enable automated and secure authentication and authorization proesses.

This research focuses on integrating blockchain with cloud storage to improve security, privacy, and auditability.

1. *Literature survey*

blockchain, ensuring tamper-proof access control and improved trust among users.

1. Blockchain-based Access Control System for Cloud Storage (2018)

This paper proposes a blockchain-based access control mechanism for cloud storage systems. The authors used a ciphertext-policy model with dynamic attributes to manage access permissions. Blockchain is used to store immutable records of access policies and user requests, ensuring transparency and security. The study highlights how decentralization removes dependency on a central authority and improves trust in cloud environments.

2. Blockchain-Based Data Security and Access Control System (2019)

This research focuses on improving cloud data security using blockchain technology. The system ensures data integrity, confidentiality, and authentication by storing transaction records on blockchain. The proposed model supports multi-user access control and prevents unauthorized data modification, making cloud storage more secure and reliable.

3. Blockchain-Based Access Control and Data Sharing (2021)

This paper introduces a decentralized access control system that integrates blockchain with IPFS. It eliminates single point failure and enhances data security by encrypting files and storing metadata on blockchain. The system achieved better performance with higher user detection accuracy and reduced response time, proving its efficiency.

4. Secure Cloud Storage Using Blockchain (2022)

This study analyzes how blockchain technology can solve cloud security issues. It emphasizes decentralization, cryptographic security, and removal of trusted third parties. The system ensures secure data storage and reduces risks related to centralized cloud systems, making it more reliable.

5. Cloud Computing Access Control Using Blockchain (2023)

This paper explores integrating blockchain with cloud computing for access control. It highlights features like immutability, transparency, and decentralization, which help secure access permissions. The system stores policies on blockchain, ensuring tamper-proof access control and improved trust among users.

6. Systematic Review on Blockchain-Based Access Control (2024)

This review paper studies multiple blockchain-based access control systems. It concludes that blockchain improves security by providing decentralized, transparent, and tamper-proof mechanisms. It also highlights challenges like scalability and transaction delays but confirms blockchain as a strong solution for cloud security.

7. Blockchain-Based IoT Data Sharing System (2017)

This paper presents a blockchain-based framework for secure data sharing in IoT systems. It replaces centralized control with distributed access management, allowing users to control their own data. The system ensures secure storage and access using blockchain as an audit layer.

8. Blockchain Access Control: State of the Art (2019)

This study reviews existing access control systems and identifies their limitations such as lack of privacy and reliance on third parties. It explains how blockchain can overcome these problems by providing decentralized and secure access control mechanisms.

9. Blockchain-Based RBAC Model for Cloud (2022)

This research proposes a role-based access control (RBAC) model using blockchain. It uses smart contracts to manage roles and permissions in a cloud environment. The system ensures secure role verification and efficient access control, improving cloud data security.

10. Fabric-Based Secure Storage ad Access Control (2021)

This paper presents a blockchain-based storage system using Hyperledger Fabric. It provides fine-grained access control using smart contracts and ensures data integrity through distributed consensus. The system achieves secure data sharing with high performance and scalability.

Methodology

A. 3 Need of study

With the exponential growth of data and the increasing adoption of cloud computing, secure data storage and access control have become critical concerns. Traditional cloud systems rely on centralized architectures, where data is controlled by a single authority. This leads to major issues such as data breaches, unauthorized access, lack of transparency, and single point of failure. Users have limited control over their data, which reduces trust in cloud service providers.

To address these challenges, there is a strong need to explore advanced technologies that provide decentralization, security, and transparency. The use of Blockchain enables a tamper-proof and immutable system where access permissions and transactions are securely recorded. Similarly, InterPlanetary File System allows decentralized file storage, ensuring data integrity and availability without relying on a central server.

Another important need of this study is to implement role-based access control, where only authorized users can access specific data. Existing systems often lack fine-grained access control and proper audit mechanisms. This study aims to provide a system where Admin and Owner can manage access, users can securely view data, and other users can request access in a controlled manner.

Furthermore, the study is important to improve auditability and accountability by recording all activities on blockchain, making the system transparent and traceable. It also aims to reduce risks associated with insider threats and data manipulation.

In addition, this research contributes to the development of scalable and real-world applicable solutions by integrating modern technologies such as blockchain, IPFS, and web-based interfaces. It helps in understanding how decentralized systems can be practically implemented to solve real-world cloud security problems.
Overall, the need of this study arises from the growing demand for secure, reliable, and decentralized cloud storage systems that provide better user control, enhanced data protection, and improved trust in digital environments.

4.Problem Statement

Cloud storage systems are widely used for storing and sharing data, but most existing solutions rely on centralized architectures. This centralization creates several issues such as data breaches, unauthorized access, lack of transparency, and single point of failure. Users must trust cloud service providers to manage their data securely, but they have limited control over how access permissions are handled. Traditional access control mechanisms are also vulnerable to insider threats and manipulation, making them unreliable for sensitive data management.
Furthermore, current systems often lack fine-grained access control and proper auditability. It is difficult to track who accessed the data and when, leading to poor accountability. Unauthorized users may gain access due to weak permission management, and there is no tamper-proof mechanism to verify access activities.
To address these challenges, there is a need for a secure, decentralized, and transparent access control system. By using Blockchain, access permissions and transactions can be stored in an immutable and verifiable manner. Additionally, integrating InterPlanetary File System enables decentralized file storage, ensuring data integrity and availability.
Therefore, the problem addressed in this project is to design and implement a system that provides secure file storage, role-based access control, and transparent data management, eliminating the limitations of traditional cloud storage systems.

5. Research Methodology

5.1 System Architecture

The proposed system follows a decentralized architecture integrating blockchain with cloud storage. Users interact with the cloud through a secure interface, while access control policies are managed on the blockchain. Smart contracts are deployed to handle authentication and authorization processes. Each access request is verified through the blockchain network, ensuring transparency and immutability. The architecture eliminates reliance on a central authority and provides secure data sharing between users.

5.2 Data Security and Access Control Mechanism
Sensitive data is stored in encrypted form in cloud storage to ensure confidentiality. Blockchain is used to maintain access control policies and user permissions in a

tamperproof manner. Smart contracts enforce finegrained access control by validating user identity and permissions before granting access. Cryptographic techniques such as hashing and encryption are used to secure user credentials and data transactions. This ensures only authorized users can access specific data.

5.3Blockchain Integration and Smart Contract Execution The system utilizes blockchain technology to record all access activities in a distributed ledger. Smart contracts automate decisionmaking for granting or denying access requests based on predefined rules. Each transaction is verified by the network, ensuring trust and preventing unauthorized modifications. The immutable nature of blockchain provides complete auditability of data access. This integration enhances security, transparency, and accountability in the cloud environment.

5.4 Web Application Framework and user-friendly interface. The backend is developed using Node.js and Express.js to handle APIs and server logic. Blockchain interaction is achieved through Web3.js connected to Ethereum. For secure storage, IPFS is used to store encrypted data in a decentralized manner

6. Results and Discussion
The proposed system was successfully designed and implemented to provide secure and decentralized access control for cloud storage. The system integrates Blockchain for managing access permissions and InterPlanetary File System for distributed file storage. The frontend developed using React enabled smooth user interaction and role-based functionality.
During testing, the system demonstrated that Admin and Owner users could upload files and grant access using usernames. The uploaded files were successfully stored on IPFS, generating unique CIDs, which were then recorded on the blockchain. Authorized users were able to directly view files without any issues, while unauthorized users were restricted from accessing them. The request-based access mechanism also worked effectively, where "Other" users could request access and receive approval or rejection from Admin/Owner.
The results indicate that the system provides improved security, transparency, and control compared to traditional cloud systems. All access activities were recorded on blockchain, ensuring auditability and preventing data tampering. The decentralized nature of IPFS eliminated reliance on a single storage server, increasing availability.
However, some limitations were observed, such as transaction delays in blockchain and dependency on internet connectivity. Despite these challenges, the system proved to be a reliable and scalable solution for secure cloud storage.
Overall, the project demonstrates that integrating blockchain with IPFS can effectively enhance data security, access control, and system transparency in modern cloud environments.
7. Conclusion
This research presents a blockchain-based access control system for cloud storage that addresses the key limitations of traditional centralized systems. By integrating Blockchain with InterPlanetary File System, the system ensures secure, transparent, and decentralized data management.

The implemented solution successfully enables role-based access control, where Admin and Owner can upload files and grant permissions, authorized users can directly access files, and other users can request access. The use of blockchain ensures that all transactions and permissions are recorded in an immutable and tamper-proof manner, improving trust and accountability. At the same time, IPFS provides efficient and distributed file storage, ensuring data integrity and availability.

The results demonstrate that the system enhances security, auditability, and user control compared to traditional cloud storage methods. Although some challenges such as transaction latency and system complexity exist, the overall performance proves the effectiveness of the proposed approach.

In conclusion, this project provides a reliable, scalable, and future-ready solution for secure cloud storage. It also highlights the potential of combining blockchain and decentralized storage technologies to solve real-world data security problems and opens opportunities for further research and improvements in this domain.

8. Future Scope
The proposed system demonstrates a secure and

decentralized approach for cloud storage; however, several enhancements can be implemented to improve its performance, usability, and scalability.

In the future, the system can be enhanced by integrating advanced encryption techniques to provide an additional layer of data security before storing files on InterPlanetary File System. This will ensure that even if data is accessed, it remains protected.

Scalability can be improved by using more efficient or high-performance Blockchain networks or Layer-2 solutions to reduce transaction costs and delays. This will make the system more suitable for large-scale real-world applications.

The system can also be extended by implementing fine-grained access control mechanisms, such as time-based or attribute-based access permissions. This would allow more flexible and dynamic control over data sharing.

Another possible enhancement is the integration of multi-factor authentication (MFA) and biometric verification to strengthen user authentication and prevent unauthorized access.
Additionally, the user interface can be further improved by adding mobile application support and better user experience features, making the system more accessible and user-friendly.

Future work may also include integration with enterprise cloud platforms, support for real-time monitoring and analytics, and implementation of AI-based anomaly detection to identify suspicious activities.
Overall, the system can evolve into a fully scalable, intelligent, and enterprise-ready secure cloud storage solution by incorporating these advancements.

9. References

[1] Mastering Blockchain, Imran Bashir, Packt Publishing, 2018.
[2] Blockchain Basics, Daniel Drescher, Apress, 2017.
[3] Ethereum Foundation, “Ethereum Whitepaper and Documentation,” https://ethereum.orghttps://ethereum.org
[4] InterPlanetary File System Documentation, https://docs.ipfs.techhttps://docs.ipfs.tech
[5] React Documentation, https://react.devhttps://react.dev
[6] Node.js Documentation, https://nodejs.orghttps://nodejs.org
[7] Solidity Documentation, https://docs.soliditylang.orghttps://docs.soliditylang.org
[8] Research Paper: “Blockchain-Based Access Control for Cloud Storage Systems,” IEEE, 2020.
[9] Research Paper: “Secure Data Sharing in Cloud Using Blockchain Technology,” Elsevier, 2021.
[10] GitHub, Open-source repositories and implementation references, https://github.comhttps://github.com