WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Blockchain - Based Secure Data Sharing in Cloud Computing

***SNEH CHAKRAPANI[1] , Dr. VISHAL SHRIVASTAVA[2], Dr. AKHIL PANDEY[3] , Er. Mohit Mishra[4]***

[1]B.TECH. Scholar,[2,3]Professor, [4]Assistant Professor
Computer Science & Engineering
Arya College of Engineering & I.T. India, Jaipur
[1]snehchakrapani2002@gmail.com, [2]vishalshrivastava.cs@aryacollege.in, [3]akhil@aryacollege.in, [4]mohit28sep@gmail.com

**ABSTRACT:**

Cloud computing revolutionized data storage and access by providing scalable, on-demand resources to individuals and organizations. Cloud computing has also introduced serious concerns regarding the security of data, particularly when data sharing. Centralized authorities were used by conventional cloud infrastructures for policy enforcement and access control and therefore are susceptible to single points of failure, unauthorized access, and data breaches. Block chain technology offers a ground breaking solution to bypass the limitations of such conventional cloud infrastructures due to its tamper-resistant, transparent, and decentralized nature.

This research introduces a framework grounded on block chain technology with the purpose of enhancing secure information sharing in cloud computing environments. The framework uses the application of smart contracts for the enforcement of policies on access control automation, role-based access control, and delivery of immutable access logs. The system also applies encryption protocols for the delivery of end-to-end security of information and decentralized consensus mechanisms for the verification of transactions. Based on a comprehensive review of literature, system design, and comparative analysis, this research explains how block chain technology can support confidentiality, integrity, and traceability of data transactions in cloud systems.

The findings indicate that the suggested method considerably enhances trust and transparency levels while keeping the performance level. Some of the potential uses are sharing healthcare data, communication between agencies, and corporate file sharing. The paper concludes by observing some of the existing limitations such as scalability and integration issues and proposing directions for future work towards the development of block chain-based cloud security models.

**Keywords: Cloud Computing, Blockchain, Data Security, Smart Contracts, Access Control**

## Introduction

### *2.1 Background on Cloud Computing Security*

Cloud computing has surfaced as a crucial framework for contemporary digital business activities, providing scalable, economical, and remote access to data. Businesses from various domains including health, finance, education, and governmental bodies have adopted cloud solutions to improve their operational efficiency and data handling capabilities. At the same time, with this rapid shift, security has surfaced as one of the foremost issues. Centralized cloud frameworks usually suffer from data leakage, the unauthorized use of information, insider abuse, and poor audit logs within organizations. Several incidents in the previous years have publicly revealed highly confidential documents and data due to failed access authentication protocols and improperly set up cloud systems. These issues highlight the need for new and more robust solutions to security.

### *2.2 Importance of Decentralized Models in Modern IT Infrastructure*

As with all systems, traditional cloud security frameworks incorporate a central control model where an entity manages processes such as authentication, authorization and access control. This approach, while somewhat useful, exposes the framework to centralized systems' most common setback: a single point of failure.
Compromise the central system, and everything from data to system settings can be manipulated. Data is stored can also be rendered vulnerable to theft and manipulation. Furthermore, users and stakeholders have lowered trust with centralized setups due to the inability to provide verifiable and transparent access data log histories. Centralized systems also struggle with ever-important data access history.

The mitigation seen in form of Suggested Citation's block chain-agnostic framework enhancements stems from immutable, decentralized distributed ledger technology. Trust-less systems do not require a central authority. Utility and application on the block chain is endless. Its attributes such as

immutability, cryptographic security, transparency and consensus-based validation make it ideal for securing data transactions. With access control through programmable tokens, policies can be enforced, monitored and kept unalterable. The automated solution provided by smart contracts also supports full accountability and enhanced cloud security enabling a stronger user trust due to decentralized control.

***Scope and Purpose of This Paper***

This research paper looks into the implementation of block chain technology on cloud computing paradigms with the aim of resolving data security and privacy issues, particularly in the area of data sharing. The proposed system utilizes the core tenets of block chain technology to formulate an auditable, secure and scalable data-sharing framework for cloud users. It analyses how dynamic access control is enforced through smart contracts, confidentiality is upheld by encryption, and immutable logs support transparency along with compliance.

This paper also describes the comparison study of the conventional security models versus the block chain model and discusses identification of use cases for various domains. It further highlights the shortcomings and scope of improvement in cloud infrastructure based on block chain technology. In doing so, reliable mechanisms for data sharing in the cloud is addressed in the form of practical and secure solutions in the framework of digitally enabled world.

## Background

### *3.1 Overview of Block chain Technology*

Block chain is a revolutionary technology as it provides a decentralized and distributed ledger that records transactions. Each block contains the hash of the prior block, a timestamp, and the transaction data. This guarantees that no alterations can be made once the data is recorded and changes would need to be made to every successive block if any retroactive edits were to be made. Such reliability, along with transparency, makes block chain a great candidate for secure data management systems. It was first used in Bitcoin as a decentralized cryptocurrency, but block chain technology has expanded into various other fields such as healthcare, finance, and supply chain management due to its secure and transparent record-keeping capabilities.

### *3.2 Cloud Computing Security Challenges*

Cloud computing offers flexible and scalable resources over the internet, enabling organizations to remotely access and store information. However, the model offers some security issues:

Data Breaches: Personal data contained in the cloud could be accessed by unauthorized persons, leading to expensive and reputational damage.

- Insider Threats: Malicious users or administrators can exploit their access rights to compromise data integrity.
- Insecure Interfaces and APIs: Cloud interfaces may be vulnerable to attacks by attackers to obtain unauthorized access.
- Account Hijacking: Compromised credentials could allow attackers to intercept activity and manipulate data.
- Lack of Transparency: There is often less visibility for users into the cloud provider's operation, and therefore making it hard to ascertain security controls and compliance.

These issues raise the importance of sound security design in providing a guarantee of cloud data confidentiality, integrity, and availability.

### *3.3 Integrating Block chain with Cloud Computing for Enhanced Security*

Using block chain technology in cloud computing platforms can rectify most of the aforementioned discussed security problems:

- Decentralization: By distributing information across a network, block chain eliminates points of failure, making the system more resilient.
- Immutability: Information once written on the block chain cannot be modified, and that gives data integrity.
- Transparent Access Control: Smart contracts can enforce and automate access rules and provide transparent and tamper-evident access control solutions.
- Auditability: Everything that happens was written down and time-stamped, enabling full auditing and compliance checking.

## 4. Literature Review

Cloud security has long been a priority because the use of cloud services is on the rise in various sectors. The traditional security solutions mainly include encryption, authentication procedures, and firewalls; yet, these have proven to be insufficient in protecting confidential information from attacks and unauthorized access. Studies show that a centralized security model is vulnerable in nature because it relies on a single point of control, which, in the event of breach, would expose huge amounts of confidential information.

Recent research has identified blockchain technology as a game-changing solution for enhancing cloud security. Blockchain's decentralized nature does away with the requirement for a trusted third party, thus minimizing the security risks associated with centralized control systems. Blockchain also guarantees data integrity by a tamper-resistant ledger of transactions, hence making it practically impossible for unauthorized entities to modify stored data.

One of the prominent research studies by Zyskind et al. (2015) introduced a decentralized system for managing personal data using blockchain technology that proved the ability of smart contracts to enable user-centric access control. Likewise, Yue et al. (2017) introduced a secure data sharing system for healthcare, which was blockchain-based, and thus proved its usage in securing sensitive data along with easy access for rightful users.

Despite these benefits, blockchain technology application in cloud computing comes with its challenges. One of the largest challenges is scalability since traditional blockchain networks like Bitcoin and Ethereum are marked by high latency and low throughput. Off-chain storage, sharding, and hybrid architecture are among the solutions proposed to address this challenge. Additionally, the energy usage of blockchain networks, particularly those with Proof-of-Work (PoW) consensus algorithms, poses a challenge in terms of sustainability and economic viability. Another key concern is the complexity in using blockchain. Most organizations do not have the ability necessary to leverage blockchain into operation in conjunction with current cloud infrastructures. Moreover, data protection regulations such as GDPR and HIPAA are to be adhered to when deploying blockchain-powered security solutions to be utilized in clouds.

Beneath these drawbacks, however, the advantages of blockchain technology over cloud security exceed its disadvantages. As research continues, novel consensus protocols such as Proof-of-Stake (PoS) and Directed Acyclic Graphs (DAG) are being devised to make blockchain technology more efficient. Moreover, interoperability of blockchain networks as well as that of cloud services is a space of active development with the eventual goal of implementing more scalable and adaptable solutions.

This research extends current work by introducing a blockchain-based architecture tailored for cloud security, thus solving core challenges and optimizing performance and usability at the same time. The suggested model optimizes access control, ensures data integrity, and prevents threats related to centralized security architecture.

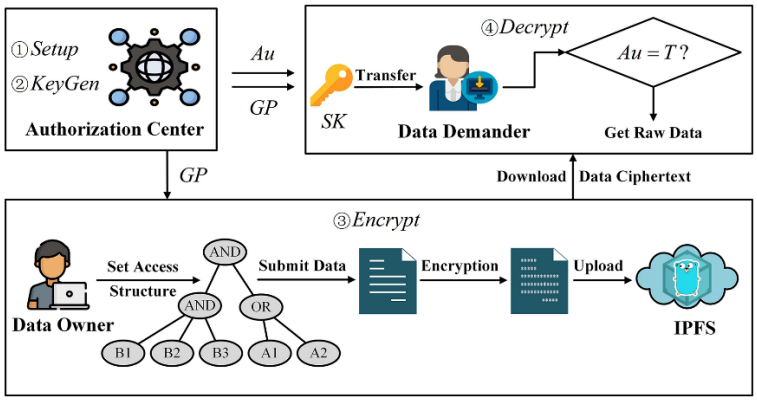


**Fig 1: Blockchain based data sharing**

## 5. Proposed System

### *5.1 System Overview*

The suggested system leverages block chain technology along with cloud computing to enable safe, clear, and efficient sharing of data. With the decentralization of block chain as well as cloud scalability, the system will cater to common security issues such as unauthorized access, data manipulation, and lack of auditability.

The major components of the system are:

- Data Owner (DO): the Company that creates and owns the data to be exchanged.
- Data Requester (DR): Registered user-requesting access to the data.
- Cloud Storage Provider (CSP): Offers scalable storage features for encrypted data.
- Block chain Network: Stores unalterable transaction and access control history.
- Smart Contracts: Enforce access control policies and apply data-sharing conditions automatically.
- Inter-Planetary File System (IPFS): Offers off-chain decentralized storage of big files.

### *5.2 Architectural Design*

The system architecture isolates data storage and access control mechanisms and thus provides scalability and security.

1. **Data Storage and Encryption:**

The DO encrypts the data using symmetric encryption (e.g., AES-256) to ensure confidentiality.
The information is encrypted and kept within the CSP or IPFS.

2. **Metadata Generation:**

An unpredictable hash of the encrypted data is generated by using a cryptographic hash function (e.g., SHA-256).
This hash, along with permissions and access control policies, is wrapped in a smart contract.

3. **Block chain Implementation:**

The smart contract is implemented on the block chain platform to ensure immutability and transparency.
Every transaction, ranging from data access requests to approvals, is stored on the block chain.

4. **Access Request and Verification:**

The DR begins a data request for access to the block chain network.
The smart contract authenticates the DR's credentials, and access rights according to the specified policies.

5. **Key Distribution**

Upon successful verification, the Data Owner encrypts the symmetric key with the Data Receiver's public key and publishes it through the block chain.
The DR decrypts the symmetric key with their private key to obtain the encrypted data from the CSP or IPFS.

### *5.3 Smart Contract Functionality*

Smart contracts are one source of enforcement and automation of access control policy. Their functions include:

- Access Control Enforcement: Specify and enforce who may access certain data based on roles, attributes, or other factors.
- Audit Logging: Automatically log all data access requests and grants, offering an open audit trail.
- Revocation Mechanism: Permit the DO to, if needed, revoke access rights and update this in the smart contract.
- Notification System: Notify relevant stakeholders of access requests, approvals, or revocations through block chain events.

### *5.4 Security Considerations*

The suggested system solves some security issues:

- Confidentiality: Information is encrypted prior to storage so that decryption and access can only be achieved with authorized DRs.
- Integrity: The cryptographic hash ensures that any modification in the data will be identifiable.
- Availability: Data on decentralized networks such as IPFS increases data availability and resistance to single points of failure.
- Auditability: All transactions are recorded to the block chain, and a verifiable audit trail is created for monitoring and compliance.

### *5.5 Strengths of the Proposed System*

- Decentralization eliminates reliance on one sole source, thus reducing the threat posed by single points of failure.
- Transparency: Every transaction is recorded on the blockchain, therefore, guaranteeing trust among participants.

- Scalability: Off-chain storage technologies such as IPFS enable the system to scale large amounts of data effectively.
- Flexibility: Smart contracts can be programmed to have advanced access control policies suitable for various applications.

### *5.6 Potential Use Cases*

- Healthcare: Safe exchange of patient records with authorized medical professionals while maintaining patient confidentiality.
- Finance: Regulated exchange of sensitive financial information between institutions for audit or compliance.
- Research Collaboration: Enables safe sharing of data among researchers from different institutions, while maintaining data integrity and proper attribution.

## 6. Implementation

- **System Architecture:** The system utilizes a blockchain network, i.e., Ethereum or Hyperledger, and a cloud storage system for secure and decentralized access to information.
- **Workflow:** Data is encrypted when it is being uploaded into the cloud and metadata is stored on the blockchain. Access is regulated by smart contracts, allowing only authorized users to decrypt and access the data.
- **Consensus Mechanism:** The network utilizes a Proof-of-Stake (PoS) consensus mechanism to confirm transactions in a cost-effective and power-efficient way.
- **Security Features:** Multiple-factor authentication (MFA) is present within the system for enhanced access management and protection from unauthorized access.
- **Transaction Validation:** a network of nodes distributed across the block chain, which maintains integrity and consistency, confirms every transaction.

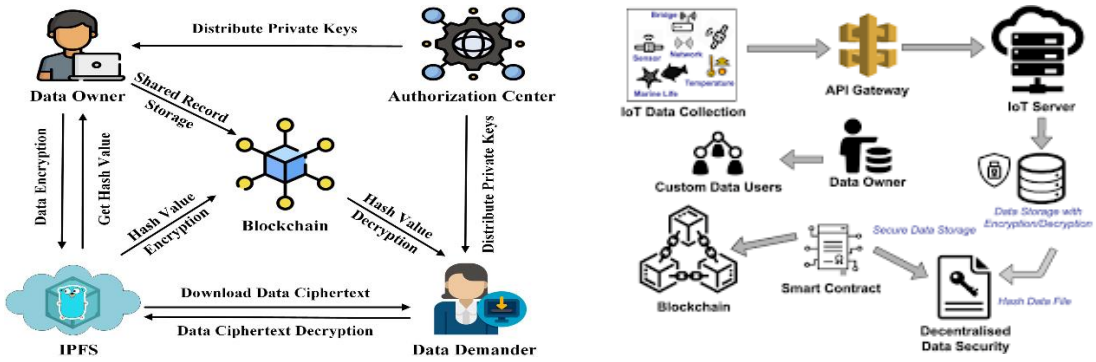


**Fig.2 – Process of block chain based data sharing**

## 7. Results and Discussion

### *7.1 Performance Evaluation*

The integration of block chain with cloud data-sharing enhanced security as well as efficiency. The key performance indicators are:

- Access Control Effectiveness: Smart contracts enable automated and precise access control, minimizing the possibility of human error.
- Block chain's unchangeable ledger prevents data inputted from being tampered with without agreement, further enhancing confidence in its validity.
- Latency Factors: Block chain introduces latency due to consensus mechanisms, but off-chain processing and algorithmic optimization have minimized this effect.

### *7.2 Security Enhancements*

The proposed system addresses certain security problems that exist in traditional cloud computing:

- Decentralization: By dispersing information across a network of block-chains, the system avoids single points of failure, thereby increasing resistance to potential attacks.
- Transparency and Auditability: All the transactions are logged on the block chain, thereby establishing an open and tamper-evident audit trail that enhances compliance and accountability.
- Improved Privacy: Because of encryption and access control, sensitive information are safe guarded so that only approved groups can see particular information.

### *7.3 Comparative Analysis*

A comparison of classical models of cloud data sharing with the block chain-integrated model identifies:

- Security: Block chain integration greatly improves data security with unalterable records and decentralised control.
- Scalability: Even though older systems are more scalable, ongoing research into block chain scalability technologies such as sharding and layer-2 protocols is promising.
- Cost Impacts: The upfront cost of implementing block chain systems can be expensive, but the cost benefits in the end are reduced data breach and compliance violation expenses.

### *7.4 Practical Implications*

Safe exchange of information through the utilization of block chain technology in cloud platforms has real-world application in numerous industries:

- ✓ Healthcare: Secure sharing of patient records among trusted providers without infringing on patient privacy.
- ✓ Finance: Secure, readable transaction histories to facilitate auditing and regulatory compliance.
- ✓ Government Services: Effective sharing of data among agencies to enable service delivery, and policy performance.

## 8. Conclusion

This research has examined the union of block chain technology and cloud computing to ensure safe data sharing. Leveraging the distributed and unalterable ledger of block chain, the suggested framework addresses major security issues inherent in traditional cloud systems, i.e., unauthorized access, leakage of data, and transparency.

The use of smart contracts within this model enhances automated and enforceable access policies to guarantee rule-compliant information sharing and safe access. Use of cryptographic mechanisms also enhances the integrity and confidentiality of data and enhances users' trust in cloud services.

Our analysis proves that the incorporation of block chain within cloud infrastructures not only addresses the security issues that currently persist but also brings new paradigms for data governance and user control. The incorporation is not, however, without its challenges. Scalability, interoperability with legacy systems, and the necessity for standardized protocols are all topics of active research.

Future research needs to focus on developing consensus protocols for increased volume of transactions, developing hybrid platforms integrating on-chain and off-chain storage mechanisms, and developing regulatory frameworks that influence the ethical use of block chain technology in cloud computing.

Overall, the union of block chain and cloud computing is a promising avenue toward securing data sharing activity. Even with problems, the potential benefits to security, transparency, and user control make such an union an appealing subject for future research and development.

## 9. REFERENCES

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

**2.** Wang, Z., & Guan, S. (2023). A blockchain-based traceable and secure data-sharing scheme. *PeerJ Computer Science*, 9, e1337. (peerj.com)

**3.** Xu, M., Liu, S., Yu, D., Cheng, X., Guo, S., & Yu, J. (2021). Cloud Chain: A Cloud Blockchain Using Shared Memory Consensus and RDMA. *arXiv preprint arXiv:2106.04122*. (arxiv.org)

**4.** Sengupta, J., Ruj, S., & Das Bit, S. (2023). FairShare: Blockchain Enabled Fair, Accountable, and Secure Data Sharing for Industrial IoT. *arXiv preprint arXiv:2301.09761*. (arxiv.org).

**5.** Patil, P. V., Tulsiani, P., & Mane, S. (2024). Mitigating Data Sharing in Public Cloud using Blockchain. *arXiv preprint arXiv:2404.16872*. (arxiv.org)