International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 2001-2006
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0292

Data Sharing in Cloud Environment through Blockchain and IPFS in Secure Manner

Mrs. S. Sri Sayelakshmi[1], Dr. R. G Suresh Kumar[2], M Harini[3], B Oviya[4]

[1]Assistant Professor, Department of CSE, Rajiv Gandhi College of Engineering and Technology, Puducherry, India.

[2]Head of the Department, Department of CSE, Rajiv Gandhi College of Engineering and Technology, Puducherry, India.

[3,4]UG Scholar, Department of CSE, Rajiv Gandhi College of Engineering and Technology, Puducherry, India.

Emails: *srisayelakshmi_s@rgcet.edu.in[1], sureshkumar_rg@rgcet.edu.in[2], harini.m0503@gmail.com[3], oviyabala31@gmail.com[4]*

Abstract

In modern cloud computing environments, data is often stored on cloud servers in the form of ciphertext to ensure security and confidentiality. Access to this encrypted data typically requires a third party to provide an access key to the consumer. However, the existing use of the SHA-256 encryption method has limitations, as it leaves the data vulnerable to tampering. To address this issue, a Proof of Stake (PoS) algorithm is proposed as a more secure alternative. In this approach, data is encrypted using a robust encryption algorithm, and all transactions are recorded on a blockchain using the PoS algorithm. This method not only enhances data security by making tampering more difficult but also ensures the integrity of transactions by securely storing them in blocks. The proposed system offers a more resilient and tamper-resistant solution for cloud data storage and access, managing sensitive information in the cloud. Additionally, it reduces dependency on third-party key providers, further minimizing security risks.

Keywords: *Cloud Security, Proof of Stake (PoS), Blockchain, Data Integrity, Encryption, Tamper-Resistant Storage.*

1. Introduction

With the rapid advancement of cloud computing, secure data sharing has emerged as a critical concern for individuals and businesses alike. Conventional cloud storage systems rely on centralized servers, which pose risks such as hacking, single points of failure, and internal misuse [1]. To tackle these security vulnerabilities, a blockchain-based hierarchical semi-decentralized model incorporating the InterPlanetary File System (IPFS) is introduced for secure and efficient data sharing. In this approach, blockchain acts as the backbone for managing access control, recording immutable permission logs, and preventing unauthorized modifications [2]. The hierarchical structure facilitates role-based access, making it well-suited for organizations with complex access needs [3]. Additionally, smart contracts automate access control, ensuring security and transparency while reducing dependency on third-party entities [4]. Meanwhile, IPFS decentralizes data storage by distributing files across a peer-to-peer (P2P) network. Data is hashed and divided into chunks, enhancing redundancy and making it tamper-resistant [5]. Instead of storing entire files on the blockchain, only their corresponding content hashes are recorded, ensuring efficient storage and faster retrieval [6]. This hybrid semi-decentralized approach balances security with performance. Unlike fully decentralized systems, which may face latency issues, this method enables designated nodes to manage access while maintaining distributed storage. By combining blockchain transparency and IPFS's decentralized framework, this system ensures a

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 2001-2006
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0292

scalable, efficient, and secure solution for modern cloud-based data sharing.

2. Literature Overview

Elias Ribeiro da Silva, Jacob Lohmer, Michelle Rohla, Jannis Angelis [1] explored how blockchain and data sharing enhance circularity in the electric vehicle (EV) battery supply chain by ensuring transparency and traceability. A blockchain-based immutable ledger records the lifecycle of a battery, enabling stakeholders to verify sustainability and regulatory compliance. This technology supports second-life applications by identifying batteries suitable for reuse or recycling. Blockchain fosters responsible recycling and resource optimization, leading to sustainable innovation and better collaboration among manufacturers and recyclers. Smita Athanere, Ramesh Thakur [2] proposed a blockchain-based decentralized system utilizing IPFS (InterPlanetary File System) to enhance data security in data transfers. Centralized storage models are vulnerable to cyberattacks due to their reliance on single-point data storage. By integrating IPFS with blockchain, this approach divides data into hash codes stored across a distributed network, significantly reducing security risks. The system employs data encryption and a two-level key management strategy to ensure confidentiality and restrict unauthorized access. The immutability of blockchain, combined with encryption, creates a secure environment for data sharing and minimizes breach risks. Pierpaolo Loreti, Lorenzo Bracciale, Emanuele Raso [3] introduced a blockchain-powered smart grid architecture that integrates Secure Multiparty Computation (SMC) and Verifiable Secret Sharing (VSS). SMC allows encrypted computations without revealing private data, while VSS enhances security by splitting encrypted data across multiple channels. This ensures privacy, transparency, and accountability in energy data management. Additionally, their multi-channel blockchain structure enhances efficiency for IoT-based smart grids by segmenting transactions, thereby reducing processing loads while maintaining smart contract functionality. This scalable, secure design ensures decentralized energy management, data integrity, and privacy protection, making it ideal for real-world smartgrid applications. Chaitanya Singh, Deepika Chauhan, Sushama A. Deshmukh, Swati Sudhakar Vishnu, Ranjan Walia [4] Chaitanya Singh, Deepika Chauhan, Sushama A. Deshmukh, Swati Sudhakar Vishnu, Ranjan Walia [4] developed Medi-Block, a blockchain-based system designed for secure medical record sharing while ensuring data privacy and accessibility. The system employs bilinear mapping for authentication, eliminating the need for third-party trust authorities. Medi-Block embeds identity management within the blockchain, reducing single-point vulnerabilities and protecting patient identities. By removing intermediaries, Medi-Block improves communication time, reduces operational costs, and enhances security, offering a cost-effective solution for efficient healthcare data management. Yixian Zhang, Feng Zhao [5] introduced ECA_MDSS (Efficient Consensus Algorithm for Medical Data Storage and Sharing) to address scalability, delay, and throughput challenges in large-scale medical data networks. Their master-slave multi-chain architecture with geographic clustering enhances efficiency and minimizes transmission delays. The system utilizes aggregation signatures to compress transaction data, improving throughput. Ring signatures ensure privacy by anonymizing primary nodes involved in transactions. ECA_MDSS reduces communication overhead, accelerates consensus, and enhances scalability, making it a secure and efficient solution for medical data sharing in modern healthcare environments. Pengyong Cao, Guijang Duan, Jianping Tu, Qimei Jiang, Xianggui Yang, and Chen Li [6] introduced a blockchain-based platform for enhancing data sharing and trust within aviation supply chains. The system addresses challenges like data silos by securely linking quality data across suppliers through a tamper-proof blockchain ledger, ensuring transparency and traceability. Their platform also integrates a real-time supplier assessment model to evaluate quality and support decision-making. This solution enables efficient and secure collaboration across the aviation industry, improving product quality management and fostering scalable, hierarchical data sharing across distributed stakeholders

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 2001-2006
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0292

3. Methodologies and Approaches

The literature on blockchain-based data access control in diverse sectors such as smart grids, aviation, big data, and healthcare—employs a variety of methodologies to collect, analyze, and validate data. Below are the primary methodologies and approaches used in the studies, emphasizing how researchers collect empirical data, test system performance, and verify the effectiveness of their proposed models.

3.1. Architectural Design and Cryptographic Integration

Authors in smart grid and healthcare applications have integrated cryptographic tools such as Secure Multiparty Computation, Verifiable Secret Sharing, and Ring Signatures into blockchain architecture to create privacy-preserving systems. In the study "Privacy and Transparency in Blockchain-Based Smart Grid Operations" by Pierpaolo Loreti et al. [3], a multi-channel blockchain architecture was designed, incorporating cryptographic methods to secure data collection from IoT devices. This ensures that energy data remains private and accessible only to authorized entities through smart contracts. The study focused on testing the cryptographic protocols in low-performance IoT environments to validate their feasibility, aiming to achieve secure and optimized smart grid data access.

3.2. Smart Contracts and Real-Time Data Sharing Mechanisms

Smart contracts are widely used across different sectors to automate and control data access, allowing for real-time data sharing between entities such as suppliers, hospitals, and medical practitioners. In the study "Blockchain-Based Process Quality Data Sharing Platform for Aviation Suppliers" by Pengyong Cao et al. [6], the authors utilized blockchain smart contracts for real-time quality data sharing. The model was designed to enable secure data exchange and supplier assessment, addressing challenges like data silos in the aviation industry. The study assessed the platform's data-sharing efficiency and security through simulations, analyzing the impact on data credibility and interactions within the supply chain.

3.3. Consensus Algorithms and Blockchain Protocol Enhancements

To improve data storage scalability and reduce latency, some studies introduced new consensus algorithms and optimized protocols that handle high-throughput data in distributed environments. In "A Secure Big Data Storage Framework Based on Blockchain Consensus Mechanism with Flexible Finality" by Sasikumar et al. [7], the authors utilized the Highway protocol to enhance scalability and allow faster block finality. The framework enables secure big data storage in environments requiring high data throughput. The study measured data processing times, energy consumption, and data request hit ratios, showing that the Highway protocol could improve both security and processing efficiency.

3.4. Prototyping and Simulation in Controlled Environments

Researchers use simulations or prototype systems to test the viability of blockchain solutions in managing data access and controlling latency, storage, and communication costs, enabling evaluation under realistic conditions. In "Medi-Block Record: Secure Data Sharing Using Blockchain Technology" by Chaitanya Singh et al. [4], the authors tested their Medi-Block framework for medical data sharing using a simulated blockchain environment. Bilinear mapping-based authentication was applied to evaluate the system’s tamper-proof and anonymous identity management capabilities. Data collection focused on the system's authentication time and communication cost metrics, with simulation results showing improved privacy and lower transmission costs compared to baseline models.

3.5. Benchmarking with Traditional and Blockchain-Based Models

Researchers often compare the proposed blockchain models against traditional centralized systems to measure improvements in latency, data security, scalability, and processing speed. In "Consensus Algorithm for Medical Data Storage and Sharing Based on Master-Slave Multi-Chain of Alliance Chain" by Yixian Zhang and Feng Zhao [5], the authors used benchmarking to demonstrate the efficiency of the ECA_MDSS consensus algorithm,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 2001-2006
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0292

which combines master-slave multi-chain architecture and aggregation signatures to optimize large-scale network performance.

3.6. Case Studies and Real-World Applications Methodology

Certain studies incorporated real-world case studies to illustrate blockchain's potential in specific industries and demonstrate the system's scalability and practicality. The study on blockchain integration in smart grids by Loreti et al. [3] represents a case study where the architecture was tailored to energy data sharing across IoT devices in a smart grid environment. The design accounted for privacy-preserving, verifiable, and transparent data sharing. Case study analysis included assessing system functionality in real-time data sharing across the network, using IoT devices as test subjects to evaluate performance, and analyzing the potential for scalability and optimization across the entire grid.

3.7. Blockchain for Supply Chain Circularity and Sustainability

Researchers have started leveraging blockchain not only for security and traceability but also for supporting circular economy principles, particularly in sectors like electric vehicle (EV) battery management. In the study by Elias Ribeiro da Silva et al. (2023), a blockchain-based data sharing framework was introduced to record each stage of an EV battery's lifecycle—from raw material sourcing to end-of-life disposal. This immutable ledger enhances traceability and regulatory compliance while promoting second-life applications for used batteries. The analysis focused on assessing blockchain's ability to provide verifiable battery health and composition data, enabling stakeholder collaboration in identifying reuse opportunities and reducing waste, thereby validating blockchain's potential for promoting sustainable practices in complex supply chains [6].

4. Findings and Trends

Over recent years, blockchain has emerged as a transformative solution for secure data sharing and decentralized access control across multiple industries. Through the integration of cryptographic tools, smart contracts, and innovative consensus mechanisms, blockchain enables secure, scalable, and efficient handling of sensitive data. The following sections highlight key findings and trends derived from current literature.

4.1. Integration of Cryptographic Methods for Enhanced Security

A key finding across sectors like healthcare and energy is the integration of cryptographic techniques—such as Secure Multiparty Computation, Ring Signatures, and Verifiable Secret Sharing—within blockchain frameworks. These tools ensure data privacy, integrity, and secure access in decentralized environments, minimizing the risk of unauthorized data exposure and enhancing trust among distributed stakeholders [3].

4.2. Smart Contracts for Automated and Real-Time Data Exchange

The use of smart contracts has emerged as a critical trend for facilitating secure, real-time data exchange across entities. These self-executing protocols reduce reliance on third parties, enforce predefined access rules, and enhance interoperability, especially in fields like aviation and healthcare, where secure collaboration is vital, They provide an automated, tamper-proof mechanism for controlling data flows across organizational boundaries [6].

4.3. Scalable Consensus Mechanisms to Support High-Throughput Applications

To address performance bottlenecks, researchers have introduced lightweight and flexible consensus algorithms such as the Highway Protocol and master-slave multi-chain designs. These advancements significantly improve processing speed and data throughput, enabling blockchain to support big data and IoT applications effectively, Such mechanisms help blockchain system adapt to high demand environment without compromising security [4],[5].

4.4. Simulation and Benchmarking for Practical Validation

Simulation-based testing and benchmarking against traditional systems are widely used to evaluate the efficiency and feasibility of proposed blockchain models. These controlled experiments help assess metrics like authentication time, communication cost, and energy efficiency, ensuring practical deployment readiness, This trend shows the important of prototyping to optimize blockchain system for real

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 2001-2006
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0292

world constraints [4].

4.5. Expanding Blockchain Applications Towards Sustainability and Circular Economy

Recent studies focus on blockchain's potential in promoting sustainable practices, particularly in the EV battery supply chain. By offering full lifecycle traceability, blockchain helps identify reuse opportunities and supports regulatory compliance, showcasing its role in circular economy models beyond traditional security use cases,This highlights blockchain's evolving utility in driving environmental responsibility and transparency across industries [1].

5. Challenges and Gaps

Despite ongoing advancements, blockchain systems still face key challenges. Issues like scalability, energy consumption, limited real-world use, and integration difficulties hinder widespread adoption. Balancing privacy with transparency and optimizing cryptographic efficiency remain ongoing concerns.

5.1. Scalability Limitations

Although improved consensus mechanisms like PBFT, PoS, and multi-chain models have emerged, blockchain networks still face scalability challenges in large-scale deployments. In data-intensive environments such as medical systems and IoT frameworks, increased transaction volumes can lead to performance bottlenecks including latency and decreased throughput. These limitations hinder blockchain's broader application in real-time, high-load scenarios [1], [2].

5.2. Energy Consumption

Even with recent advances in energy-efficient protocols, blockchain technology remains computationally demanding. High energy consumption associated with consensus processes such as Proof of Work (PoW) continues to be a significant barrier to sustainability, particularly in IoT and mobile environments where low power usage is essential. Ongoing research stresses the need for lightweight and green blockchain solutions [3], [4].

5.3. Limited Real-World Implementation

While many studies present promising prototypes and simulations, few blockchain systems have matured into real-world deployment. Implementation challenges arise from regulatory constraints, technical integration issues, and high operational costs. In critical sectors like healthcare and aviation, compliance with data standards and certification requirements further delays adoption [5], [6].

5.4. Interoperability Challenges

Integrating blockchain with existing legacy systems is still a major obstacle, especially in industries with established digital infrastructures. A lack of standardization and interoperability protocols restricts seamless data sharing across platforms. This integration gap limits blockchain's usability across heterogeneous environments [1], [7].

5.5. Privacy vs. Transparency Trade-off

Blockchain's immutability and transparency, while crucial for accountability, often conflict with privacy needs in sensitive data contexts such as smart grids and medical records. Achieving fine-grained control over what data is visible and to whom remains complex. Balancing transparency with strong privacy protections is an ongoing research gap [6], [8].

Conclusion

This survey has comprehensively explored the integration of blockchain technologies for secure and efficient data sharing across sectors such as healthcare, aviation, smart grids, and supply chain systems. By incorporating cryptographic techniques, smart contracts, and scalable consensus algorithms, recent research demonstrates blockchain's strong potential in enabling decentralized, tamper-resistant, and privacy-preserving data exchange. Simulation-based testing, real-time interoperability mechanisms, and applications in sustainability—such as electric vehicle battery management—further underscore blockchain's versatility in handling complex data-sharing requirements. Despite these advancements, key challenges persist, including limited scalability in high-throughput environments, energy inefficiencies, interoperability issues with legacy systems, and a lack of large-scale real-world deployments. Moreover, balancing transparency with privacy and ensuring lightweight cryptographic operations remain critical technical hurdles. Addressing these gaps will be essential for transitioning blockchain from proof-of-concept models to full-scale, industrial adoption. The insights from this survey reinforce

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 2001-2006
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0292

blockchain's transformative potential while emphasizing the need for continued innovation to overcome practical constraints in secure and scalable data-sharing ecosystems [9-15].

References

[1]. Elias Ribeiro da Silva, Jacob Lohmer, Michelle Rohla, and Jannis Angelis, Blockchain-enabled data sharing for circular economy: Opportunities and challenges, Journal of Cleaner Production, 2023.

[2]. Smita Athanere and Ramesh Thakur, A Comprehensive Review on Blockchain-Based Secure Storage Techniques in Cloud, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 2022.

[3]. Pierpaolo Loreti, Lorenzo Bracciale, Emanuele Raso, Giuseppe Bianchi, Eleonora Riva Sanseverino, and Pierluigi Gallo, Blockchain-based data access control for energy grids, Computers & Electrical Engineering, 2022.

[4]. [Chaitanya Singh, Deepika Chauhan, Sushama A. Deshmukh, Swati Sudhakar Vishnu, and Ranjan Walia, Blockchain-based secure healthcare framework for IoT and cloud integration, IEEE Access, 2023.

[5]. Yixian Zhang and Feng Zhao, Privacy-preserving data sharing with re-encryption for decentralized storage using blockchain, Future Generation Computer Systems, 2023.

[6]. Pengyong Cao, Guijiang Duan, Jianping Tu, Qimei Jiang, Xianggui Yang, and Chen Li, A tiered blockchain architecture for efficient and secure industrial data sharing, IEEE Access, 2023

[7]. Sasikumar, Logesh Ravi, Ketan Kotecha, Ajith Abraham, Alathi Devarajan, and Subramaniya Swamy Vaira Sundaram, Blockchain for secure smart grid management: A hybrid consensus approach, IEEE Transactions on Industrial Informatics, 2022.

[8]. Maximilian Wöhrer and Uwe Zdun, Smart Contracts: Security Patterns in the Ethereum Ecosystem and Solidity, IEEE IWBOSE, 2018.

[9]. Qiwu Zou, Yuzhe Tang, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, and Laurent Njilla, ChainFS: Blockchain-Secured Cloud Storage, IEEE CLOUD, 2018.

[10]. Fran Casino, Thomas K. Dasaklis, and Constantinos Patsakis, A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues, Elsevier, 2018.

[11]. R. Gowthami Saranya and A. Kousalya, A Comparative Analysis of Security Algorithms Using Cryptographic Techniques in Cloud Computing, IEEE, 2017.

[12]. Ilya Sukhodolskiy and Sergey Zapechnikov, A Blockchain-Based Access Control System for Cloud Storage, IEEE ElConRus, 2018.

[13]. Shubham Desai, Rahul Shelke, Omkar Deshmukh, Harish Choudhary, and S. S. Sambhare, Blockchain-Based Secure Data Storage and Access Control System Using Cloud, IEEE ICCUBEA, 2019.

[14]. Gurudatt Kulkarni, Rani Waghmare, Rajnikant Palwe, Vidya Waykule, Hemant Bankar, and Kundlik Koli, Cloud Storage Architecture, IEEE TSSA, 2012.

[15]. Iwendi C., Khan S., Anajemba J.H., Mittal M., Alenezi M., and Damasevicius R., Enhanced Secure Blockchain-Based Remote Patient Monitoring in IoT Devices Using Ensemble Deep Learning, Neural Computing and Applications, 2022.