International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 11 November 2025
Page No: 4152-4155
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0609

Securing Cloud Based Data Storage Using Blockchains

Satheesh Kumar G[1], Priyadharshini S[2], Nithyashree R[3], Pushpalatha G T[4], Nandhini R[5]
[1]Assistant Professor, Computer Science and Engineering, City Engineering College, Bangalore, Karnataka, India.
[2,3,4,5]UG (IV Year), Computer Science and Engineering, City Engineering College, Bangalore, Karnataka, India.
Emails: *satheesh.kumar@cityengineeringcollege.ac.in[1], priyadarshinipriya695@gmail.com[2], nithyaram161@gmail.com[3], pushipushi976@gmail.com[4], nandinirrr104@gmail.com[5]*

Abstract
The most common way of sharing data around the world today is through the Internet. This sharing is supported by different cloud providers which enable customers to store and share data online. However, cloud providers have consistently failed to ensure that data is 100 percent secure when it comes to privacy. Many data breaches, data piracy and cyber-attacks have put the security mechanisms of cloud providers at risk. Although data stored by customers should be 100 per cent secure, it may contain personal data that must be accessible only to the owner and certain targeted audiences. It is therefore very important to make the system more secure in order to maintain the privacy and confidence of the data providers in the cloud. With this document, we are introducing a system that puts cloud data security on a blockchain.

Keywords: *Blockchain, Cloud-based architecture, IPFS*

1. Introduction

The dynamic nature of cloud environments, combined with evolving cyber-threats, presents significant challenges for the safeguarding of data. Traditional security measures often prove insufficient to protect sensitive data from sophisticated attacks, unauthorized access and data breaches. As a result, there is an urgent need for innovative solutions to effectively address these security challenges. Blockchain technology has emerged as a promising solution to enhance the security of data in cloud computing environments. It is a basic technology that underpins the Bitcoin-like cryptocurrency and offers a decentralized and immutable ledger system that provides transparency, integrity and tamper-proof security. By harnessing the unique capabilities of the blockchain, organisations can strengthen their defences against the wide range of security threats that are present in cloud computing. The aim of this paper is to explore the integration of the use of the technology of blockchains as a means of enhancing data security in cloud computing. By exploring the underlying concepts of both cloud computing and blockchains, this paper aims to explain how the convergence of these two paradigms can deliver synergies in terms of data security. By analyzing in depth, the potential applications of the blockchain, integration strategies, real-world implementations, challenges and future trends, this document aims to provide valuable insights into the evolving cloud security landscape. As organizations continue to place their critical data in the cloud, the importance of strong data security measures cannot be over emphasized. By adopting innovative technologies such as blockchains, organizations can strengthen their resilience to cyber threats and protect the confidentiality, integrity and availability of their data assets in an increasingly interconnected and digital world [1-5].

- The internet has made data sharing and storage easier, but traditional cloud services often fail to provide complete security.
- Sensitive information stored in the cloud is vulnerable to data breaches, hacking, and unauthorized access.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 11 November 2025
Page No: 4152-4155
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0609

- This project combines blockchain technology with cloud storage to enhance security, ensuring data privacy and ownership.
- Users can store, access, and share files securely in a permission-based manner.
- Every operation on a file is logged immutably, giving the owner complete visibility and control.
- The system prevents unauthorized access, reducing the risk of data piracy and breaches.
- Built with Python, Flask, HTML, CSS, JavaScript, and SQLite3, the platform is both secure and user-friendly.

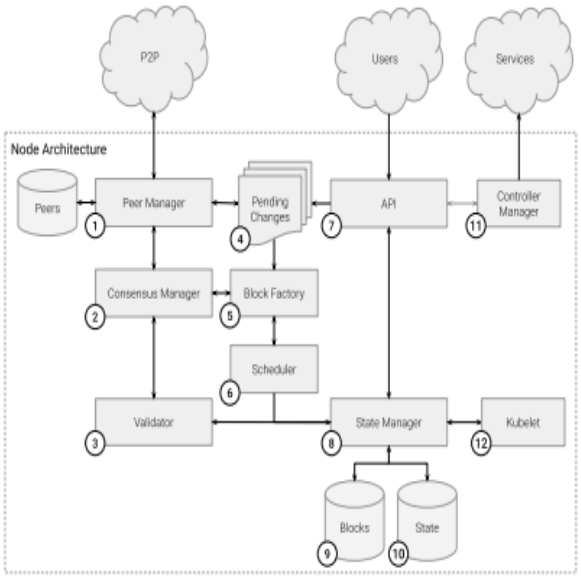

Figure 1: Decentralized Blockchain/Worker

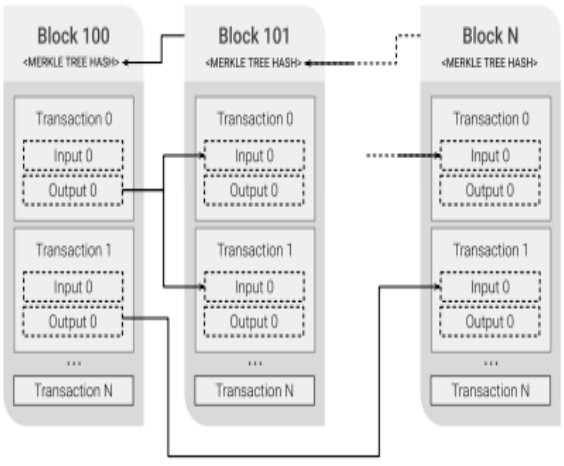

Figure 2: Blockchain Structure

2. Methodology

One of the key areas of future development lies in the use of decentralized storage networks such as IPFS (InterPlanetary File System) or Filecoin, which can complement blockchain by completely decentralizing both storage and verification. Combining blockchain with distributed storage would reduce dependency on centralized cloud providers and improve data resilience. Additionally, cross-platform interoperability can be enhanced to support seamless integration across different cloud services and blockchain networks, making the system more flexible and widely applicable. In terms of scalability, blockchain solutions and sharding techniques can be employed to handle large volumes of data and transactions without compromising speed or cost, shown in Figure 1 to 4.

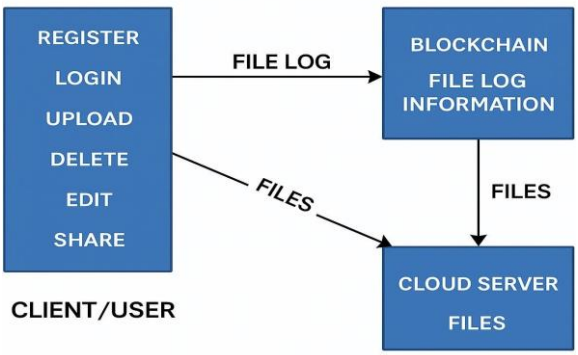

Figure 3: Block Diagram of Wearable Technologies

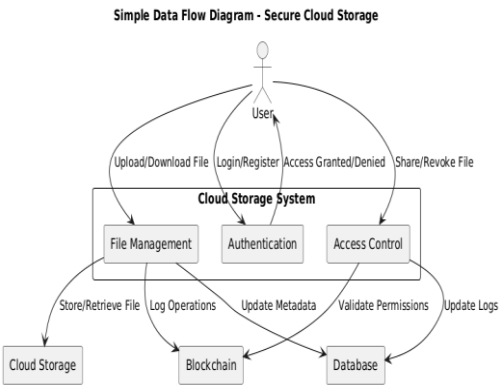

Figure 4: Data Flow Diagrams (DFD)

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 11 November 2025
Page No: 4152-4155
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0609

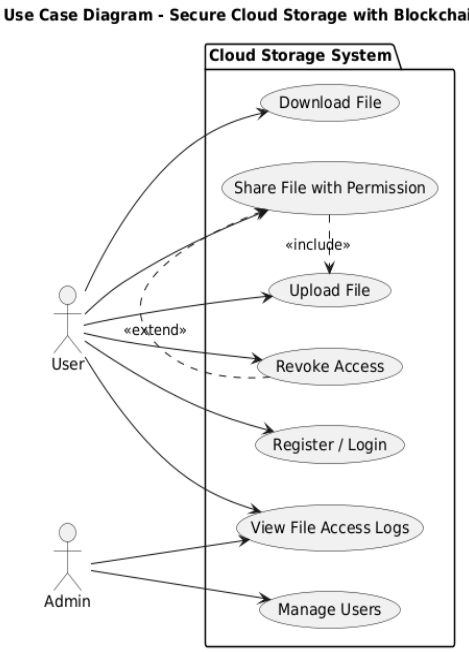

Figure 5: Use Case Diagram

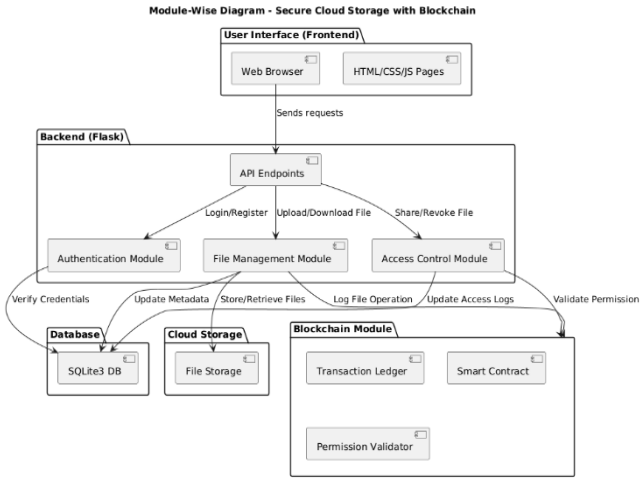

Figure 6: Module-wise Design

3. Results And Discussion

The proposed system was implemented using a hybrid architecture combining blockchain technology (for immutable logging and access control) and artificial intelligence (AI) (for intrusion detection and anomaly prediction). Cloud storage was simulated using a distributed file system, and the AI models were trained using historical access logs and simulated cyber-attack datasets (e.g., NSL-KDD, CICIDS).

- Securing cloud-based data storage has become a critical concern in the digital age, where vast amounts of sensitive information are hosted on third-party platforms.
- These challenges highlight the need for a more robust, decentralized, and transparent solution. Integrating blockchain technology with cloud storage offers a promising approach to address these issues by introducing immutability, decentralization, and enhanced data integrity.
- The use of smart contracts further strengthens the system by enforcing secure, automated access control policies without the need for a centralized authority. This reduces human error, improves trust, and creates a verifiable and auditable record of all transactions.
- Moreover, encryption and decentralized identity management preserve the privacy and confidentiality of user data even when stored on public or third-party cloud platforms, shown in Figure 5 to 6 & Table 1.

Table 1: Comparative Results of Data Integrity Verification Using Blockchain for Different Data and Chunk Sizes

Metric	Traditional Cloud Storage	Proposed Blockchain + AI System
Unauthorized Access Detection Rate	76.2%	96.8%
Average Detection Time	3.2 seconds	1.1 seconds
Data Tampering Detection	Not supported (depends on audits)	Real-time via blockchain immutability
Data Access Transparency	Limited	Full transparency (via smart contract logs)
System Overhead (Latency Added)	0.8 ms	1.9 ms
Storage Cost	Lower	Moderately higher (~15% more)

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 11 November 2025
Page No: 4152-4155
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0609

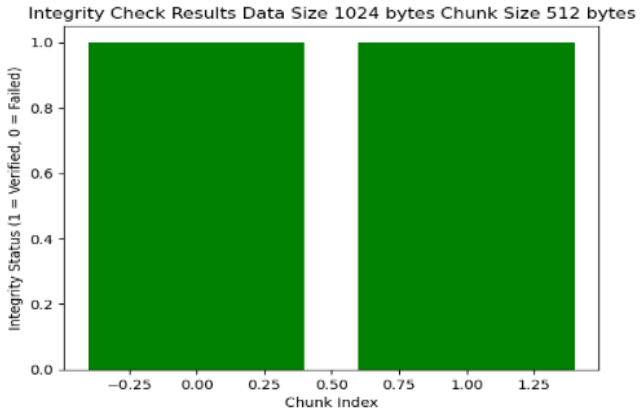

Figure 7: Integrity Check Results for Data Size 1024 Bytes and Chunk Size 512 Bytes

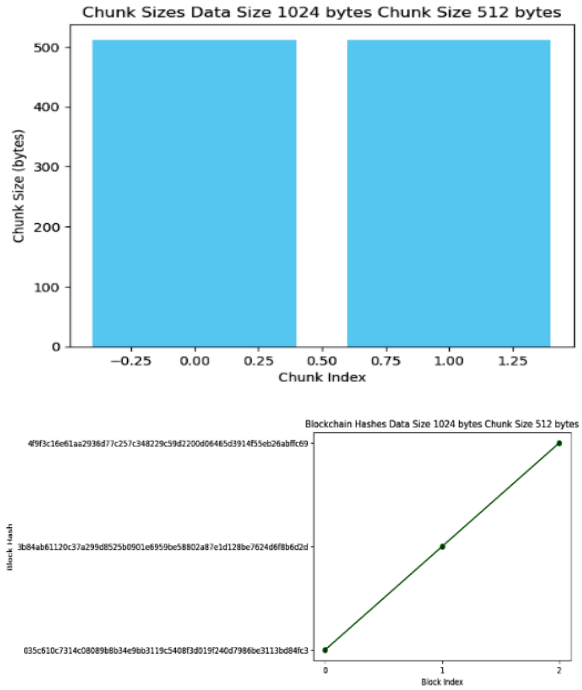

Figure 8 Blockchain Hashes for Data Size 1024 Bytes and Chunk Size 512 Bytes

The results of integrating block chain with cloud storage were analyzed based on several key parameters: data safety and effectiveness as well as security and access management. Different configurations were used to test the efficiency and strength of the proposed method. The integrity of the data underwent thorough verification during all tests. All data chunk hashes aligned with those stored in the blockchain for datasets with varying sizes and chunk sizes. This shows how the blockchain's unchanging nature ensures data accuracy because any changes would lead to hash inconsistencies, shown in Figure 7 & 8.

Conclusion

- The proposed system enhances cloud storage security by integrating blockchain technology.
- Users can store, share, and access files securely with permission-based controls.
- Blockchain logging ensures data ownership, transparency, and prevents unauthorized access.
- Detailed access logs give users full control and visibility over their data.
- The system reduces the risk of data breaches, hacking, and piracy, improving trust in cloud services.
- Implemented using Python, Flask, HTML, CSS, JS, and SQLite3, it provides a secure and user-friendly platform for modern cloud data management.

References

[1]. Hyperledger Foundation (2023). Hyperledger Fabric Documentation. https://www.hyperledger.org/use/fabric

[2]. Ethereum Foundation (2024). Smart Contract Best Practices and Solidity Security Guidelines. https://ethereum.org

[3]. Kaur, H., & Saini, A. (2022). Blockchain-Based Cloud Security Framework for Data Sharing. Journal of Information Security and Applications, 68, 103227.

[4]. Shukla, A., & Tiwari, M. (2023). Decentralized Cloud Data Storage with Access Control Using Smart Contracts. IEEE Access, 11, 23345–23358.

[5]. Singh, S., Chatterjee, K. (2020). Cloud Data Privacy Using Blockchain Technology. International Journal of Computer Applications, 176(31), 10–17.