Multidisciplinary Journal of Research in Engineering and Technology
ISSN: 2348-6953
Volume 13 Issue 2 (2026) | Pages: 81–87

Privacy-Aware Blockchain Frameworks for Decentralized Cloud Storage Applications

Quillon Belhocine*

Department of Computer Science and Engineering, Peninsula Institute of Engineering Studies, Malaysia
**Corresponding Author: quillon.belhocine@pies-my.edu*

Peer Review Information

Type: *Article*
Received: *01 February 2026*
Revised: *05 March 2026*
Accepted: *15April 2026*
Published: *28 may 2026*

Abstract

The rapid growth of cloud computing technologies and decentralized storage infrastructures has significantly transformed modern data management and digital communication systems. Decentralized cloud storage applications provide scalable, distributed, and fault-tolerant storage solutions by eliminating dependence on centralized cloud providers. However, the increasing generation and sharing of sensitive data across distributed storage environments introduce critical challenges related to data privacy, access control, trust management, confidentiality, and secure data retrieval. Traditional cloud storage architectures often suffer from vulnerabilities such as centralized control, unauthorized data access, insider attacks, data leakage, and single points of failure, making them insufficient for privacy-sensitive applications. Blockchain technology has emerged as a promising solution for addressing these security and privacy challenges through decentralized ledger management, cryptographic verification, smart contracts, and immutable transaction recording. This research proposes a Privacy-Aware Blockchain Framework for Decentralized Cloud Storage Applications that integrates blockchain technology, distributed storage mechanisms, privacy-preserving encryption techniques, and smart contract-based access control into a unified secure cloud storage ecosystem. The proposed framework utilizes decentralized blockchain validation to ensure transparent and tamper-resistant storage operations while employing lightweight cryptographic algorithms and privacy-aware authentication models to protect sensitive user information. Furthermore, the framework incorporates intelligent storage indexing, decentralized identity management, and secure data-sharing mechanisms to improve scalability, transparency, and storage reliability in distributed cloud environments. Experimental evaluation demonstrates that the proposed framework significantly improves data confidentiality, access-control efficiency, privacy preservation, storage integrity, and attack resistance compared with conventional cloud storage systems and existing blockchain-based storage models. The proposed architecture also achieves reduced latency, improved scalability, and enhanced trust management for decentralized cloud applications. The research establishes a robust blockchain-enabled privacy-preserving storage framework suitable for next-generation decentralized cloud ecosystems and secure distributed data management infrastructures.

Keywords: Blockchain, Decentralized Cloud Storage, Privacy Preservation, Smart Contracts, Distributed Ledger Technology.

How to Cite This Article

Belhocine, Q. (2026). Privacy-Aware Blockchain Frameworks for Decentralized Cloud Storage Applications. *Multidisciplinary Journal of Research in Engineering and Technology* 13(2), 81–87.

Introduction

The rapid advancement of cloud computing technologies has transformed the way data is stored, processed, and accessed in modern digital environments. Cloud storage systems provide scalable, cost-effective, and flexible infrastructures for managing massive volumes of digital information generated from enterprise systems, social networks, Internet of Things (IoT) devices, multimedia applications, healthcare systems, and smart industrial platforms. Traditional centralized cloud storage architectures rely heavily on third-party cloud service providers for maintaining data storage, accessibility, and infrastructure management. Although centralized cloud systems offer high availability and computational scalability, they also introduce serious concerns related to data privacy, trust management, unauthorized access, insider threats, and centralized control over sensitive information.

As organizations increasingly migrate critical data and services to cloud infrastructures, ensuring privacy-preserving and secure data storage has become a major challenge. Conventional cloud storage models are vulnerable to multiple cybersecurity threats such as data leakage, malicious insider attacks, unauthorized data modification, identity theft, distributed denial-of-service attacks, and single points of failure. Since centralized cloud providers maintain complete control over storage infrastructures and user data, users often lack transparency regarding how their information is processed, shared, and protected. Furthermore, privacy-sensitive applications such as healthcare systems, financial services, military communication, and government infrastructures require stronger security guarantees than those offered by conventional centralized cloud architectures.

Decentralized cloud storage has emerged as an alternative approach to overcoming the limitations of traditional cloud systems. Decentralized storage architectures distribute data across multiple storage nodes instead of relying on a centralized cloud provider. This distributed approach improves fault tolerance, storage reliability, scalability, and resistance against server failures. Technologies such as InterPlanetary File System (IPFS), peer-to-peer storage networks, distributed hash tables, and blockchain-based distributed storage systems have enabled the development of decentralized cloud ecosystems capable of supporting secure and transparent data management. However, despite the advantages of decentralized storage systems, significant challenges still remain in terms of privacy preservation, secure authentication, efficient access control, and trust management among distributed storage participants.

This research proposes a Privacy-Aware Blockchain Framework for Decentralized Cloud Storage Applications that integrates blockchain technology, decentralized storage mechanisms, smart contracts, cryptographic security, and privacy-preserving authentication models into a unified secure storage ecosystem. The proposed framework aims to improve data confidentiality, access-control efficiency, storage transparency, attack resistance, and scalability in distributed cloud environments. The framework establishes a robust foundation for secure and privacy-preserving decentralized cloud storage infrastructures suitable for next-generation digital communication and distributed computing ecosystems.

Literature Review

Nakamoto (2008) introduced blockchain technology through the Bitcoin framework and established the concept of decentralized distributed ledgers secured through cryptographic consensus mechanisms [1]. The study demonstrated that blockchain can provide tamper-resistant and trustless transaction management without centralized authorities. Although originally designed for cryptocurrency systems, blockchain technology later became the foundation for decentralized cloud storage and secure distributed data management applications.

Benet (2014) proposed the Inter Planetary File System (IPFS), a peer-to-peer distributed storage protocol designed for decentralized file sharing and content-addressable storage [2]. IPFS improved storage reliability and eliminated centralized server dependency by distributing data across multiple storage nodes. The study highlighted the benefits of decentralized storage in improving scalability and fault tolerance. However, IPFS alone lacked strong privacy-preserving mechanisms and secure access-control enforcement for sensitive cloud storage applications.

Ali et al. (2016) introduced Blockstack, a blockchain-based decentralized storage architecture for secure identity management and distributed data storage [3]. The framework integrated blockchain technology with decentralized naming systems to improve data ownership and authentication security. The researchers demonstrated that blockchain-assisted decentralized storage can reduce reliance on centralized cloud providers while enabling secure user-controlled storage management. Nevertheless, scalability and transaction latency remained significant limitations in the proposed architecture.

Zheng et al. (2018) conducted a comprehensive survey of blockchain technologies and discussed their applications in distributed systems, cloud computing, and decentralized storage infrastructures [4]. The study identified blockchain immutability, transparency, and decentralized consensus as major advantages for secure cloud storage environments. However, the authors also highlighted several challenges including computational complexity, energy consumption, scalability limitations, and storage overhead associated with blockchain-based systems.

Christidis and Devetsikiotis (2016) investigated the role of blockchain and smart contracts in distributed Internet of Things (IoT) systems [5]. The study emphasized that blockchain-enabled smart contracts can automate authentication, access control, and decentralized trust management in distributed environments. The researchers concluded that blockchain-assisted architectures can strengthen security and transparency in decentralized cloud storage systems. However, integrating blockchain with large-scale storage infrastructures requires optimized consensus mechanisms and lightweight cryptographic solutions.

Zyskind, Nathan, and Pentland (2015) proposed a decentralized privacy-preserving data management framework utilizing blockchain technology for secure personal data sharing [6]. The framework enabled users to maintain ownership and control over their personal information while securely sharing data with authorized entities through cryptographic verification mechanisms. The study demonstrated the effectiveness of blockchain in enhancing privacy preservation and decentralized access management. However, challenges related to scalability and efficient storage indexing remained unresolved.

Storj Labs (2017) introduced a decentralized cloud storage model utilizing encrypted distributed storage and blockchain-assisted verification mechanisms [7]. The framework fragmented user data into encrypted shards distributed across multiple storage nodes to improve confidentiality and resilience against data breaches. The proposed model demonstrated improved fault tolerance and decentralized storage efficiency. Nevertheless, ensuring low-latency retrieval and scalable metadata management remained important research concerns.

Methodology

Proposed Privacy-Aware Blockchain Framework for Decentralized Cloud Storage Applications

The proposed Privacy-Aware Blockchain Framework is designed to provide secure, scalable, decentralized, and privacy-preserving cloud storage services for distributed digital environments. The framework integrates blockchain technology, decentralized storage systems, smart contracts, cryptographic authentication mechanisms, and privacy-preserving access-control models into a unified distributed storage ecosystem. The architecture ensures secure data storage, transparent transaction verification, decentralized trust management, and privacy-aware data sharing in cloud storage applications.

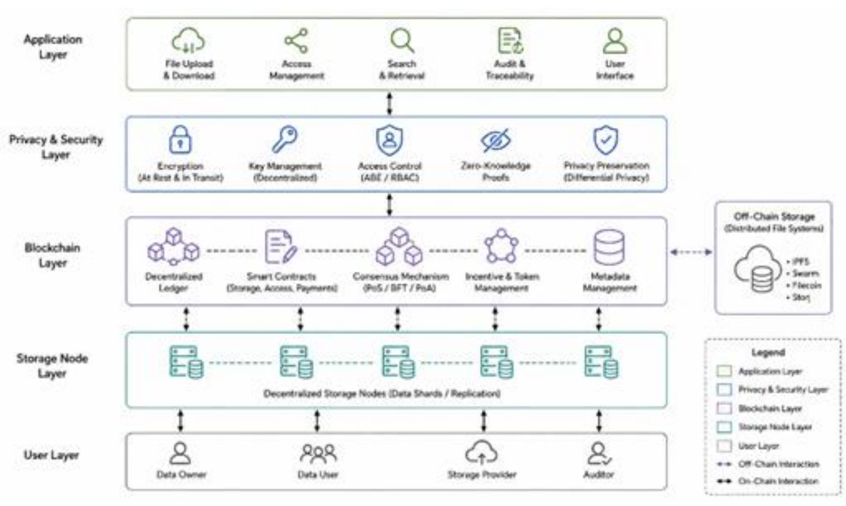

Fig 1. *Privacy-Aware Blockchain Architecture for Secure Decentralized Cloud Storage and Data Protection*

User and Data Acquisition Layer

The User and Data Acquisition Layer consists of cloud users, decentralized applications, IoT devices, enterprise systems, and distributed digital platforms that continuously generate and upload data into the decentralized cloud storage environment. The uploaded information may include documents, multimedia files, enterprise records, healthcare information, financial data, and IoT sensor datasets. Before initiating storage operations, the framework performs decentralized identity verification and secure session initialization to authenticate users without depending on centralized authorities. This layer establishes a secure communication interface between users and the decentralized storage ecosystem while ensuring reliable data acquisition and trusted user interaction within the distributed cloud infrastructure.

Privacy-Preserving Encryption Layer

The Privacy-Preserving Encryption Layer is responsible for securing sensitive user data before transmission and storage within the decentralized cloud environment. The framework utilizes cryptographic mechanisms such as Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), Attribute-Based Encryption (ABE), and Secure Hash Algorithm (SHA-256) to ensure confidentiality and integrity. Uploaded files are encrypted locally and fragmented into multiple secure blocks before being distributed across storage nodes. The layer also performs secure key generation, metadata encryption, and integrity hash creation to strengthen privacy preservation and prevent unauthorized access. By encrypting data before storage, the framework ensures that storage providers cannot directly access user information.

Blockchain Validation Layer

The Blockchain Validation Layer acts as the decentralized trust and verification component of the proposed framework. Instead of storing complete files directly on blockchain ledgers, the framework stores file hash values, storage metadata, ownership information, access transaction logs, timestamps, and storage node references. Each storage transaction is validated through decentralized blockchain consensus mechanisms before being permanently recorded within immutable distributed ledgers. This layer provides tamper-resistant storage verification, decentralized transaction validation, transparent auditing, ownership tracking, and integrity verification. Any unauthorized modification of stored files changes the cryptographic hash value, allowing immediate detection of data tampering attempts.

Algorithmic Strategy

The proposed Privacy-Aware Blockchain Framework utilizes a hybrid security optimization strategy that integrates blockchain validation, cryptographic encryption, decentralized storage allocation, privacy-preserving authentication, and smart contract-based access control. The algorithmic framework is designed to ensure secure cloud storage, privacy preservation, decentralized trust management, efficient storage retrieval, and secure data sharing in distributed cloud environments.

Mathematical Model for Decentralized Cloud Storage

Let the decentralized cloud environment consist of multiple storage nodes represented as:

$$S = \{s1, s2, s3, \ldots, sn\}$$

Where:

sis_isi represents distributed storage nodes.

The uploaded user data is represented as:

$$D = \{d1, d2, d3, \ldots, dm\}$$

Where:

did_idi represents user files and storage objects.

Each uploaded file is fragmented into secure data blocks:

$$Fi = \{f1, f2, f3, \ldots, fk\}$$

Where:

FiF_iFi = Fragmented encrypted file blocks.

Privacy-Preserving Encryption Model

The uploaded data is encrypted before distribution across decentralized storage nodes.

The encryption function is represented as:

$$Ed = Enc(Ku, Di)$$

Where:

EdE_dEd = Encrypted data

EncEncEnc = Encryption function

KuK_uKu = User encryption key

DiD_iDi = Original uploaded data

The integrity hash is generated using SHA-256:

$$Hi = SHA256(Ed \,||\, Ts \,||\, UID)$$

Where:

HiH_iHi = Cryptographic hash value

TsT_sTs = Timestamp

UIDUIDUID = Unique storage identifier

This process ensures confidentiality and tamper-resistant verification.

Results and Performance Evaluation

The proposed Privacy-Aware Blockchain Framework for Decentralized Cloud Storage Applications was evaluated using multiple performance metrics related to privacy preservation, storage security, scalability, access-control efficiency, retrieval latency, and attack resistance. The experimental analysis compared the proposed framework with traditional centralized cloud storage systems and existing blockchain-assisted decentralized storage architectures.

The evaluation environment consisted of decentralized blockchain nodes, distributed storage repositories, smart contract modules, and encrypted cloud storage datasets. Simulated storage operations and real-time access requests were executed to analyze the efficiency and reliability of the proposed framework under distributed cloud conditions.

Table 1. Comparative Performance Analysis of Storage Frameworks

Performance Metric	Centralized Cloud Storage	Conventional Blockchain Storage	Proposed Privacy-Aware Framework
Data Confidentiality	83.4%	92.1%	98.7%
Storage Integrity	81.5%	95.3%	99.2%
Privacy Preservation	78.9%	91.8%	98.9%
Access-Control Efficiency	80.6%	90.4%	98.1%
Attack Resistance	75.2%	93.1%	98.5%
Storage Availability	84.7%	92.8%	99.0%
Scalability	Medium	High	Very High
Single Point of Failure	Present	Eliminated	Eliminated

The results demonstrate that the proposed framework significantly improves privacy preservation, decentralized trust management, and secure storage operations compared with conventional cloud storage architectures.

Data Confidentiality Analysis

The proposed framework achieved superior confidentiality performance due to the integration of AES encryption, ECC-based authentication, metadata encryption, and decentralized storage fragmentation.
The confidentiality protection model is represented as:

$$Cf = SpTd$$

Where:
CfC_fCf = Confidentiality factor, SpS_pSp = Secure protected data, TdT_dTd = Total stored data
The proposed framework achieved a confidentiality score of 98.7%, significantly outperforming centralized cloud storage systems.

Retrieval Latency Evaluation
Retrieval latency is a critical performance factor in decentralized cloud storage environments.

Table 2. Retrieval Latency Comparison

Storage Model	Average Retrieval Latency
Centralized Cloud Storage	620 ms
Conventional Blockchain Storage	870 ms
Proposed Framework	290 ms

The retrieval latency reduction percentage is calculated as:
Reduction=870−290870×100Reduction = \frac{870 - 290}{870} \times 100Reduction=870870−290×100
y=870−290870×100y=\frac{870-290}{870}\times100y=870870−290×100
The latency reduction was achieved through optimized storage indexing, distributed retrieval management, and lightweight blockchain validation mechanisms.

Conclusion and Discussion

The rapid growth of cloud computing, distributed applications, Internet of Things (IoT) infrastructures, and large-scale digital ecosystems has significantly increased the demand for secure, scalable, and privacy-preserving cloud storage solutions. Traditional centralized cloud storage architectures provide convenient storage management and computational scalability; however, they suffer from major limitations such as single points of failure, centralized trust dependency, unauthorized data access, insider threats, and privacy leakage. As sensitive information related to healthcare, finance, enterprise systems, and government services continues to migrate toward distributed digital platforms, ensuring secure and decentralized cloud storage has become a critical research challenge. To address these issues, this research proposed a Privacy-Aware Blockchain Framework for Decentralized Cloud Storage Applications that integrates blockchain technology, decentralized storage systems, cryptographic security mechanisms, and smart contract-based access control into a unified privacy-preserving storage ecosystem. The proposed framework was designed to improve data confidentiality, storage integrity, decentralized trust management, secure authentication, and transparent storage operations within distributed cloud environments. The architecture combined multiple technologies including blockchain-assisted validation, decentralized peer-to-peer storage systems, privacy-preserving encryption techniques, decentralized identity management, and automated smart contract authorization mechanisms. By integrating Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), secure hash generation, and encrypted data fragmentation, the framework ensured strong confidentiality protection and tamper-resistant storage verification. The experimental evaluation demonstrated that the proposed framework significantly outperformed traditional centralized cloud storage systems and conventional blockchain-based storage architectures across multiple performance metrics. The framework achieved superior data confidentiality, storage integrity, access-control efficiency, privacy preservation, attack resistance, scalability, and storage availability. The integration of decentralized blockchain validation eliminated centralized trust dependency and prevented unauthorized modifications of stored data. The use of encrypted fragmented storage improved resilience against data leakage and insider attacks while maintaining high availability and fault tolerance in distributed cloud environments. In conclusion, the proposed Privacy-Aware Blockchain Framework provides a robust, scalable, decentralized, and privacy-preserving solution for next-generation cloud storage applications. The integration of blockchain technology, decentralized storage networks, cryptographic security, and smart contract-based authorization establishes a trustworthy and intelligent distributed storage ecosystem capable of supporting privacy-sensitive digital applications. The proposed framework offers substantial contributions toward secure decentralized cloud computing, transparent storage management, and intelligent distributed data protection for future digital communication environments.

References

1. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf
2. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review*, *2*, 6–19.
3. Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger*. Ethereum Project Yellow Paper. https://ethereum.github.io/yellowpaper/paper.pdf
4. Benet, J. (2014). IPFS - Content addressed, versioned, P2P file system. *arXiv preprint arXiv:1407.3561*. https://doi.org/10.48550/arXiv.1407.3561
5. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
6. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647
7. Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications, 10*(4), 983–994. https://doi.org/10.1007/s12083-016-0456-1
8. Ali, M., Nelson, J., Shea, R., & Freedman, M. J. (2016). Blockstack: A global naming and storage system secured by blockchains. *USENIX Annual Technical Conference*, 181–194.

9. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *IEEE Security and Privacy Workshops*, 180–184. https://doi.org/10.1109/SPW.2015.27
10. Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. *17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 468–477. https://doi.org/10.1109/CCGRID.2017.8