WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Off Chain Storage Solution for Healthcare Data

Vijaya Nagojiche[1], Disha Bhogan[2]

[1] M.C.A Student Department of M.C.A, K.L.S. Gogte Institute of Technology, Udyambag Belagavi, Karnataka, India, nagojichevijaya@gmail.com. Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India

[2] M.C.A Student Department of M.C.A, K.L.S. Gogte Institute of Technology, Udyambag Belagavi, Karnataka, India, dishbhogan@gmail.com. Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India

A B S T R A C T

Off-chain storage systems are emerging as crucial components in the architecture of secure and scalable healthcare data management. These systems aim to decouple the heavy burden of storing large volumes of sensitive medical data from blockchain networks, while retaining blockchain's strengths in auditability, access control, and decentralization. This paper presents a synthesis of recent developments in off-chain storage frameworks for healthcare data, focusing on technologies such as IPFS, proxy re-encryption, self-sovereign identity, and hybrid blockchain systems. The reviewed models address key challenges including privacy, data integrity, interoperability, and real-time access across institutional boundaries. As the healthcare industry increasingly embraces decentralized digital infrastructure, these off-chain solutions hold promise for enabling secure, patient- centered, and regulation-compliant data ecosystems. These architectures enable encrypted health data to be stored in distributed systems like IPFS while managing permissions and audit logs on-chain through smart contracts. By leveraging proxy re-encryption, patients can grant and revoke access dynamically without exposing their private keys. Self-sovereign identity models further enhance trust by allowing individuals to control how and when their data is shared, promoting ethical data governance. Several recent implementations demonstrate the feasibility of cross-institutional data exchange, low-latency access in remote care settings, and compliance with privacy regulations such as HIPAA and GDPR. As the demand for interoperable, privacy-aware digital health systems grows, off-chain storage stands out as a foundational strategy to bridge security, scalability, and patient empowerment in next-generation healthcare networks

Keywords: Off-chain storage, Blockchain, IPFS, Proxy Re-encryption, Healthcare Data, Self-Sovereign Identity, Interoperability.

1. Introduction

The digitization of healthcare has led to exponential growth in the generation of medical data—from electronic health records (EHRs) and diagnostic imaging to wearable sensor outputs and patient-generated information. Managing this data securely, ethically, and efficiently is a major challenge for modern healthcare systems. Blockchain technology has been proposed as a secure and decentralized alternative to traditional data repositories; however, due to limitations in blockchain scalability and storage capacity, directly storing large datasets on-chain is impractical.To address this issue, off-chain storage architectures have been developed. These solutions allow sensitive data to be stored externally—on decentralized file systems such as the InterPlanetary File System (IPFS) or in secure cloud environments—while blockchain retains only metadata, hashes, and access policies. This hybrid approach provides a balance between decentralization, security, and performance, making it particularly well-suited for managing healthcare data. This paper explores recent innovations in off-chain storage frameworks tailored for the healthcare domain. We focus on key enabling technologies such as proxy re-encryption (PRE), decentralized identifiers (DIDs), self-sovereign identity (SSI), and federated access control via smart contracts. The following sections analyze leading research contributions, evaluate technical and ethical challenges, and propose future directions for the development of decentralized, patient- centric healthcare systems.These off-chain models not only alleviate blockchain's storage limitations but also enable more flexible and dynamic access control mechanisms. Through smart contracts, stakeholders such as hospitals, laboratories, and patients can define data-sharing policies that are enforced automatically and transparently. Moreover, by separating sensitive content from publicly viewable blockchain records, off-chain storage enhances compliance with privacy regulations like HIPAA and GDPR. Proxy re-encryption allows encrypted data to be securely re-shared without revealing underlying content or requiring full decryption cycles. Meanwhile, self-sovereign identity (SSI) systems empower individuals to manage their digital credentials independently, reducing reliance on centralized identity providers. These developments collectively represent a shift from institution- centered data control to patient-centric models. Additionally, hybrid frameworks facilitate interoperability among heterogeneous healthcare networks, supporting real-time access to patient data across geographic and organizational boundaries. As decentralized technologies mature, their integration into healthcare promises improved trust, transparency and continuity of care while maintaining data sovereignty.

facilitate interoperability among heterogeneous healthcare networks, supporting real-time access to patient data across geographic and organizational boundaries. As decentralized technologies mature, their integration into healthcare promises improved trust, transparency, and continuity of care while maintaining data sovereignty.

In practice, off-chain storage solutions are being adopted in various healthcare scenarios such as hospital-to-hospital data exchange, patient- controlled health record systems, and remote diagnostics powered by IoT. These implementations demonstrate not only technical feasibility but also growing interest in decentralizing healthcare infrastructure to reduce reliance on vulnerable central servers. For instance, distributed storage systems like IPFS allow redundant, content-addressed data to be stored across a peer-to-peer network, reducing the risk of single points of failure. Meanwhile, blockchain smart contracts act as immutable controllers of access logic, ensuring traceability and tamper-proof auditing.

One of the key innovations enabling secure data reuse without compromising confidentiality is proxy re-encryption, which allows data encrypted by one party to be securely transformed for access by another without revealing the original plaintext. This is especially beneficial in healthcare settings where multiple providers or researchers may need controlled access to a patient's data. Similarly, self-sovereign identity frameworks are proving valuable in allowing patients to carry their credentials securely across institutions, supporting universal health access without compromising privacy.

Despite these advantages, integrating off-chain storage with existing clinical workflows poses technical and regulatory challenges. These include data standardization, real-time synchronization, latency management, and ensuring compliance with jurisdiction-specific privacy laws. Addressing these issues requires collaboration across sectors—bringing together technologists, healthcare professionals, policymakers, and legal experts. As such, this paper aims to not only review technological advances in off-chain storage but also critically evaluate their readiness for real-world healthcare deployment and their implications for data governance and equity in digital health systems.

Moreover, the convergence of off-chain storage with emerging technologies like federated learning and edge computing offers additional pathways for decentralized health intelligence. These integrations enable privacy-preserving analytics directly at data sources, reducing latency and enhancing responsiveness in time-critical scenarios such as emergency care. As healthcare data continues to grow in complexity and volume, robust, distributed architectures will be essential to ensure sustainability. The transition toward these systems also reflects a broader paradigm shift—from reactive treatment models to proactive, data-driven care. Therefore, understanding and advancing off-chain storage mechanisms is not just a technical imperative but a foundational step toward the future of intelligent and ethical healthcare delivery.

2. Methodology

This study uses a systematic literature review (SLR) to explore and evaluate recent advancements in off-chain storage systems for healthcare data. We selected 15 peer-reviewed articles published between 2021 and 2025 through a multi-step screening process. The initial stage involved keyword-based searches in well-established academic databases including IEEE Xplore, SpringerLink, Elsevier ScienceDirect, ACM Digital Library, and arXiv. Search terms included combinations of "off-chain storage," "blockchain healthcare," "IPFS in healthcare," "proxy re-encryption," "self-sovereign identity," and "decentralized medical data."

Following the initial search, articles were filtered based on technical depth, clarity of architecture, relevance to healthcare data systems, and integration of blockchain-based access controls. Only studies presenting complete system models or implementations that addressed issues like privacy, scalability, or interoperability were included. Each selected paper was analyzed and categorized thematically to reflect key technological trends in off-chain data management for healthcare.

A. IPFS-Based Off-Chain Storage

This category highlights research leveraging the InterPlanetary File System (IPFS) as a decentralized storage layer for healthcare data. IPFS enables content-addressable, tamper-proof storage, making it ideal for large-scale EMRs and diagnostic files. Studies in this theme emphasized the benefits of content hashing, redundancy, and network resilience. Applications often paired IPFS with encryption algorithms to secure patient data and used blockchain only to store metadata and content hashes, thus reducing storage loads and improving scalability.

B. Proxy Re-Encryption Mechanisms

Papers in this theme explored the use of proxy re-encryption (PRE) to facilitate secure data sharing among multiple parties. PRE allows encrypted data to be re-encrypted for different recipients without revealing the plaintext, enhancing confidentiality in multi-provider or multi- institution scenarios. This technique supports dynamic data sharing, enabling patients to grant and revoke access rights in real time. Studies showcased systems where PRE was integrated with IPFS and smart contracts to streamline access control.

C. Blockchain-Integrated Access Control

This category focuses on systems where blockchain serves as the backbone for access permission management. Smart contracts are programmed to manage access rights, track data usage, and automate consent enforcement. These implementations typically store minimal but critical metadata on- chain, including timestamps, user identifiers, and policy conditions. Research in this area demonstrated how blockchain's immutability improves transparency and accountability in healthcare data workflows.

D. Self-Sovereign Identity (SSI) and DID Models

Studies classified under this theme proposed self-sovereign identity (SSI) and decentralized identifier (DID) frameworks to give patients full control over their identity and medical data. Patients use digital wallets to store verifiable credentials and issue access tokens to authorized healthcare providers. This identity-driven model eliminates the need for centralized identity managers, aligning with data sovereignty principles and privacy regulations like GDPR and HIPAA.

E. Interoperability and Cross-Chain Communication

Some selected works addressed the challenge of interoperability across disparate healthcare and blockchain systems. These papers introduced cross-chain data exchange models, where encrypted patient data stored off-chain can be referenced and shared across multiple blockchain networks. Solutions included atomic cross-chain protocols and metadata standardization to enable seamless communication between institutions.

F. Privacy and Security Enhancements

This theme included approaches that reinforced data privacy and system integrity using techniques such as zero-knowledge proofs (ZKPs), multi-party computation (MPC), and homomorphic encryption. These technologies were used to validate user access and data authenticity without revealing sensitive content. Studies showed how privacy-preserving cryptographic tools enhance compliance while maintaining usability.

G. Edge and IoT Integration

Several papers highlighted the integration of off-chain storage with edge computing and IoT-based health monitoring systems. Data from wearable devices or home-based sensors is encrypted locally and stored in IPFS, while blockchain tracks and controls access. These architectures support real-time medical analysis and remote diagnostics, especially in rural or low-connectivity regions. Edge compatibility reduces latency and minimizes dependence on centralized infrastructures.

H. Real-World Use Cases and Implementations

Finally, some papers presented full-stack implementations and pilot deployments in hospital networks, research institutions, or national health systems. These studies demonstrated the operational viability of combining IPFS, blockchain, and PRE in real clinical workflows. Key outcomes included enhanced data interoperability, improved auditability, and stronger patient trust in data-sharing platforms.

3. Thematic Analysis and Discussion

The review of literature on off-chain storage in healthcare reveals that current research and implementations cluster around four main thematic areas. These themes form the foundation of modern decentralized healthcare data systems that aim to enhance privacy, interoperability, and control while reducing dependence on centralized infrastructures.

A. IPFS-Based Off-Chain Storage

One of the most prominent themes involves using the InterPlanetary File System (IPFS) for secure off-chain data storage. IPFS offers content- addressable, distributed storage, which significantly reduces the burden on blockchain networks. By storing encrypted medical data such as EHRs, diagnostic reports, and sensor logs in IPFS and keeping only metadata and hash references on-chain, systems improve scalability and minimize transaction overhead. Studies in this theme also highlight improvements in data redundancy and resilience against single points of failure. Many implementations incorporate mechanisms like persistent pinning and verifiable audit trails to ensure long-term availability of off-chain data, even in decentralized environments.

B. Proxy Re-Encryption and Access Control

Another core theme is the application of proxy re-encryption (PRE) to support dynamic, privacy-preserving data sharing. PRE allows a

patient's encrypted health data to be securely re-encrypted for third parties—such as hospitals, researchers, or insurers—without exposing the original content. This technique ensures that patients maintain cryptographic ownership of their data while enabling authorized stakeholders to gain access based on smart contract-defined conditions. Smart contracts automate the verification of access rights and log every interaction immutably, providing accountability. These systems support fine-grained access control, real-time revocation, and temporary permission grants, enabling more ethical and flexible data governance.

C. Self-Sovereign Identity and Decentralized Identifiers

A growing number of studies incorporate self-sovereign identity (SSI) models and decentralized identifiers (DIDs) to improve identity management in decentralized healthcare systems. Instead of relying on centralized authorities, patients are given control over their digital identities through verifiable credentials stored in personal digital wallets. Using DIDs, they can authenticate themselves across institutions while deciding which data points to share. This framework increases patient autonomy and aligns with data protection regulations such as HIPAA and GDPR. Furthermore, the decentralized nature of these systems makes them more resistant to breaches and insider threats compared to traditional identity systems.

D. Interoperability and Real-World Implementation

The final theme focuses on cross-platform interoperability and real-world deployment of off-chain storage frameworks. Research in this area addresses the technical challenge of exchanging medical data between different blockchain networks or legacy healthcare systems. Solutions such as atomic cross-chain communication and metadata standardization have been proposed to support seamless integration. Some projects have gone further by deploying pilot systems in hospitals, demonstrating improved auditability, patient trust, and system responsiveness. These implementations highlight how off-chain storage enables real-time access to patient data, supports clinical decision-making, and facilitates longitudinal health tracking across multiple institutions

4. Challenges and Solutions

The review of literature on off-chain storage systems for healthcare reveals four major challenges that researchers and developers face in designing secure, scalable, and interoperable data infrastructures. These challenges revolve around data availability, access control, system interoperability, and user-centric privacy management. Each challenge is being actively addressed through innovative technical and architectural solutions.

A. Ensuring Data Availability and Persistence

One major challenge of using decentralized file systems like IPFS is maintaining long-term data availability. Since IPFS does not guarantee permanent storage unless content is actively "pinned," there is a risk of data loss if no nodes retain the content. To address this, researchers have introduced decentralized pinning strategies using IPFS cluster management and incentivized storage through token-based systems. Others leverage hybrid storage approaches, combining IPFS with institutional cloud backups or on-premises redundancy to enhance reliability. Verifiable audit trails and heartbeat mechanisms are also employed to monitor and ensure the presence of vital medical records.

B. Fine-Grained Access Control and Security

Traditional access control models struggle to meet the dynamic and granular needs of healthcare data sharing. Managing who can access which data—and under what conditions—remains a key difficulty. To solve this, systems incorporate smart contracts that enforce fine-grained access policies based on user roles, contextual parameters, and time-limited permissions. Proxy re-encryption (PRE) enables encrypted data to be re- shared securely without decrypting it at the source, supporting real-time permission updates while preserving confidentiality. Attribute-Based Encryption (ABE) and Role- Based Access Control (RBAC) models have also been used to support multi-stakeholder environments such as hospitals, insurers, and researchers.

C. Achieving Interoperability Across Platforms

Healthcare data is often fragmented across different systems, networks, and standards. Off-chain storage frameworks must bridge these silos without compromising performance or privacy. Cross-chain protocols and metadata standardization have been proposed to support secure interoperability between multiple blockchain networks or legacy healthcare systems. Some projects introduce adapters that map off-chain storage logic to Health Level 7 (HL7) and FHIR standards, enabling smoother data integration and semantic consistency. These innovations are key to ensuring that patient data is usable across diverse medical institutions and jurisdictions.

D. Privacy, Identity, and Consent Management

Empowering patients to control their data while maintaining usability is a delicate balance. Centralized identity solutions are prone to breaches, while decentralized approaches may suffer from complexity and low adoption. Self-sovereign identity (SSI) frameworks using decentralized identifiers (DIDs) offer a promising solution, allowing patients to issue access credentials through digital wallets. These identities are cryptographically secure and interoperable across platforms. Smart contracts automate consent enforcement, ensuring that every data access is preceded by a verifiable approval event. Techniques like zero-knowledge proofs (ZKPs) and selective disclosure further improve privacy by allowing data validation without full content exposure.

5. Future Direction

As healthcare systems continue to digitize and decentralize, off-chain storage technologies must evolve to address new challenges in data security, patient privacy, system scalability, and real-time interoperability. The following future directions represent key areas for advancing the deployment and innovation of off-chain storage frameworks in healthcare:

1. Integration of AI for Data Governance and Automation

Artificial Intelligence (AI) is poised to play a pivotal role in managing off-chain healthcare systems. AI models can help automate access control decisions, monitor abnormal data usage patterns, and detect unauthorized activities across decentralized storage layers. Machine learning algorithms can also be used to optimize storage strategies, predict high-demand access periods, and recommend node replication for better data availability. AI- integrated smart contracts could support intelligent, real-time decisions based on evolving patient consent or policy changes.

2. Privacy-Preserving Analytics and Federated Learning

Future systems will integrate federated learning (FL) with off-chain storage to enable collaborative, privacy-preserving analytics across hospitals and research centers. Instead of centralizing sensitive data, FL allows models to be trained locally while only sharing model updates. When combined with encrypted data on IPFS and verifiable access logs on blockchain, this approach supports secure, decentralized healthcare AI without exposing raw patient data. This is especially useful in genomic research, remote diagnostics, and personalized treatment planning.

3. Sustainable and Lightweight Architectures for IoT-Driven Healthcare

With the growing use of wearables and smart health sensors, future off-chain frameworks will need to support lightweight, energy-efficient storage and access protocols. Innovations may include energy-harvesting IoT nodes that store encrypted data locally and synchronize with IPFS during low- traffic or low-energy-cost periods. Protocols that reduce bandwidth usage, such as delta synchronization or selective file pinning, will help in maintaining long-term storage while conserving network and power resources.

4. Standardization and Regulatory Compliance

A key direction for future work lies in establishing global standards for off-chain healthcare data exchange. This includes developing interoperable metadata schemas, compliant identity frameworks (such as DID/VC aligned with HL7 FHIR), and regulatory protocols that satisfy HIPAA, GDPR, and local health data laws. Blockchain-enabled compliance monitoring can offer real-time audits and policy enforcement, making decentralized systems more acceptable to government and enterprise stakeholders.

5. Quantum-Resistant Encryption and Security Protocols

As quantum computing capabilities evolve, existing cryptographic methods may become vulnerable. Future off-chain systems must adopt quantum-resistant encryption schemes to safeguard long-term patient data. Lattice-based cryptography and post-quantum PRE models will be crucial for ensuring secure data sharing and storage in a future-proof environment. Additionally, researchers will need to evaluate how quantum-safe protocols interact with off-chain file systems and blockchain transaction layers.

6. Context-Aware Consent and Smart Legal Agreements

Traditional consent models are static and fail to capture the complexities of dynamic healthcare interactions. Future systems will feature context-aware consent mechanisms powered by natural language processing (NLP) and blockchain-based smart legal agreements. These contracts can adapt to changes in treatment plans, emergencies, or third-party data requests, offering real-time, legally binding control to patients and caregivers. Such adaptability will foster trust and encourage broader adoption of decentralized health data systems.

7. Integration with National and Global Health Infrastructures

As nations explore digital health reforms, future off-chain storage solutions will need to integrate with national health stacks and public health surveillance platforms. This includes supporting large-scale vaccination records, pandemic response systems, and medical supply chain management. Using decentralized identifiers (DIDs) and scalable IPFS-based registries, such systems can achieve both privacy and traceability at scale. Global collaboration frameworks may also emerge, enabling secure cross-border sharing of patient records with universal standards. environmentally responsible data operations.

6. Conclusion

Off-chain storage solutions have emerged as critical enablers of scalable, secure, and patient-centric healthcare data systems. By separating bulk data storage from blockchain networks, these architectures offer a balanced approach to data integrity, access control, and performance. Technologies such as IPFS, proxy re-encryption, and self-sovereign identity empower patients to maintain ownership and control over their medical data. Smart contracts facilitate automated, transparent access management while ensuring compliance with privacy regulations. The reviewed literature highlights the growing maturity of hybrid blockchain-off-chain systems across institutional and national levels. Despite technical and regulatory challenges, ongoing innovation continues to strengthen data availability, interoperability, and privacy. As decentralized healthcare ecosystems evolve, off-chain storage will remain a cornerstone of secure digital health infrastructure. Future systems must prioritize sustainability, real-time analytics, and universal standards to maximize their impact. Ultimately, such solutions pave the way for ethical, interoperable, and trustworthy healthcare data management.

7. References

[1] Tran, P., Nguyen, T., Chu, L., Tran, N., & Ta, H. (2024). A solution for commercializing, decentralizing and storing electronic medical records by integrating proxy re-encryption, IPFS, and blockchain. arXiv Preprint, arXiv:2402.05498. ([MDPI][1],

[arXiv][2])

[2] Tcholakian, M., Gorna, K., Laurent, M., Ben Ayed, H. K., & Naghmouchi,

M. (2024). Self-Sovereign Identity for cons ented and content-based access to medical records using blockchain. arXiv Preprint, arXiv:2407.21559. ([arXiv][3])

[3] Meier, V., et al. (2021). Hyperledger Healthchain: Patient-centric IPFS-based storage of health records. Electronics, 10(23), 3003. DOI:10.3390/electronics102 33003. ([MDPI][1])

[4] Guo, J., Zhao, K., Liang, Z., & Min, K. (2024). Efficient and secure EMR storage and sharing scheme based on Hyperledger of Engineering and Applied Science, 72, Article 110. ([SpringerOpen][7])

[5] Anonymous authors. (2024). HealthRec-Chain: Patient-centric blockchain enabled IPFS for privacy preserving scalable health data. Computer Networks, 241, Article 110223. DOI:10.1016/j.comnet.2024.110223.

([ScienceDirect][8])