International Journal of Scientific Research and Engineering Development-–Volume 8 Issue 4, July-Aug 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Off-Chain Storage Options for Medical Data

Mrutyunjaya S Emmi*, Prajwal Allayyanavar**, Pramod Poojari***
* (Assistant Professor, Department of MCA, KLS Gogte Institute of Technology, Belagavi-590006, India
Email: msemmi@git.edu)
** (Master of Computer Applications, KLS Gogte Institute of Technology, Belagavi-590006, India
Email: allayyanavarprajwal@gmail.com)
*** (Master of Computer Applications, KLS Gogte Institute of Technology, Belagavi-590006, India
Email: pramodpoojari36@gmail.com)

--************************----------------------------------

Abstract:

Blockchain technology has gained popularity in healthcare systems because to its potential to improve data security, privacy, and interoperability. However, the inherent limitations of blockchain, such as scalability and storage constraints, have led to the exploration of off-chain storage solutions. The Interplanetary File System (IPFS) and hybrid blockchain models are the main topics of this paper's thorough analysis of off-chain storage solutions for healthcare data management. We analyze the strengths and limitations of existing approaches, propose a novel framework for secure and scalable off-chain storage, and discuss future research directions. According to our research, off-chain solutions have the ability to solve important issues with healthcare data management while maintaining privacy laws.

Keywords — **Healthcare data, blockchain, off-chain storage, IPFS, data privacy, scalability, and distributed systems.**

--************************----------------------------------

I.INTRODUCTION

Electronic health records (EHRs), medical imaging data, and patient diagnostic reports are only a handful of the many sensitive data sets produced by the healthcare sector. Given the rising frequency of cyberattacks and data breaches, it is critical to ensure the security, privacy, and integrity of this data [1]. Because blockchain technology is decentralized, irreversible, and transparent, it has shown great promise as a solution for managing healthcare data [2]. However, the storage limitations and scalability issues of blockchain networks have hindered their widespread adoption in healthcare systems [3].

Offchain storage solutions, which store big datasets outside the blockchain while preserving a secure connection to the on-chain data, have been offered by researchers as a solution to these problems. For handling healthcare data, off-chain storage solutions like distributed cloud storage and the InterPlanetary File System (IPFS) provide scalable and affordable options [4]. These solutions enable healthcare systems to leverage the benefits of blockchain without compromising performance or incurring excessive storage costs.

This study intends to present a thorough analysis of offchain storage options for medical data, emphasizing their development, application, and effects on privacy and data security. Additionally, we offer a revolutionary framework that combines blockchain technology with off-chain storage to improve the scalability and effectiveness of healthcare data management systems.

The scope of this study is conceptual, focusing on how decentralized storage mechanisms can be integrated with blockchain to manage electronic health data more securely and efficiently. Rather than proposing a fully implemented system, this work presents a theoretical model for data handling, access control, and integrity verification using smart contracts and IPFS.

The key contributions of this paper are:
- A review of existing blockchain and off-chain storage approaches in the healthcare domain.
- A conceptual framework that integrates IPFS with blockchain to securely store and manage sensitive health records.
- A discussion on ethical, legal, and interoperability considerations critical to real-world deployment.
- Proposed evaluation metrics and an implementation outlook for future prototyping.

The remainder of this paper is organized as follows: Section II presents related studies and background on blockchain and off-chain storage in healthcare. Section III provides a detailed literature review comparing notable frameworks. Section IV outlines the proposed hybrid architecture, followed by the conceptual methodology in Section IV-B. Section V describes a real-world use-case scenario, and Section VI details the data flow of the system. Section VII discusses the advantages and limitations of off-chain storage. Section VIII compares different blockchain storage approaches. Section IX outlines the security features of the framework. Section X highlights future research directions. Sections XI to XIII explore ethical, interoperability, and implementation perspectives. Finally, Section XIV concludes the paper.

II.RELATED STUDY

A. *BLOCKCHAIN IN HEALTHCARE*

Blockchain technology has been widely explored for healthcare applications, including EHR management, medical data sharing, and supply chain tracking [5]. Its decentralized architecture ensures data integrity and eliminates the need for trusted intermediaries. However, the storage of large datasets on-chain is impractical due to the limited block size and high transaction costs [6].

B. OFF-CHAIN STORAGE MECHANISMS AND RELATED WORK

To overcome the scalability and storage constraints of blockchain, off-chain storage techniques including IPFS, distributed databases, and cloud storage have been suggested [7].IPFS, in particular, has gained traction due to its decentralized and content-addressable nature, which ensures data availability and integrity [8].

C. RELATED WORK

The use of off-chain storage for medical data has been the subject of several studies. For example, Randhir Kumar and colleagues [10] proposed a distributed off-chain storage system for patient diagnostic reports that makes use of blockchain and IPFS. For the protection of medical data, Jayapriya Jayabalan [6] introduced a scalable blockchain concept with off-chain IPFS storage. Bessem Zaabar [7] developed HealthBlock, a blockchain-based system for managing medical data that leverages off-chain storage to increase scalability.

III. LITERATURE REVIEW

Recent studies have emphasized the importance of integrating blockchain technology with decentralized off-chain storage to address the scalability and privacy challenges associated with healthcare data.

Jayapriya and Jeyanthi [6] proposed a scalable blockchain framework using IPFS for managing Electronic Health Records (EHRs). Their system implements multi-factor authentication and employs symmetric (AES-128) and asymmetric (RSA-4096) encryption to secure data. By storing encrypted health data in IPFS and only recording hashes on the blockchain, they preserve data integrity while significantly reducing the on-chain storage burden. Their patient-centric access model ensures that patients retain control over who can view their medical data, with the ability to revoke access post consultation. This approach also introduces key transactions, allowing dynamic key sharing and revocation, thus enhancing the security and flexibility of the system.

In another study, Randhir Kumar et al. [10] introduced a consortium blockchain framework for storing patient diagnostic reports using IPFS. They highlighted the limitations of centralized storage models and proposed a system that uses content-addressed hash storage on-chain while retaining large files off-chain in IPFS. Their model employs Proof-of-Work (PoW) consensus for validating transactions and ensures access control through Proof-of-Identity (PoI) verification for healthcare providers. The system was implemented using Python Flask and IPFS, and experiments showed reduced block mining time and efficient access of diagnostic reports across peers. This framework prioritizes privacy, scalability, and fast data retrieval within a decentralized setup.

Both studies confirm that combining blockchain with off-chain storage mechanisms like IPFS offers a secure and efficient alternative to traditional centralized systems. However, Jayapriya's model focuses more on granular access control and transaction structure, whereas Randhir's work emphasizes practical deployment and peer authorization in a consortium setting.

These frameworks laid the groundwork for our proposed hybrid model, which adopts the strengths of both — ensuring robust privacy, seamless access control, and scalable health data management.

IV. PROPOSED FRAMEWORK

A. *SYSTEM ARCHITECTURE*

In order to manage healthcare data, we propose a hybrid blockchain framework that combines off-chain and on-chain storage.

The framework consists of the following components:

- **On-Chain Layer:** This layer stores cryptographic hashes of medical files, metadata such as patient and provider identifiers, timestamps, and access policies. By recording only hashed pointers instead of full datasets, it ensures the immutability and verifiability of off-chain content while reducing storage overhead on the blockchain [1], [6], [10].

- **Off-Chain Layer:** The off-chain layer handles the storage of large and sensitive healthcare files, including electronic health records (EHRs), diagnostic images, and lab reports. These files are encrypted and uploaded to decentralized storage systems like the InterPlanetary File System (IPFS) or distributed cloud networks. This approach improves system scalability and minimizes costs associated with on-chain data expansion [4], [10], [30].

- **Access Control Mechanism:** Fine-grained access control is enforced through smart contracts deployed on the blockchain. These contracts automate permission checks, key sharing, and audit logging based on patient-defined rules. Only authorized entities can retrieve the IPFS hash and decrypt the data, ensuring compliance with privacy regulations such as HIPAA, GDPR, and DISHA [2], [6], [27].

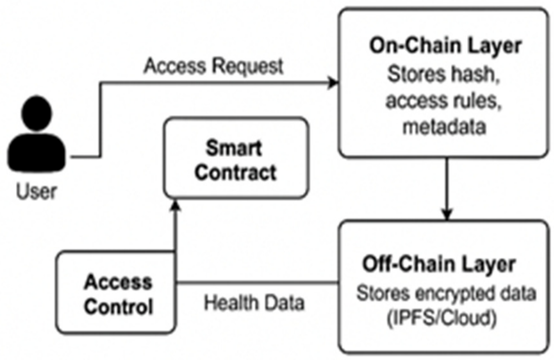


Fig.1.System architecture to manage patient healthcare data.

B. *METHODOLOGY*

This section outlines the conceptual operation of the proposed hybrid system, which combines blockchain with decentralized storage to enable secure and privacy-compliant management of healthcare data. The methodology presents a logical flow of how each component interacts to facilitate data handling and access.

1. Identity Registration and Data Collection:
Users such as patients and healthcare professionals are issued a unique digital identity after registering with the system. During medical visits, patient data including diagnostic results and prescriptions are securely captured and formatted for further processing [6],[11],[20].

2. Data Encryption and External Storage:
Before transmission, sensitive health data is encrypted locally to protect it against unauthorized access. The encrypted files are then stored using the Interplanetary File System (IPFS) or a cloud-based distributed storage solution. Upon successful upload, IPFS returns a content-based address (hash), which serves as a retrieval pointer [4],[10],[30].

3. Secure Hash Storage on Blockchain:
Rather than storing full medical records on-chain, the system logs only the IPFS hash along with relevant metadata—such as timestamps, file descriptors, and user identifiers—using smart contracts. This approach maintains the immutability and auditability of blockchain without introducing storage inefficiencies [1],[5],[9].

4. Role-Based Access Control:
Access to medical records is governed through smart contracts that define and enforce authorization rules. Patients retain full control over their data and can grant or revoke access to specific providers. When access is permitted, it is recorded on the blockchain for transparency and accountability [2],[6].

5. Record Retrieval and Decryption:
Authorized healthcare professionals can retrieve the IPFS hash from the blockchain and use it to download the encrypted file. The required decryption key is securely shared by the patient, typically using public key encryption methods. This ensures that only designated recipients can unlock and view the original content [9],[10].

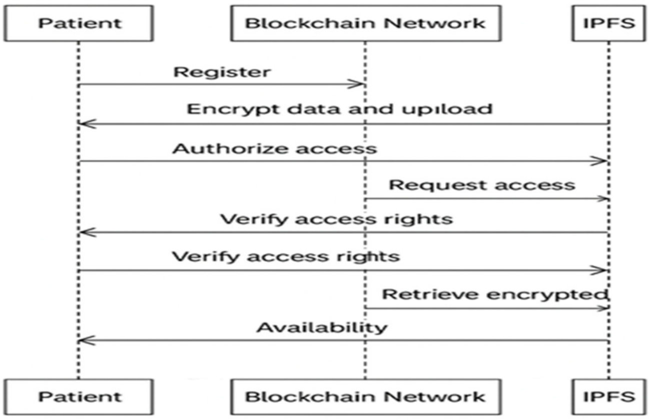
6. Access Verification and Smart Contract Triggering:
When a healthcare provider initiates a data access request, the system verifies their credentials and permissions against the rules encoded in the smart contract. If validated, the smart contract triggers the process of securely releasing the IPFS hash, ensuring only authorized access without the need for manual intervention [2], [9].

7. Audit Trail and Consent Logging:
The system incorporates automated audit trail generation to log every data-related event, such as uploads, access requests, and permission changes. Each event is immutably recorded on the blockchain along with a timestamp and user identity. This traceability ensures that any access to sensitive healthcare records is transparent and accountable. Furthermore, patient consent is captured through digital signatures embedded in blockchain transactions, reinforcing compliance with data protection regulations and ethical standards.

Fig.2. Sequence of interactions for healthcare data registration, access, and retrieval.

The steps below explain each interaction illustrated in Fig.2:

1. The patient registers with the system and is assigned a unique digital identity linked to their health profile.
2. Doctors or authorized healthcare providers also register and obtain verified credentials for accessing medical records.



3. Upon consultation, the doctor generates diagnostic reports or treatment data and securely shares it with the patient.
4. The patient encrypts the medical file using symmetric encryption and prepares it for upload.
5. The encrypted file is uploaded to the IPFS network, which returns a unique content identifier (hash).
6. The patient or system records the IPFS hash on the blockchain via a smart contract, along with metadata like timestamp and file type.
7. A healthcare provider submits an access request through the system to view the patient's medical file.
8. The smart contract checks whether the requester has valid access rights based on patient-defined rules.
9. If authorized, the blockchain returns the IPFS hash to the requester, who fetches the encrypted file from IPFS.
10. The patient securely shares the decryption key with the provider, who decrypts and accesses the medical data.

V. USE-CASE SCENARIO

Table. 1. Use case scenario: Hybrid Blockchain Model.

VI. DATA FLOW

1. **Data Encryption and Off-Chain Storage**

   Patient medical data is encrypted locally using symmetric encryption (e.g., AES) and uploaded to decentralized storage like IPFS. A unique content hash (CID) is generated to reference the file [4], [6], [30].

2. **Hash Generation and On-Chain Storage:**

Actor	Action
Patient	Uploads encrypted diagnostic report.
IPFS Node	Stores file and returns content-addressed hash.
Smart Contract	Records hash, timestamp, and metadata on-chain.
Patient	Grants access to doctor via transaction.
Doctor	Requests access to patient report.
System	Verifies rights and provides IPFS hash.
Doctor	Downloads and decrypts file.
Patient	Revokes access after consultation.

   The IPFS hash, along with associated metadata such as timestamp, patient ID, and access permissions, is stored on the blockchain through a smart contract. This ensures immutability and integrity of the data reference without exposing the actual medical content [1], [5], [10].

3. **Access Control and Retrieval by Authorized Users:**

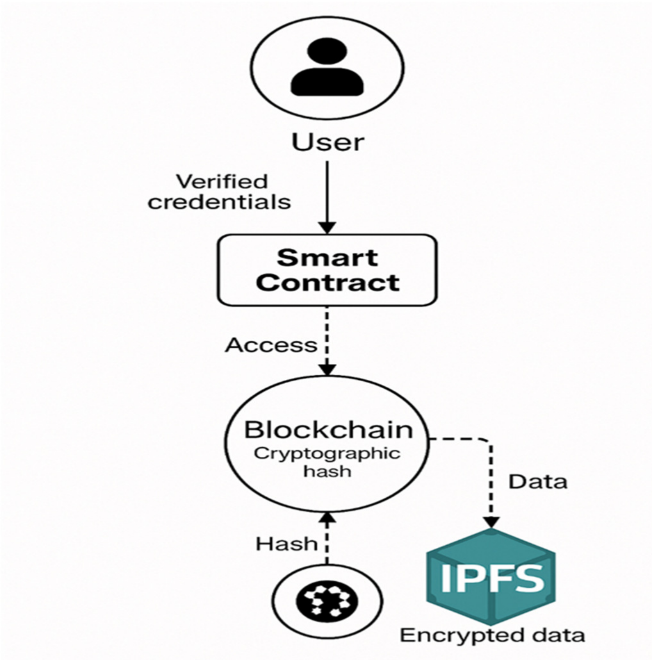
   When an authorized user requests access, the smart contract verifies permissions and shares the IPFS hash. The user can then retrieve and decrypt the data using a key shared by the patient. All access events are logged on-chain for auditability [2], [6], [9].

Fig. 3. Data flow diagram for blockchain-based data storage and access system.

VII. DISCUSSION

A. *Advantages Of Off-Chain Storage*

- **Scalability:** Off-chain storage solutions like IPFS support the handling of large datasets, such as medical images and diagnostic records, without burdening the blockchain. Since only the content hash is stored on-chain, the blockchain



remains lightweight and efficient even as the volume of health data grows [4], [6].

- **Cost-Effectiveness:** Storing large volumes of data directly on-chain results in higher transaction fees and limited scalability. Off-chain storage minimizes this cost by significantly reducing the data stored on the blockchain layer, which is especially beneficial in healthcare use cases [4], [15].

- **Data Privacy:** Patient records are encrypted before being stored in IPFS, and access control is managed through smart contracts on the blockchain. This dual-layer security approach ensures data confidentiality while still allowing authorized access [1], [2], [9].

- **Efficient Data Access:** IPFS supports peer-to-peer distributed file retrieval, allowing users to access medical records from the nearest available node. This helps reduce latency and improves the overall data availability and responsiveness of the system [6], [16].

B. *Challenges and Limitations*

- **Data Availability:** Although IPFS is decentralized, there is no guarantee that a particular file will always be available unless actively pinned or frequently accessed. Without dedicated availability mechanisms, this could lead to missing data during critical operations [7], [30].

- **Interoperability:** Integrating blockchain and off-chain storage with legacy hospital systems, EHRs, and cloud-based infrastructure remains a complex task due to varying standards, APIs, and data schemas [3], [12], [17].

- **Regulatory Compliance:** Compliance with data protection laws such as HIPAA, GDPR, and national health policies poses a challenge for immutable blockchain systems. Features like the "right to erasure" conflict with blockchain immutability, requiring additional solutions for legal alignment [2], [11], [27].

- **User Adoption:** Despite technical robustness, real-world deployment depends heavily on user trust and digital literacy. Patients and providers must feel confident managing access rights and using blockchain-based interfaces [8], [19], [28].

VIII. Comparative Analysis

Parameter	On-Chain Only	Off-Chain with IPFS	Hybrid Approach (Proposed)
Storage Cost	High	Medium	Low
Data Availability	High	Medium	High
Scalability	Low	High	High
Access Control	Limited	Medium	Strong(via Smart Contract)

Table. 2. Comparison of Blockchain Storage Approaches.

IX. Security Analysis

The proposed hybrid framework enhances healthcare data security by leveraging the combined strengths of blockchain technology and decentralized storage. This section outlines how the system addresses key security objectives: confidentiality, integrity, availability, and access control.

1. Data Confidentiality

Data confidentiality is maintained through encryption mechanisms applied before data is uploaded to the off-chain storage (IPFS). Patients encrypt their medical records locally using symmetric encryption (e.g., AES), and the decryption key is only shared with authorized healthcare providers using public-key cryptography (e.g., RSA). This ensures that even if the data is accessed maliciously from the storage layer, it remains unintelligible without the correct key [2],[6].

2. Data Integrity
Blockchain ensures the immutability and verifiability of medical records by storing the cryptographic hash of each file on-chain. Any tampering with the data stored in IPFS will result in a hash mismatch, immediately indicating that the file has been altered. This built-in mechanism makes unauthorized modifications detectable and traceable [1],[5].

3. Access Control
The framework employs smart contracts to enforce fine-grained access control. Patients define access rules that are recorded and executed on the blockchain. Only verified users (e.g., healthcare professionals) with granted permissions can retrieve the IPFS hash and decrypt the file. This ensures that access to sensitive health data is governed by transparent and tamper-proof logic [6],[9].

4. Auditability
Each transaction involving data access, modification, or permission updates is logged on the blockchain. These records serve as an immutable audit trail that can be reviewed for compliance, dispute resolution, or forensic analysis in case of unauthorized access attempts [1],[2].

5. Availability
Using IPFS for off-chain storage enhances data availability through distributed peer-to-peer nodes. Even if some nodes go offline, the data can still be accessed from other nodes in the network. This decentralized architecture minimizes the risk of single points of failure commonly found in centralized cloud systems [4],[7].

6. Governance and Consent Control
In addition to technical safeguards, effective data governance plays a crucial role in decentralized healthcare environments. The proposed framework adopts a patient-centric model, wherein individuals retain full authority over their medical data and control access permissions dynamically. Smart contracts are used to encode consent policies, allowing patients to grant, monitor, and revoke access in real time. Each transaction related to data access is immutably logged on the blockchain, ensuring transparency and traceability. This approach not only automates the enforcement of privacy rules but also minimizes administrative overhead, offering a scalable solution that aligns with modern data protection principles and regulatory requirements [6],[11].

7. Key Management and Revocation
A secure blockchain-based healthcare system must include reliable key management practices. In the proposed model, patients are responsible for generating and controlling their private keys, which are used to encrypt and decrypt sensitive health records. However, key compromise or loss poses a critical risk. To address this, the framework could incorporate mechanisms for key rotation and revocation, enabling patients to update or invalidate old keys through smart contracts. This ensures that access remains secure even in the event of suspected breaches or lost credentials, thereby preserving long-term data confidentiality and control.

8. Resistance to Insider Threats
By decentralizing data access and enforcing policies through smart contracts, the system reduces reliance on centralized administrators, who are often targets of insider abuse. Since access rights and interactions are governed by immutable blockchain logic, unauthorized internal modifications are prevented, and any suspicious activity becomes easily traceable through the audit trail [3], [6], [9].

X.FUTURE RESEARCH DIRECTIONS

- **Hybrid Storage Models:** While IPFS is widely used for off-chain storage in blockchain-based healthcare systems, future work could explore integrating multiple distributed storage technologies such as Filecoin, Storj, or Swarm to enhance reliability and scalability. This would allow the system to dynamically select storage backends based on file type, urgency, or network conditions, improving data access efficiency and resilience [7], [16],[30].
- **Data Provenance:** Ensuring the authenticity and traceability of healthcare records over time is a crucial research direction. Mechanisms for maintaining data provenance—tracking who generated the data, when it was modified, and by whom—can significantly improve trust and compliance in medical systems. Blockchain's immutable ledger provides a strong foundation, but extending this to track off-chain content lifecycle is an area for further exploration [6], [9], [29].
- **Quantum-Resistant Encryption:** As quantum computing becomes more viable, traditional cryptographic algorithms like RSA and ECC may become vulnerable. Future systems should investigate quantum-resistant encryption techniques such as lattice-based cryptography or post-quantum key exchange protocols to protect patient records stored off-chain. Adopting these technologies proactively will help ensure the long-term security of decentralized healthcare solutions [12], [24], [18].

XI.ETHICAL AND SOCIAL IMPLICATIONS

As blockchain and decentralized storage technologies are being explored for healthcare applications, their ethical and societal consequences must be evaluated thoroughly. The proposed conceptual model empowers patients with ownership and control over their medical records through smart contract-based access mechanisms, a design inspired by current trends in privacy-preserving healthcare systems [2], [6], [9].

This theoretical approach offers strong ethical alignment with principles of digital consent and data sovereignty. However, challenges such as digital literacy gaps and unequal access to digital infrastructure may hinder equitable participation. These concerns are particularly relevant in regions where the infrastructure for decentralized systems is still emerging [11], [19], [20].

Furthermore, the concept of consent fatigue, where patients may repeatedly approve data access without full comprehension, remains a concern in any patient-driven model. Future implementations based on this framework should explore audit visibility and simplified permission layers to ensure trust and usability [27], [28].

XII. DATA STANDARDS COMPLIANCE

One of the critical challenges for blockchain adoption in healthcare is achieving interoperability with existing digital health systems. Current hospital infrastructure often relies on centralized architectures, proprietary data formats, and compliance-driven workflows. For a blockchain-based solution—especially one involving off-chain storage—to be viable, it must be designed to work alongside established healthcare data standards and regulatory requirements.

A central aspect of this interoperability is alignment with data exchange standards like HL7 (Health Level Seven) and FHIR (Fast Healthcare Interoperability Resources). These standards define how healthcare information is structured and transmitted between systems. The proposed conceptual model is designed with modular compatibility, where APIs and smart contracts could be built to interact with FHIR-compliant data elements. This would allow the blockchain layer to store metadata such as access logs, timestamps, and file hashes, while off-chain systems continue to manage large files like diagnostic images, prescriptions, or lab results [12], [17].

Another important consideration is semantic interoperability—the ability for different systems to interpret and use data meaningfully. To enable this, healthcare data elements referenced on-chain (e.g., patient IDs, treatment codes) should conform to globally accepted vocabularies such as SNOMED CT, LOINC, or ICD-10. This ensures that information shared across systems, institutions, or borders retains its meaning and can be correctly interpreted by receiving platforms [5], [17].

Additionally, the system must incorporate authentication and authorization protocols that comply with widely adopted security standards. For example, integrating OAuth 2.0, OpenID Connect, or digital signature verification techniques could allow interoperability with electronic health portals and ensure that blockchain-based access control does not conflict with existing IT policies in hospitals [2], [11].

From a legal interoperability perspective, the system must also be designed with flexibility to accommodate varying privacy laws such as HIPAA in the United States, GDPR in Europe, and DISHA in India. These regulations govern consent management, data retention, and the "right to erasure." Since blockchain is inherently immutable, the proposed framework suggests storing only encrypted hashes and metadata on-chain, with actual data stored off-chain to facilitate compliance with deletion or revocation requests [6], [9], [27].

Finally, to encourage future adoption, the model should support open-source standards and interfaces, which can be audited, extended, or adapted by different healthcare institutions or developers. This would enable hospitals, insurance providers, and regulatory bodies to participate in a shared, trustless data environment without vendor lock-in.

By embracing technical, semantic, and legal interoperability, the conceptual framework improves its adaptability and lays the groundwork for integration into real-world healthcare ecosystems.

XIII. IMPLEMENTATION OUTLOOK

Although the proposed framework is conceptual, it provides a practical direction for future implementation. A prototype system could utilize the Ethereum blockchain with smart contracts written in Solidity and deployed on a public test network such as Ropsten or Goerli. IPFS would serve as the off-chain storage layer, enabling secure upload and retrieval of encrypted healthcare records.

User identity management could be incorporated through decentralized identity methods such as Self-Sovereign Identity (SSI) or blockchain-linked digital wallets. Access control logic would be managed by smart contracts that validate user roles and permissions. A web-based interface, developed using frameworks like React or Angular, could allow healthcare providers and patients to interact securely with the system.

Standard public-private key cryptography would be employed for data encryption and secure key sharing. In a future prototype, system performance could be evaluated by testing data access latency, contract execution speed, and network resilience. This outline offers a foundational roadmap for translating the proposed design into a functional, real-world solution [6], [10].

XIV. CONCLUSION

The proposed conceptual framework introduces a hybrid blockchain architecture that integrates off-chain storage systems like IPFS to address the scalability, privacy, and interoperability challenges inherent in traditional healthcare data management. By separating encrypted data from the blockchain and storing only content hashes on-chain, the model achieves cost efficiency and compliance with data protection regulations. Smart contracts ensure role-based, consent-driven access control while providing transparent audit trails for each interaction. The framework's design aligns with current healthcare standards such as FHIR and considers ethical factors like patient autonomy and digital inclusivity. Although implementation remains future work, this model lays a strong foundation for developing secure, decentralized, and regulation-aware healthcare data ecosystems.

REFERENCES

[1] R. Zhang, "Security and Privacy for Healthcare Blockchains," IEEE Transactions on Services Computing, 2021. [Online]. Available: https://arxiv.org/abs/2106.06136.va

[2] A. D. Dwivedi, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT," Sensors, vol. 19, no. 2, 2019. [Online]. Available: https://doi.org/10.3390/s19020326.

[3] C. Esposito, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" IEEE Cloud Computing, vol. 5, no. 1, 2018. [Online]. Available: https://doi.org/10.1109/MCC.2018.011791712.

[4] M. Kaur, "IPFS: An Off-Chain Storage Solution for Blockchain," Proceedings of the International Conference on Recent Innovations in Computing, 2023. [Online]. Available: https://doi.org/10.1007/978-981-19-9876-8_39.

[5] T. Hardin, "Blockchain in Health Data Systems: A Survey," Proceedings of the BCCA 2019 Conference, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8939174.

[6] J. Jayabalan and N. Jeyanthi, "Scalable Blockchain Model Using Off-Chain IPFS Storage for Healthcare Data Security and Privacy," Journal of Parallel and Distributed Computing, vol. 164, pp. 152–167, 2022. [Online]. Available: https://doi.org/10.1016/j.jpdc.2022.03.009.

[7] B. Zaabar, "HealthBlock: A Secure Blockchain-Based Healthcare Data Management System," Computer Networks, vol. 200, art. 108500, 2021. [Online]. Available: https://doi.org/10.1016/j.comnet.2021.108500.

[8] K. Miyachi, "hOCBS: A Privacy-Preserving Blockchain Framework for Healthcare Data," Information Processing and Management, vol. 58, art. 102535, 2021. [Online]. Available: https://doi.org/10.1016/j.ipm.2021.102535.

[9] S. Chenthara, "Healthchain: A Novel Framework on Privacy Preservation of Electronic Health Records Using Blockchain," PLOS ONE, vol. 15, no. 12, 2020. [Online]. Available: https://doi.org/10.1371/journal.pone.0243043.

[10] Kumar, R., Marchang, N., & Tripathi, R. (2020). *Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain*. In Proceedings of the 2020 International Conference on Communication Systems & Networks (COMSNETS) (pp. 1–5). IEEE. https://doi.org/10.1109/COMSNETS48256.2020.9027313

[11] M. Tcholakian, K. Gorna, M. Laurent, H. Kaffel Ben Ayed, and M. Naghmouchi, "Self-Sovereign Identity for Consented and Content-Based Access to Medical Records using Blockchain," arXiv, 2024. [Online]. Available: https://arxiv.org/abs/2407.21559.

[12] Bender, D., Sartipi, K.: "HL7 FHIR: An Agile and Restful Approach to Healthcare Information Exchange." In: Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems, pp. 326–331 (2013). https://doi.org/10.1109/CBMS.2013.6627810.

[13] Buterin, V., Griffith, V.: "Casper the Friendly Finality Gadget." arXiv preprint arXiv:1710.09437 (2017).

[14] Cisneros, B., Ye, J., Park, C.H., Kim, Y.: "CoviReader: Using IOTA and QR Code Technology to Control Epidemic Diseases Across the US." In: 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0610–0618. IEEE (2021). https://doi.org/10.1109/CCWC51732.2021.9376093.

[15] Donawa, A., Orukari, I., Baker, C.E.: "Scaling Blockchains to Support Electronic Health Records for Hospital Systems." In: 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0550–0556. IEEE (2019). https://doi.org/10.1109/UEMCON47517.2019.8993101.

[16] Filecoin: "Filecoin - A Decentralized Storage Network Designed to Store Humanity's Most Important Information." (2017). https://filecoin.io.

[17] Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., He, J.: "BlocHIE: A Blockchain-Based Platform for Healthcare Information Exchange." In: 2018 IEEE International Conference on Smart Computing (Smartcomp), pp. 49–56. IEEE (2018). https://doi.org/10.1109/SMARTCOMP.2018.00073.

[18] Kiayias, A., Russell, A., David, B., Oliynykov, R.: "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol." In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10401, pp. 357–388. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_12.

[19] Kordestani, H., Barkaoui, K., Zahran, W.: "HapiChain: A Blockchain-Based Framework for Patient-Centric Telemedicine." In: 2020 IEEE 8th International Conference on Serious Games and Applications for Health (SeGAH), pp. 1–6. IEEE (2020). https://doi.org/10.1109/SeGAH49190.2020.9201726.

[20] Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A.: "Blockchain for Secure EHRS Sharing of Mobile Cloud-Based E-Health Systems." IEEE Access 7, 66792–66806 (2019). https://doi.org/10.1109/ACCESS.2019.2917555.

[21] Ranjan, P., Srivastava, S., Gupta, V., Tapaswi, S., Kumar, N.: Decentralised and distributed system for organ/tissue donation and transplantation. In: 2019 IEEE Conference on Information and Communication Technology, pp. 1–6. IEEE (2019). https://doi.org/10.1109/CICT48419.2019.9066225

[22] Seliem, M., Elgazzar, K.: BioMT: blockchain for the internet of medical things. In: 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), pp. 1–4. IEEE (2019). https://doi.org/10.1109/BlackSeaCom.2019.8812784

[23] Szabo, N.: Formalizing and securing relationships on public networks. First Monday (1997). https://doi.org/10.5210/fm.v2i9.548

[24] Liu Y, Ma Z, Liu X, Ma S, Ren K (2019) Privacy-preserving object detection for medical images with faster R-CNN. IEEE Trans Inf Forensics Secur 17:69–84

[25] Do, H.G., Ng, W.K.: Blockchain-based system for secure data storage with private keyword search. Processing—2017 IEEE 13th World Congress Services Services 2017, pp. 90–93. (2017) https://doi.org/10.1109/SERVICES.2017.23

[26] Kumar, S., Bharti, A.K., Amin, R.: Decentralized secure storage of medical records using Blockchain and IPFS: a comparative analysis with future directions. Secur. Priv. 4(5) (2021). https://doi.org/10.1002/spy2.162

[27] Dimitrov, D.V.: Blockchain applications for healthcare data management. Healthc. Inform. Res. 25(1), 51–56 (2019). https://doi.org/10.4258/hir.2019.25.1.51

[28] Henry, R., Herzberg, A., Kate, A.: Blockchain access privacy: challenges and directions. IEEE Secur. Priv. 16(4), 38–45 (2018). https://doi.org/10.1109/MSP.2018.3111245

[29] Eberhardt, J., Heiss, J.: Off-chaining Models and Approaches to Off-chain Computations, pp. 7–12. ISBN: 9781450361101

[30] Gao, H., Ma, Z., Luo, S., Xu, Y., Wu, Z.: BSSPD: a blockchain-based security sharing scheme for personal data with fine-grained access control. Wirel. Commun. Mob. Comput. 2021(2021). https://doi.org/10.1155/2021/6658920.