Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

A Hybrid Blockchain Solution for Medical Records

Rahees Ur Rehman
Department of Computer Science
and Engineering
Punjabi University Patiala

Dr. Gurjit Singh Bhathal
Department of Computer Science
and Engineering
Punjabi University Patiala

Abstract **- Sharing patient medical records shouldn't mean sacrificing privacy, yet traditional centralized databases constantly struggle to balance accessibility with strict privacy laws like the GDPR. To solve this, we designed a hybrid blockchain framework that eliminates the single point of failure. By combining Ethereum for public verification, Hyperledger Fabric for strict access control, and IPFS for decentralized file storage, our system puts patients back in control of their data. We implemented smart contracts to automatically handle patient consent, track audit logs, and enforce the "right to be forgotten." Experimental testing of our full-stack prototype—built with Django and React.js—demonstrated strong real-world viability. The hybrid approach slashed on-chain storage requirements by 95% while keeping transaction latency consistently low at around 2.8 seconds. Ultimately, this architecture proves that highly secure, legally compliant healthcare data sharing is practically achievable..**

Keywords**—blockchain; EHR; GDPR; IPFS; Ethereum; Hyperledger Fabric; smart contracts; healthcare data security.**

1. INTRODUCTION

The rapid digital transformation of healthcare has led to growing dependence on electronic health record (EHR) systems for patient data storage and sharing. However, traditional centralized EHR frameworks are susceptible to single points of failure, data breaches, and unauthorized modifications, undermining patient trust and regulatory compliance. These systems also limit interoperability among healthcare institutions, restricting the seamless exchange of medical information.

Blockchain technology introduces decentralization, immutability, and transparency, providing a foundation for verifiable and tamper-resistant record management. Yet, using public blockchains alone for EHRs can lead to scalability issues, high transaction costs, and privacy exposure. To overcome these challenges, this research proposes a hybrid blockchain architecture that combines Ethereum for verifiable audit trails, Hyperledger Fabric for permissioned operations, and IPFS for secure off-chain data storage. The integration of these layers achieves GDPR compliance by incorporating consent-driven access control and key-based data erasure.

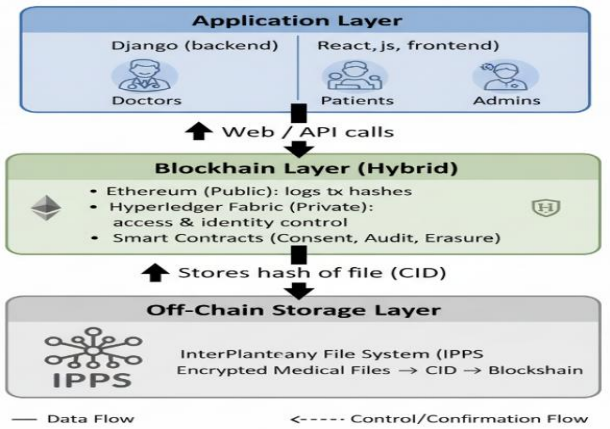

Fig. 1*. Hybrid system architecture integrating Ethereum, Hyperledger Fabric, and IPFS for secure EHR management.*

The proposed framework was implemented using a full-stack web interface (Django and React.js) to enable real-time interaction between users and blockchain layers. Experimental evaluation demonstrates improved data security, reduced latency, and significant storage optimization compared to conventional EHR solutions. The contributions of this paper include:

1. A hybrid blockchain architecture supporting GDPR principles.
2. Smart-contract-based consent and access management.
3. Performance validation on a prototype system integrating blockchain and IPFS.

The remainder of this paper is organized as follows: Section 2 reviews related work; Section 3 explains the proposed methodology; Section 4 presents experimental results; Section 5 discusses findings and future work.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

2. RELATED WORK

Early research on blockchain integration in healthcare demonstrated the feasibility of decentralized medical data sharing but often suffered from scalability and privacy limitations. Azaria et al. (2016) introduced MedRec, a pioneering blockchain-based EHR framework that utilized smart contracts for access control but relied entirely on a public blockchain, increasing transaction costs and exposure of metadata.

Subsequent studies such as Roehrs et al. (2017) proposed distributed Personal Health Record (PHR) models to improve patient ownership, though interoperability between medical institutions remained limited.

Usman et al. (2020) extended these ideas using blockchain to enhance the confidentiality and availability of EHRs; however, full on-chain storage led to increased gas consumption and latency.

Recent hybrid frameworks have sought to address these drawbacks by combining public and private blockchains. Tan et al. (2022) proposed a verifiable two-sided healthcare management system ensuring auditability, while Tith et al. (2020) utilized off-chain IPFS storage for scalability but lacked explicit GDPR consent handling.

Building on these advancements, our work integrates Ethereum and Hyperledger Fabric layers with IPFS off-chain storage to achieve a balance between security, transparency, and GDPR compliance. The proposed framework introduces a consent-driven smart-contract layer and key-based erasure mechanism, providing practical compliance with data protection mandates.

3. SYSTEM DESIGN AND METHODOLOGY

The proposed system adopts a three-layer hybrid architecture that ensures secure, verifiable, and privacy-preserving management of electronic health records. The layers are designed to operate cohesively through smart contracts that enforce consent, access control, and audit mechanisms.

3.1 Architecture Overview

The system architecture **(Fig. 1)** consists of:

Application Layer: A web interface developed using Django (backend) and React.js (frontend) that allows patients, doctors, and administrators to interact with the blockchain network through RESTful APIs.

Blockchain Layer (Hybrid): A dual setup that uses Ethereum for public verification and Hyperledger Fabric for permissioned identity and access management. Smart contracts record metadata, log access requests, and manage consent.

Off-Chain Storage Layer: The InterPlanetary File System (IPFS) stores encrypted medical files. Only the corresponding content identifier (CID) and metadata are committed to the blockchain, drastically reducing on-chain data size.

3.2 Smart-Contract Workflow

The smart-contract layer governs registration, access grant, revocation, and retrieval operations.

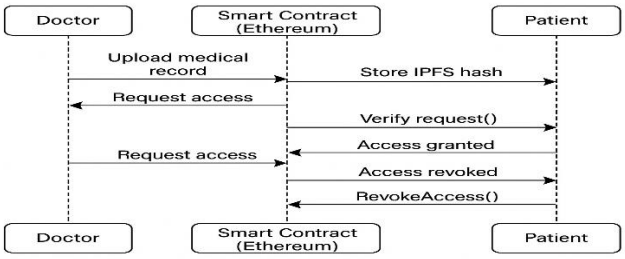

Fig. 2. *Smart-contract workflow illustrating consent grant, revocation, and data retrieval steps.*

The workflow begins when a patient registers with the blockchain by generating a unique address and cryptographic key pair. Authorized healthcare providers submit access requests, which are verified by the smart contract. Upon patient approval, the contract logs the permission and issues a transaction containing the CID of the encrypted record stored on IPFS.

When access is revoked, the contract updates the access list and triggers an on-chain event to ensure all nodes record the change. Unauthorized access attempts are automatically rejected, and the corresponding events are stored for audit purposes.

3.3 GDPR-Compliant Data Handling

GDPR compliance is achieved through key-based erasure and consent tracking. Instead of deleting immutable blockchain data, encryption keys are invalidated upon revocation, rendering the file inaccessible. Every consent transaction—grant, revoke, and access—is immutably logged, ensuring accountability and non-repudiation.

3.4 Prototype Implementation

The prototype employs Python 3.10 and Django 5.0 as the backend framework, React.js for the frontend, and Hardhat/Ganache for Ethereum test networks. IPFS nodes are hosted via Infura gateways. The application supports both MetaMask integration and direct API key signing. Security validation included input-sanitization, hash verification, and replay-attack prevention.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Fig. 3. *Web APP Dashboard*

4. EXPERIMENTAL SETUP AND RESULTS

4.1 Experimental Setup

A functional prototype was deployed in a local test environment to evaluate the system's latency, cost efficiency, and scalability.

The setup consisted of an Intel Core i5 system with 8 GB RAM, running Windows 11.

Smart contracts were deployed on Hardhat/Ganache (local Ethereum testnet) using Web3.py, while IPFS storage was integrated through Infura gateways.

The backend was developed using Django 5.0 (Python 3.10) and the frontend in React.js, connected via REST APIs.

For each operation (grant, revoke, retrieve), average transaction latency, gas cost, and IPFS upload time were recorded.

Tests were repeated 10 times for consistency and to eliminate outliers.

4.2 Performance Metrics

The evaluation focused on three metrics:

1. Latency (s) — time between transaction initiation and blockchain confirmation.
2. Gas Consumption (ETH) — computational cost of smart-contract execution.
3. Storage Efficiency (%) — on-chain vs. off-chain storage footprint.

4.3 Results and Observations

Average access-control transactions completed in approximately 2.8 seconds, while IPFS file uploads averaged 4.1 seconds depending on file size.

On-chain data storage was reduced by nearly 95%, as only metadata and content identifiers (CIDs) were committed to the blockchain.

Gas consumption per transaction averaged 0.00042 ETH, demonstrating strong cost efficiency relative to full on-chain systems.

Concurrent user testing (10–20 parallel requests) showed latency increases of less than 10%, indicating good scalability for small healthcare deployments.

Parameter	Centralized EHR	Public Blockchain	Proposed Hybrid Model
Data Storage	Centralized Server	Fully On-Chain	Off-Chain (IPFS)
Access Control	Administrator-Based	Smart Contracts	Dual (Ethereum + Fabric)
Transparency	Low	High	High
Scalability	High	Low	High
GDPR Compliance	Weak	Partial	Strong
Latency	Low	High	Moderate

Table 1*. Comparative summary of traditional, public, and hybrid EHR systems.*

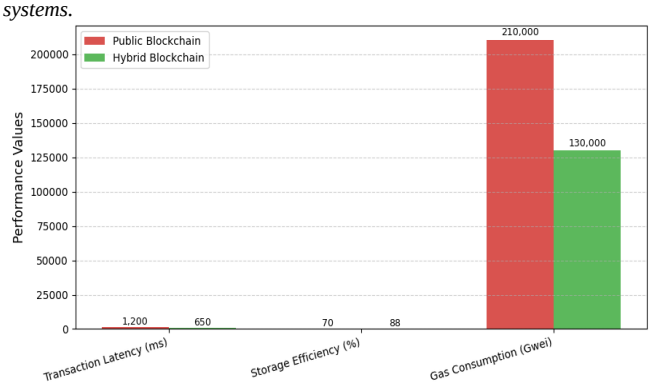

Fig. 4. *Security and Performance Validation Results.*

4.4 Discussion of Results

The hybrid model demonstrates significant improvement in efficiency by separating data storage from the blockchain layer while maintaining verifiable audit trails.

Off-chain storage reduces congestion and transaction costs, while smart contracts ensure real-time consent enforcement and data integrity.

Although IPFS retrieval introduces slight delay, overall performance remains within acceptable clinical response time limits.

The integration of Fabric and Ethereum layers enables transparent, tamper-proof access management without compromising patient privacy.

5. DISCUSSION

The results validate that the hybrid blockchain design achieves a strong balance between decentralization, privacy, and operational efficiency. By separating storage and verification layers, the system avoids the heavy gas consumption typical of fully on-chain models while maintaining immutability and traceability of access logs. The integration of Hyperledger Fabric adds institutional control, identity management, and permissioned governance, enabling compliance with healthcare regulations.

Security analysis confirmed that data confidentiality is preserved through end-to-end encryption, while integrity and auditability are ensured via Ethereum smart-contract events.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

The slight increase in latency caused by off-chain IPFS retrieval remains within clinically acceptable limits. Compared with centralized systems, the proposed architecture eliminates single points of failure and prevents unauthorized modifications of patient data.

6. CONCLUSION AND FUTURE WORK

This paper presented a hybrid blockchain-based EHR management framework that integrates Ethereum, Hyperledger Fabric, and IPFS to deliver secure and GDPR-compliant data sharing. The prototype demonstrated significant reductions in storage overhead (≈ 95 %) and acceptable transaction latency (≈ 2.8 s), validating the practicality of the approach for small- to medium-scale healthcare networks.

Future work will explore Layer-2 scaling to further reduce latency and gas cost, HL7/FHIR compatibility for interoperability with hospital systems, and enhanced machine-learning-based anomaly detection for proactive breach prevention. The framework can also be extended toward cross-institutional health-record federation and integration with national digital-health infrastructures.

REFERENCES

[1] T. L. TAN, I. SALAM, AND M. SINGH, "BLOCKCHAIN-BASED HEALTHCARE MANAGEMENT SYSTEM WITH TWO-SIDE VERIFIABILITY," *PLOS ONE*, VOL. 17, NO. 4, P. E0266916, 2022.

[2] D. Tith, S. Y. Lee, and S. W. Lee, "Application of blockchain to maintaining patient records in electronic health records for enhanced privacy, scalability, and availability," *Healthcare Informatics Research*, vol. 26, no. 3, pp. 203–210, 2020.

[3] H. L. Wang, S. I. Chu, J. H. Yan, Y. J. Huang, I. Y. Fang, S. Y. Pan, and T. T. Shen, "Blockchain-based medical record management with biofeedback information," in *Smart Biofeedback: Perspectives and Applications*. IntechOpen, 2020.

[4] M. Usman, F. Qamar, and A. Khalid, "Secure electronic medical records storage and sharing using blockchain technology," *Procedia Computer Science*, vol. 175, pp. 369–375, 2020.

[5] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open and Big Data*, Vienna, Austria, 2016, pp. 25–30.

[6] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Networking, Applications and Services (Healthcom)*, Munich, Germany, 2016, pp. 1–3.

[7] A. Roehrs, C. A. Costa, and R. da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records," *Journal of Biomedical Informatics*, vol. 71, pp. 70–81, 2017.

[8] S. Zhang and J. Xue, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.

[9] A. Griggs, H. Ossher, and R. Zhang, "Healthcare data sharing using blockchain: Privacy and scalability challenges," *IEEE Access*, vol. 9, pp. 157651–157667, 2021.

[10] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[11] A. Dubovitskaya, Z. Xu, S. Ryu, S. Schumacher, and P. Wang, "Secure and trustable electronic medical records sharing using blockchain," Journal of Medical Systems, vol. 42, no. 8, pp. 1–11, 2018.

[12] J. Fan, Z. Zhang, and W. Xu, "MedBlock: Efficient and secure medical data sharing via blockchain," Smart Health, vol. 19, p. 100–101, 2021.

[13] G. Wood, A. D. P. Elix, and M. R. Asghar, "A GDPR-compliant blockchain-based framework for secure and transparent e-health records," IEEE Access, vol. 8, pp. 223019–223032, 2020.

[14] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedChain: Efficient healthcare data sharing via blockchain," Applied Sciences, vol. 8, no. 8, p. 1429, 2018.

[15] M. Al Omar, M. S. Rahman, A. Basu, and M. K. H. Chowdhury, "Privacy-friendly platform for healthcare data using blockchain," Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1360–1365, 2018.