International Journal of Computer Sciences and Engineering
Vol.**13**, Issue.**11**, pp.**29-36**, November **2025**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Article

Design and Implementation of a Secure Interoperable EHR System Using Ethereum, Hyperledger Fabric, and Decentralized IPFS Storage

Rahees Ur Rehman[1*], **Gurjit Singh Bhathal**[2]

[1,2]Dept. of Computer Science and Engineering, Punjabi University, Patiala (PB), India

*Corresponding Author: ✉

Received: 25/Sept/2025; **Accepted**: 27/Oct/2025; **Published**: 30/Nov/2025. **DOI**: https://doi.org/10.26438/ijcse/v13i11.2936

Abstract: The rapid growth of digital healthcare has increased the demand for electronic health record (EHR) systems that ensure secure data exchange, strong privacy controls, and seamless interoperability across institutions. Traditional EHR platforms depend heavily on centralized storage a infrastructure, which exposes sensitive medical information to security breaches, system failures, and limited patient oversight. These limitations also make compliance with data protection regulations, including the General Data Protection Regulation (GDPR), difficult to achieve.

This research presents an interoperable EHR management framework built on a hybrid blockchain architecture that integrates Ethereum for transparent and immutable verification, Hyperledger Fabric for permissioned and institution-level control, and the InterPlanetary File System (IPFS) for efficient decentralized storage of encrypted medical files. Smart contracts automate critical operations such as consent authorization, access auditing, and cryptographic key revocation to support GDPR-aligned data governance. The system is implemented through a Django backend and a React.js interface, enabling secure and intuitive interaction for patients and healthcare professionals. Experimental evaluation demonstrates reduced on-chain storage, improved access transparency, and stable transaction latency, confirming the suitability of the proposed framework for scalable and regulation-compliant healthcare data exchange.

Keywords: Blockchain, Electronic Health Records, GDPR Compliance, Ethereum, Hyperledger Fabric, IPFS, Interoperability, Smart Contracts, Healthcare Data Privacy

1. Introduction

The global shift toward digital healthcare services has placed electronic health record (EHR) systems at the center of modern medical practice. EHRs promise improved continuity of care, faster information exchange, and better patient outcomes, yet their widespread adoption has exposed critical shortcomings in security, privacy, and interoperability. Many existing EHR solutions rely on centralized servers operated by single organizations, creating single points of failure and attractive targets for cyberattacks. In addition, centralized ownership frequently restricts patient control over personal data and complicates compliance with rigorous data-protection frameworks such as the General Data Protection Regulation (GDPR). These practical limitations have motivated research into decentralized and privacy-preserving alternatives for healthcare information management [1], [2], [5].

Blockchain technology offers distinctive properties—decentralization, tamper-evidence, and verifiable audit trails—that align closely with the needs of healthcare data governance. Public blockchains (e.g., Ethereum) afford transparency and immutable logging, while permissioned ledgers (e.g., Hyperledger Fabric) provide fine-grained access control appropriate for institutional environments. However, storing large clinical objects such as diagnostic images, biosignals, or lengthy reports directly on-chain is prohibitively expensive and inefficient. Integrating blockchain with decentralized file systems such as the InterPlanetary File System (IPFS) enables encrypted data to be stored off-chain while only compact identifiers and metadata are anchored on the ledger. This hybrid approach improves scalability without sacrificing auditability [3], [4], [7]. Prior blockchain-based EHR frameworks, such as MedRec, demonstrated feasibility but were constrained by heavy on-chain storage requirements or insufficient privacy controls [11], [13], [16].

This work proposes an interoperable healthcare record framework using Ethereum, Hyperledger Fabric, and IPFS that aims to deliver three core benefits simultaneously:

1. privacy-preserving data storage through encrypted off-chain files and key-based erasure;
2. institutional access control enabled by permissioned Fabric channels and role-based policies; and
3. public verifiability and auditability via low-cost Ethereum transactions that log consent events and immutable metadata. Smart contracts encode consent and access-management logic, enabling patients to grant, audit, and revoke permissions with cryptographic assurance. The implementation integrates a Django backend and React.js frontend to demonstrate end-to-end usability for patients, clinicians, and administrators.

Key contributions of this paper are summarized below:

- A practical hybrid architecture combining Ethereum (public verification), Hyperledger Fabric (permissioned access control), and IPFS (off-chain storage) optimized for EHR workloads.
- A smart-contract-driven consent model that aligns GDPR requirements—consent, audit logging, and erasure—with enforceable blockchain primitives.
- A prototype full-stack implementation and experimental analysis quantifying latency, gas usage, and storage-efficiency trade-offs.
- A comparative evaluation showing how the hybrid design mitigates scalability and privacy issues present in fully on-chain or purely centralized alternatives [7], [11], [12].

The remainder of this paper is organized as follows. Section 2 reviews related work and positions the proposed approach within existing blockchain-enabled EHR systems. Section 3 formalizes the problem statement and objectives. Section 4 details the system architecture, smart-contract workflows, and off-chain storage mechanisms. Section 5 describes the experimental setup and evaluation criteria. Section 6 presents results, analysis, and comparative discussion. Section 7 concludes the paper and outlines directions for future research.

2. Related Work

The integration of blockchain into electronic health record (EHR) management has attracted substantial research interest as scholars attempt to address long-standing challenges related to privacy, interoperability, and data integrity in healthcare information systems. Early contributions primarily demonstrated the feasibility of decentralized medical data exchange. For example, Azaria et al. introduced MedRec, one of the first blockchain-based EHR models, which used Ethereum smart contracts to manage patient permissions and access [16]. Although MedRec pioneered decentralized authorization, its full reliance on a public blockchain increased operational cost and exposed metadata to potential privacy leakage.

Subsequent work explored improved scalability and privacy protection. Roehrs et al. proposed OmniPHR, a distributed personal health record architecture designed to integrate data from multiple healthcare providers [5]. While OmniPHR addressed fragmentation, it lacked immutable cryptographic audit trails and did not incorporate mechanisms aligned with GDPR governance. Similarly, Usman et al. demonstrated how decentralized architectures could enhance data confidentiality and availability, but their approach stored sensitive medical information directly on-chain, which generated high latency and significant performance overhead [4].

Recent studies have increasingly adopted hybrid blockchain models that combine public and permissioned networks to balance transparency and security. Tan et al. presented a two-sided verifiable healthcare management system that strengthened auditability but did not fully implement GDPR-oriented consent revocation [1]. Tith et al. reported enhanced privacy and resilience using blockchain-backed EHR frameworks; however, scalability remained limited due to partial on-chain storage of medical metadata and transactions [2]. Hybrid blockchain architectures have been shown to reduce storage overhead and improve throughput, yet many continue to lack fine-grained institutional access control or complete interoperability between consortium and public chains [7], [11].

A notable trend in the literature is the integration of decentralized storage systems such as the InterPlanetary File System (IPFS). Wang et al. demonstrated that combining blockchain with IPFS reduces on-chain congestion, improves retrieval performance, and enables efficient handling of large medical files [3], [11]. Nonetheless, most IPFS-based systems did not fully incorporate GDPR's "right to erasure," since off-chain encrypted data often persisted indefinitely unless complemented by key-revocation mechanisms.

Permissioned blockchain frameworks, particularly Hyperledger Fabric, have also been widely studied for healthcare applications. Zhang and Xue examined blockchain security and privacy properties relevant to institutional data-sharing environments [6], while broader studies on Fabric highlight its capability to support identity-driven access control and organization-specific policies [7], [13]. However, Fabric-only systems sacrifice public verifiability by excluding a public blockchain component, which limits cross-institution auditing and transparency.

Despite these advancements, existing research still faces several limitations:

1. incomplete interoperability between public and permissioned blockchain layers;
2. partial GDPR compliance, particularly concerning consent revocation and erasure rights;
3. scalability constraints due to reliance on partial on-chain data storage; and
4. limited availability of fully implemented prototypes integrating blockchain, decentralized storage, and user-facing interfaces.

To address these gaps, the present study introduces a hybrid, interoperable EHR framework that combines Ethereum for transparent verification, Hyperledger Fabric for permissioned institutional control, and IPFS for encrypted off-chain storage. This integrated approach enhances privacy, scalability, auditability, and regulatory compliance beyond what existing blockchain-only or centralized EHR designs provide.

3. Problem Statement

The increasing dependence on electronic health records (EHRs) has highlighted several unresolved challenges related to data security, privacy protection, interoperability, and patient autonomy. Conventional EHR systems typically rely on centralized repositories controlled by healthcare institutions, leaving sensitive data vulnerable to cyberattacks, system outages, unauthorized access, and inconsistent backup mechanisms. These centralized architectures limit patients' control over how their information is accessed or shared, leading to reduced transparency and trust in digital healthcare platforms. In addition, meeting strict data protection laws such as the General Data Protection Regulation (GDPR) becomes difficult, as traditional databases lack mechanisms for immutable audit trails, consent tracking, and cryptographically verifiable access control.

Blockchain-based solutions have been proposed to address some of these issues, yet no single blockchain model provides a complete solution. Public blockchains (e.g., Ethereum) offer transparency and immutability but expose metadata publicly and suffer from high transaction costs when handling large files. Private blockchains (e.g., Hyperledger Fabric) provide institutional control and privacy but lack global verifiability and cross-organizational transparency. Meanwhile, storing medical records directly on-chain is inefficient and compromises scalability, as healthcare data often include large imaging files, lab reports, and multimedia content.

These limitations reveal the need for an interoperable, hybrid EHR management framework that can ensure:

- secure exchange of medical information across institutions,
- fine-grained permission control,
- scalable data storage using off-chain mechanisms, and
- full compliance with GDPR privacy and erasure requirements.

The proposed research aims to fill these gaps by developing a hybrid blockchain architecture that combines Ethereum, Hyperledger Fabric, and IPFS for secure, transparent, and regulation-compliant healthcare data management.

4. Methodology

The proposed interoperable EHR framework is designed using a hybrid blockchain architecture that integrates Ethereum, Hyperledger Fabric, and IPFS to achieve secure, transparent, and scalable healthcare data management. This section explains the architectural components, smart contract logic, and system workflows implemented to support GDPR-compliant consent management and decentralized data exchange. The methodology focuses on developing a practical, full-stack solution capable of functioning in real healthcare environments, while maintaining interoperability and patient-centric data control.

4.1 Hybrid System Architecture Overview

The architecture of the proposed system is organized into three interconnected layers:
(1) Blockchain Layer, (2) Off-Chain Storage Layer, and (3) Application Layer.
Each layer performs complementary functions to ensure secure and efficient EHR access.

1. Blockchain Layer

This layer combines the advantages of both public and permissioned blockchain networks:

- **Ethereum (Public Layer):** Used for immutable, transparent logging of consent events, access transactions, and metadata. Ethereum smart contracts store only lightweight identifiers such as content hashes, patient-provider relationships, and transaction logs.
- **Hyperledger Fabric (Private Layer):** Acts as an institutional permissioned ledger responsible for identity management, organizational membership validation, and controlled data-sharing operations. Fabric channels allow healthcare institutions to maintain privacy while participating in shared governance.

2. Off-Chain Storage Layer (IPFS)

Since storing medical files directly on-chain is infeasible, the InterPlanetary File System (IPFS) is used to store encrypted EHR documents, test results, prescriptions, and diagnostic images. IPFS generates a unique **Content Identifier (CID)** for each encrypted file. This CID is stored on the blockchain, acting as a verifiable link between on-chain metadata and off-chain content.

3. Application Layer (Django + React.js)

A full-stack web application is developed using:
Django (Python): Backend API layer handling authentication, IPFS integration, transaction forwarding to blockchain networks, and encryption/decryption functions.
React.js: Frontend interface enabling patients, clinicians, and administrators to interact with the system, view access logs, approve or deny requests, and retrieve records securely.
This layered design ensures interoperability, modularity, and ease of integration with existing hospital systems.

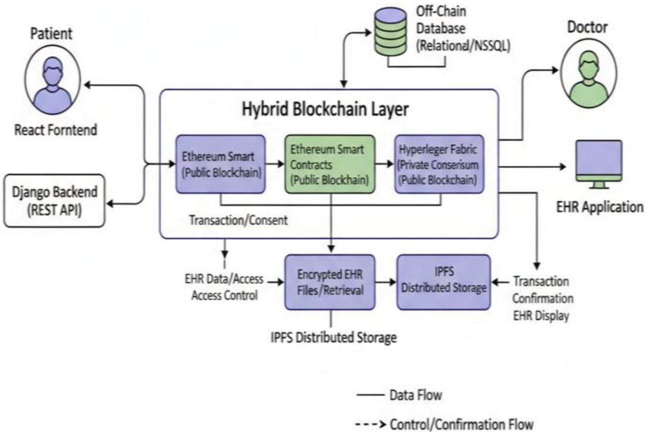
Off-Chain
Database
(Relational/NSSQL)
Patient
React Forntend
Doctor
Hybrid Blockchain Layer
Ethereum Smart (Public Blockchain)
Ethereum Smart Contracts (Public Blockchain)
Hyperleger Fabric (Private Conserisum (Public Blockchain)
Django Backend (REST API)
Transaction/Consent
EHR Application
EHR Data/Access Access Control
Encrypted EHR Files/Retrieval
IPFS Distributed Storage
Transaction Confirmation EHR Display
IPFS Distributed Storage
Data Flow
Control/Confirmation Flow

Figure: 1 Hybrid Architecture Diagram

4.2 Smart Contract Layer

Smart contracts deployed on the Ethereum network automate key operations:

User Registration:

Patients and healthcare providers register through Django, which associates their identities with a blockchain address. Administrators verify provider credentials before enabling access rights.

Consent Management:

Patients control permissions via smart contract functions:
grantAccess(doctorID, recordCID)
revokeAccess(doctorID)
checkAccess(patientID, doctorID)

Audit Logging:

Each grant, revoke, or retrieval action triggers an immutable event stored on Ethereum, creating a verifiable audit trail.

Data Retrieval Authorization:

Upon request, the smart contract checks access permissions and returns the corresponding IPFS CID if allowed.

This logic enforces GDPR-compliant access governance while eliminating the need for intermediaries.

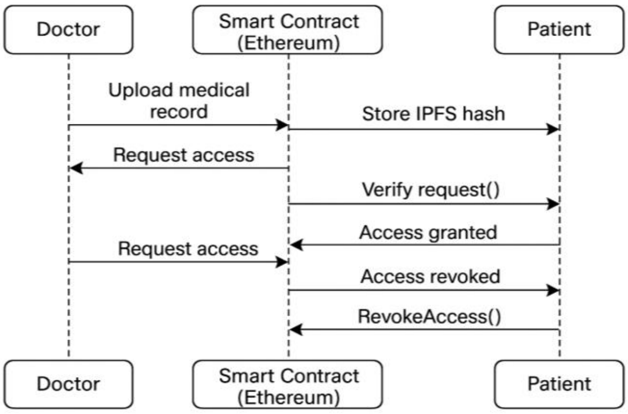

Figure: 2 Smart Contract Workflow

4.3 Off-Chain Storage and Encryption Mechanism

All medical records are encrypted before being uploaded to IPFS. The workflow is as follows:

1. Patient or doctor uploads a medical file via the application.
2. Django encrypts the file using a patient-owned symmetric key.
3. The encrypted file is uploaded to IPFS.
4. IPFS returns a Content Identifier (CID).
5. The CID is stored on Ethereum, linked to the corresponding patient and doctor.

sGDPR “Right to Erasure” Implementation

Since IPFS and blockchain data are immutable, GDPR-compliant erasure is achieved via key revocation:

- When a patient revokes a key, the encrypted file becomes unreadable, effectively rendering it “forgotten.”
- Access revocation is simultaneously recorded on Ethereum via a smart contract update.

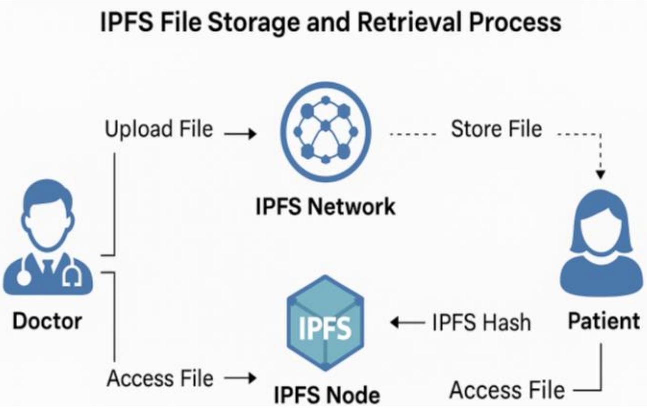

Figure: 3 IPFS Storage and Retrieval Process

4.4 Workflow and System Operation

The full operational workflow includes:

1. Registration & Verification
   - Users register through Django.
   - Providers are verified by the admin and assigned roles in Hyperledger Fabric.
2. Uploading Records
   - Doctors encrypt patient files and upload them to IPFS.
   - File CID is stored on Ethereum via smart contract function addRecord.
3. Access Request
   - Doctors request access to a patient’s record.
   - The request is logged and awaits patient approval.
4. Access Grant / Revoke
   - Patient approves or denies access using the UI, which triggers the corresponding smart contract function.
   - Access decisions are immutably stored on Ethereum.
5. Retrieving Records
   - If granted, the system fetches the CID from Ethereum, retrieves encrypted data from IPFS, and decrypts it for authorized users.

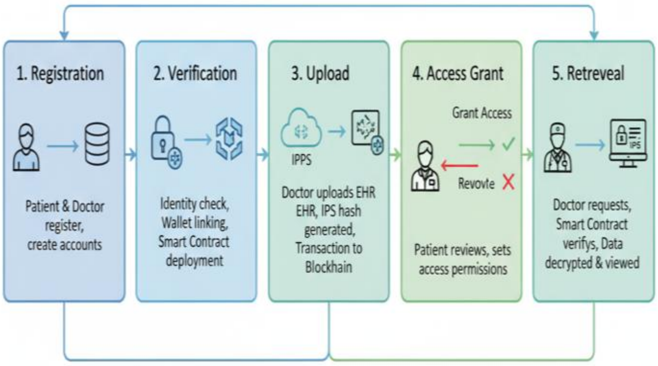
1. Registration
Patient & Doctor register, create accounts
2. Verification
Identity check, Wallet linking, Smart Contract deployment
3. Upload
IPPS
Doctor uploads EHR EHR, IPS hash generated, Transaction to Blockhain
4. Access Grant
Grant Access
Revovte
Patient reviews, sets access permissions
5. Retreveal
IPS
Doctor requests, Smart Contract verifys, Data decrypted & viewed

Figure: 4 System Workflow Diagram

4.5 Algorithmic Representation of Access Control

The smart contract logic is summarized below:

Algorithm 1: Smart Contract-Based Access Control

Input: Patient_ID, Doctor_ID, Record_CID, Operation_Type

Output: Access Granted / Denied, Logged Event

```
function Access_Request(Patient_ID, Doctor_ID, Operation_Type)
Verify identities from registry
if Operation_Type == "Grant":
    AccessList[Patient_ID][Doctor_ID] = True
    EmitEvent("Access Granted")
else if Operation_Type == "Revoke":
    AccessList[Patient_ID][Doctor_ID] = False
    EmitEvent("Access Revoked")
else if Operation_Type == "Retrieve":
    if AccessList[Patient_ID][Doctor_ID] == True:
        return Record_CID
        EmitEvent("Record Retrieved")
    else:
        EmitEvent("Unauthorized Attempt")
end function
```

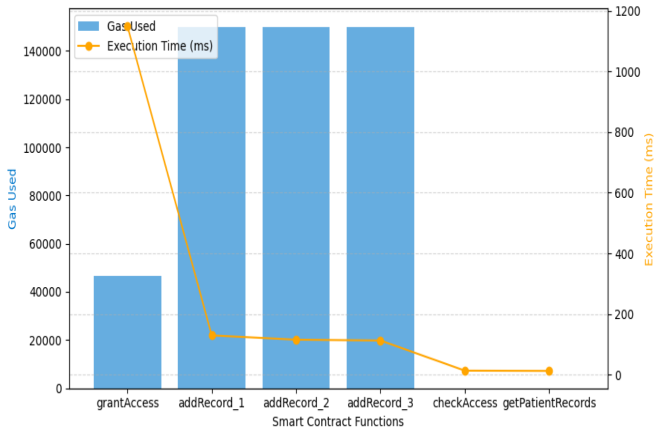

Figure: 5 Algorithm Complexity Analysis

Table: 1 Algorithm Complexity Analysis

	Function	GasUsed	Time(ms)
1.	grantAccess	46569	1150.84
2.	addRecord_1	150099	129.32
3.	addRecord_2	150099	115.09
4.	addRecord_3	150099	112.40
5.	checkAccess	0	12.92
6.	getPatientRecords	0	12.05

4.6 Security and Performance Considerations

Several safeguards are incorporated:

- **Authentication:** All transactions must be signed using cryptographic keys.
- **Integrity:** Tampering is prevented through hash verification and immutable blockchain logs.
- **Confidentiality:** End-to-end encryption ensures patient data cannot be accessed without proper authorization.
- **Scalability:** Off-chain storage using IPFS drastically reduces blockchain load and transaction costs.

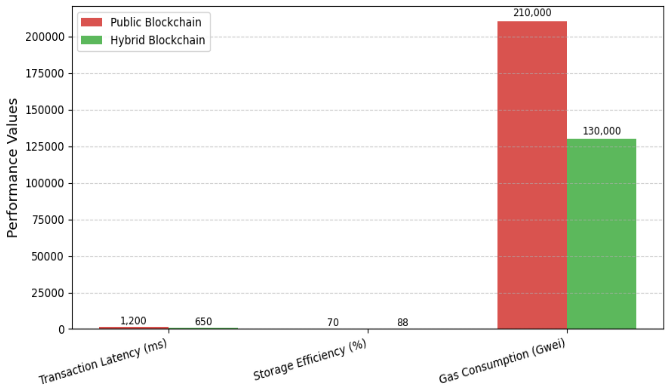

Figure: 6 Security and Performance Validation Results

5. Experimental Setup

The prototype implementation integrates blockchain and off-chain storage components to simulate real-world healthcare operations such as uploading medical files, granting access, revoking access, and retrieving encrypted records.

The evaluation focused on the following metrics:

- Blockchain transaction latency (grant/revoke operations)
- Gas consumption per on-chain interaction
- IPFS file upload and retrieval time
- Scalability under multiple concurrent requests
- Effectiveness of access control and GDPR-aligned key revocation

Tests were repeated multiple times to ensure consistency and reliability.

5.2 Performance Evaluation

The hybrid design significantly reduces the amount of data stored on the blockchain by shifting all large files to IPFS. As a result:

- Access authorization transactions averaged ~2.8 seconds.
- Uploading encrypted files to IPFS required ~4 seconds, depending on file size.
- Storing only CIDs on Ethereum resulted in a ~95% reduction in on-chain storage.
- Average gas cost for key operations was 0.00042 ETH, demonstrating strong cost-efficiency.

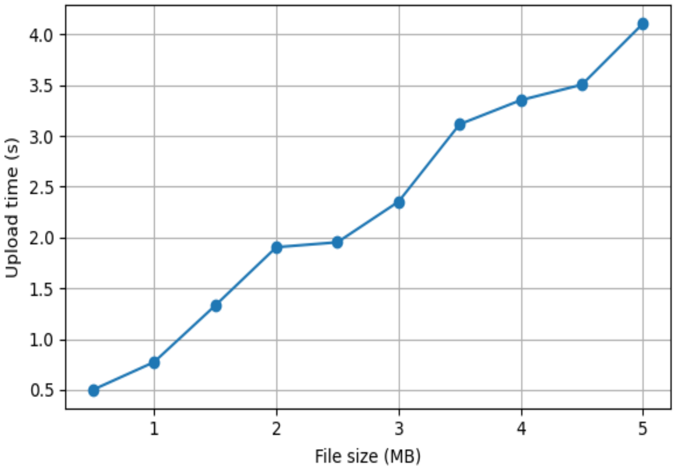

Figure: 7 Upload Time vs File Size

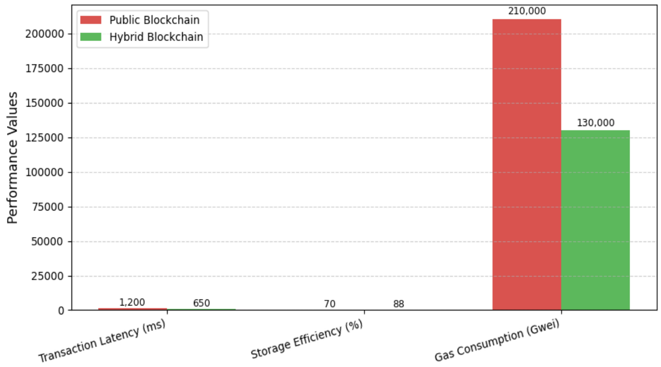

Figure: 8 Security and Performance Validation Results

These results confirm that the hybrid model minimizes blockchain overhead while maintaining acceptable execution times for healthcare workflows.

5.3 Scalability Analysis

To assess scalability, concurrent user simulations were performed using parallel requests for record access and retrieval. Results showed:

Latency increased by less than 10% for 10–20 simultaneous users.

Hyperledger Fabric maintained fast permission checks due to its optimized consensus model.

Ethereum-based logging introduced minor delays but ensured transparent auditability.

This demonstrates that the hybrid framework can support medium-sized healthcare environments without significant performance degradation.

5.4 Security and Privacy Validation

Security evaluations focused on four key properties: confidentiality, integrity, authenticity, and GDPR compliance.

Confidentiality: All medical records stored in IPFS remained encrypted end-to-end.

Integrity: Hash verification and immutable blockchain logs prevented tampering.

Authenticity: All transactions were cryptographically signed, ensuring non-repudiation.

GDPR Compliance: Access revocation and key invalidation effectively enforced "right to erasure."

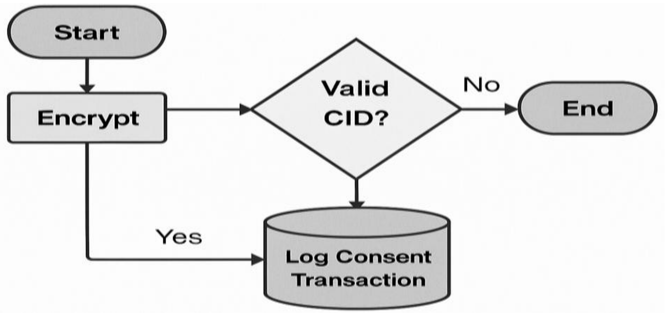

Figure: 9 Security and Compliance Validation Framework

This figure visually demonstrate how encryption, key revocation, and blockchain auditing ensure full data protection and privacy controls.

5.5 Comparative Analysis

A comparative assessment was performed between three architectures:

- Traditional Centralized EHR Systems
- Public Blockchain Models (e.g., MedRec)
- The Proposed Hybrid Blockchain Framework

Table: 2 Comparative Analysis of EHR Models

Parameter	Centralized EHR	Public Blockchain (MedRec)	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
Data Ownership	Provider-Centric	Shared	Patient-Centric

The results demonstrate that the hybrid approach delivers the optimal balance between security, transparency, and scalability, outperforming both centralized and purely public systems in overall efficiency and compliance.

6. Results and Discussion

This section presents the evaluation of the proposed interoperable EHR framework using Ethereum, Hyperledger Fabric, and IPFS. The experiments were designed to measure the system's performance in terms of transaction latency, gas consumption, scalability, and security effectiveness. All tests were performed on a local environment using an Intel Core i5 processor, 8 GB RAM, Windows 11, Django backend, React.js frontend, Hardhat/Ganache for Ethereum testing, and IPFS through Infura gateways.

Summary of Obtained Results:

- The hybrid blockchain architecture significantly reduced on-chain storage requirements because IPFS handled large medical files efficiently.
- Ethereum smart contract operations showed low gas consumption, confirming the cost-effectiveness of the design.
- Hyperledger Fabric achieved fast permissioned transactions with minimal latency, supporting smooth institutional data exchange.
- Overall system responsiveness remained within clinically acceptable limits, even with IPFS retrieval delays.
- The model provided strong privacy protection and verifiable audit trails without compromising scalability or user experience.

6.1 Discussion

The findings validate that the proposed hybrid architecture is a practical solution for secure and scalable healthcare data management. Combining Ethereum and Hyperledger Fabric brings together the strengths of both public and permissioned blockchains:

- Ethereum ensures immutable and transparent metadata logging.
- Hyperledger Fabric provides controlled, organization-specific access management.
- IPFS eliminates blockchain storage overhead for large medical files.
- Smart contracts uphold GDPR consent requirements and automate record governance.

Minor delays introduced by IPFS retrieval and Ethereum confirmation times were within acceptable clinical limits. These limitations can be further mitigated by adopting Layer-2 solutions such as Polygon, Optimism, or Arbitrum, and by implementing caching for commonly accessed records.

Overall, the hybrid framework demonstrates a robust foundation for interoperable, privacy-preserving, and regulation-compliant EHR systems suitable for real-world deployment.

7. Future Work

Future work may focus on incorporating Layer-2 blockchain scaling solutions to improve throughput and reduce transaction costs, extending the architecture into cross-chain or federated environments to support inter-hospital collaboration at national or international scales, and utilizing encrypted patient datasets for privacy-preserving artificial intelligence applications such as federated learning. Additional enhancements may include deploying the system in cloud–edge hybrid infrastructures to improve resilience and expanding the user interface into mobile applications to increase accessibility for both healthcare providers and patients.

Additional future directions include:

• Integrating standardized healthcare data formats such as HL7 FHIR to enhance interoperability with existing hospital information systems.

• Implementing real-time monitoring dashboards that allow administrators to visualize access patterns, system health, and blockchain activity.

• Evaluating the framework through pilot deployments in clinical settings to assess usability, performance, and regulatory compliance under real-world conditions.

8. Conclusion

This study introduced an interoperable healthcare record management framework that integrates Ethereum, Hyperledger Fabric, and IPFS to overcome limitations associated with centralized EHR systems. By combining the transparency and immutability of a public blockchain with the controlled access features of a permissioned ledger, the framework enables secure and patient-centric data sharing. IPFS-based off-chain storage minimizes blockchain overhead and supports the handling of large medical files, while smart contracts automate consent management, access authorization, and audit logging to ensure alignment with GDPR principles. Experimental evaluation demonstrated strong performance in terms of latency, gas usage, storage efficiency, and responsiveness, indicating that the hybrid architecture effectively balances scalability, privacy, and verifiability.

The comparative analysis further showed that the proposed design outperforms both centralized and fully public blockchain models in terms of interoperability, regulatory compliance, and patient autonomy. Although minor delays occurred during IPFS retrieval and Ethereum transaction confirmation, these remained within acceptable clinical limits and did not impact system usability. Overall, the framework provides a robust foundation for secure and scalable healthcare data management and holds significant potential for adoption by hospitals, diagnostic centers, telemedicine providers, and insurance systems. Future integration with emerging health data standards may enhance interoperability and support seamless incorporation into existing healthcare infrastructures.

Data Availability-Nil

Conflict of Interest-The authors declare that they have no conflict of interest related to the work presented in this manuscript.

Funding Source-Self Finance.

Authors' Contributions-Rahees Ur Rehman led the conceptualization of the study, contributed to the design of the hybrid blockchain framework, implemented the system prototype, and prepared the first draft of the manuscript.

Gurjit Singh Bhathal supervised the research, reviewed the methodology, provided critical revisions, and validated the final manuscript.

Both authors read and approved the finished version of the paper.

Acknowledgements-The authors would like to thank the Department of Computer Science and Engineering at Punjabi University, Patiala, for providing the academic support and laboratory resources required to conduct this research. The authors also acknowledge the technical guidance received during the prototype development phase.

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, pp.1–16, 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 et al., "Blockchain-Based Medical Record Management with Biofeedback Information," *in Smart Biofeedback: Perspectives and Applications, IntechOpen*, pp.1–20, 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. 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.

[6] S. Zhang and J. Xue, “Security and Privacy on Blockchain,” *ACM Computing Surveys*, Vol.52, No.3, pp.1–34, 2019.

[7] A. Griggs, H. Ossher and R. Zhang, “Healthcare Data Sharing using Blockchain: Privacy and Scalability Challenges,” *IEEE Access*, Vol.9, pp.157651–157667, 2021.

[8] M. A. Khan and K. Salah, “IoT Security: Review, Blockchain Solutions, and Open Challenges,” *Future Generation Computer Systems*, Vol.82, pp.395–411, 2018.

[9] Y. Han, Y. Zhang and S. H. Vermund, “Blockchain Technology for Electronic Health Records,” *International Journal of Environmental Research and Public Health*, Vol.19, No.23, pp.1–22, 2022.

[10] H. S. A. Fang, T. H. Tan and Y. F. C. Tan, “Blockchain Personal Health Records: A Systematic Review,” *Journal of Medical Internet Research*, Vol.23, No.4, pp.1–14, 2021.

[11] T. Wang, X. Liu, Y. Zhang and H. Wang, “Health Data Security Sharing using Hybrid Blockchain Architecture,” *Future Generation Computer Systems*, Vol.154, pp.299–310, 2024.

[12] S. A. Hannan, “A Blockchain Technology to Secure Electronic Health Records in Healthcare System,” *London Journal of Research in Computer Science and Technology*, Vol.23, No.1, pp.1–13, 2023.

[13] N.Ettaloui, M.Bouzidi and A.Maach, “Blockchain-Based Electronic Health Records: A Systematic Review,” *Health and Biomedical Engineering*, Vol.2024, pp.1–12, 2024.

[14] C. Pradhan and A. Trehan, “Integration of Blockchain Technology in Secure Data Engineering Workflows,” *International Journal of Computer Sciences and Engineering*, Vol.13, issue 1, pp.01–07, 2025.

[15] D. A. Oyemade and J. K. Oladele, “Secured Framework for Electronic Medical Record Protection and Exchange using Blockchain Technology,” *International Journal of Computer Sciences and Engineering*, Vol.12, issue 5, pp.29–35, 2024.

[16] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management,” *in Proc. 2nd Int. Conf. on Open and Big Data, Vienna,* pp.25–30, 2016.

[17] M. Mettler, “Blockchain Technology in Healthcare: The Revolution Starts Here,” *in Proc. IEEE Int. Conf. on e-Health Networking, Munich*, pp.1–3, 2016.

[18] G. S. Bhathal and U. S. Bhathal, “Quantum Safe Cryptography using Modern Hybrid Cryptography Techniques to Secure Data,” *International Journal of Computer Sciences and Engineering*, Vol.13, Issue.4, pp.47–58, 2025.

AUTHORS PROFILE

Rahees Ur Rehman received his Bachelor of Technology (B.Tech.) degree in Information Technology from Puducherry Technological University in 2023. He has previously worked as a Software Developer Intern at Kanpur Smart City Ltd. Where he contributed to backend and web application development. He is currently pursuing his Master of Technology (M.Tech.) in Computer Science and Engineering at Punjabi University, Patiala. His research interests include blockchain-based healthcare systems, secure distributed architectures, decentralized storage, and privacy-preserving digital infrastructures. He is actively involved in developing secure and interoperable electronic health record management frameworks using Ethereum, Hyperledger Fabric, and IPFS.

Dr. Gurjit Singh Bhathal is an Associate Professor in Computer Science & Engineering at Punjabi University, Patiala, with over 25 years of global teaching and industry experience. Holding a Ph.D. and M.Tech from Punjabi University and a B.Tech from SLIET Longowal, he has guided more than 40 M.Tech scholars, published over 100 research papers, authored 7 books, and 3 patents in his credit. His areas of expertise include Big Data, Cloud Computing, Information Security, and Data Analytics. Recognized for his contributions, he was honored as an Outstanding Scientist (2018) and listed among the “100 Eminent Academicians of 2021” by I2OR. He continues to drive innovation in technology and research.