IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure Healthcare Data Systems with Blockchain: A Decentralized Framework for EHR Management

Kalash Malge
BE IT Student
International Institute of Information technology
Pune, India

Deepika Walanjkar
Assistant Professor
International Institute of Information technology

Amit Laware
BE IT Student
International Institute of Information technology

Sujal Jagtap
BE IT Student
International Institute of Information technology

Yash Kabade
BE IT Student
International Institute of Information technology

Abstract: ***Electronic Health Records (EHRs) represent a monumental shift in modern healthcare, yet their centralized storage models remain plagued by fragmented data silos, single points of failure, and a systemic lack of patient authority. This research paper presents a robust, decentralized framework utilizing Hyperledger Fabric and the Interplanetary File System (IPFS) to create a secure, interoperable, and patient-centric healthcare environment. The architecture is structured into a three-tier model comprising presentation, application logic, and decentralized infrastructure. By keeping sensitive medical records encrypted and stored off-chain via IPFS, the system ensures scalability while maintaining the immutability of record pointers on the blockchain. Smart contracts are utilized to automate access control policies, ensuring that patients retain ultimate sovereignty over their medical history. The result is a highly durable and auditable system that mitigates the risks of traditional centralized databases. Experimental results demonstrate improved transaction transparency and high usability for clinicians and patients alike. This framework serves as a foundational step toward an equitable, efficient, and blockchain-enabled healthcare ecosystem.***

Index Terms **– Blockchain, healthcare, EHR management, decentralized system. Hyperledger .**

1.Introduction

The digitization of medical practices has led to the widespread adoption of Electronic Health Records (EHRs), which serve as electronic repositories for vital patient data, including clinical history, lab results, and medication plans. EHRs are fundamental to modern diagnostics, allowing for faster referrals and better-informed clinical decisions. However, the current infrastructure relies heavily on centralized databases, which create significant administrative and technical bottlenecks. Centralization often results in "data signification," where patient data is isolated within a single institution's proprietary software. This fragmentation makes it nearly impossible for physicians at different clinics to access a comprehensive medical history without significant manual effort, leading to redundant tests and delayed emergency care. The lack of real-time synchronization between these silos remains one of the greatest hurdles in urban healthcare management. To address these challenges, this project leverages Distributed Ledger Technology (DLT) to move away from the traditional client-server model. Blockchain provides a shared, immutable ledger that acts as a universal "source of truth." By distributing control across a consortium of trusted nodes (e.g., hospitals, regulatory bodies), we can ensure that medical data remains accessible, secure, and under the direct control of the patient. 1.2 Objective The primary objective of this research is to design and implement a decentralized EHR management system that prioritizes security and patient sovereignty. We aim to eliminate the risks associated with centralized storage, such as unauthorized data tampering and large-scale breaches. By utilizing a hybrid on-chain/off-chain storage model, the system maintains a lightweight blockchain while securing large medical files in a distributed file network. Another core goal is to automate the enforcement of patient consent through smart contracts. In traditional systems, patients often have no say in how their data is shared or monetized. This framework empowers patients with a dedicated mobile application to grant or revoke access permissions in real-time, ensuring that only authorized healthcare providers can retrieve sensitive medical documents. Furthermore, the project strives to enhance interoperability by providing a standardized API gateway. This gateway allows diverse healthcare institutions to communicate through a unified protocol without needing to overhaul their proprietary internal

systems. The objective is to foster a collaborative environment where data flows seamlessly yet securely between authorized nodes in the healthcare consortium. 1.3 Problem Definition Current EHR management is crippled by the proprietary nature of healthcare IT systems, which prevents different hospitals from sharing data effectively. Patients referred from primary care to specialized surgery often find that their previous lab results and history are unavailable to the new provider. This lack of interoperability leads to diagnostic errors and increases the overall cost of treatment due to redundant data collection. Security is the second major pillar of the problem. Centralized databases represent high-value targets for ransomware attacks and data breaches. If a central hospital server is compromised, the privacy of thousands of patients is at risk. Additionally, centralized logs can be altered by insiders, making it difficult to maintain a truly verifiable audit trail of who accessed or modified a specific medical record. Finally, the lack of patient control is a critical ethical and technical issue. In most existing systems, patients are passive recipients of care with no direct influence over their digital footprint. They cannot easily see who has accessed their records or prevent specific providers from viewing history. This absence of agency undermines the trust between the patient and the healthcare institution. 1.4 Purpose The purpose of this project is to redefine the healthcare data landscape by establishing a "Patient-Centric" model. By integrating Hyperledger Fabric and IPFS, we create a system where the patient is the ultimate owner of their data. The blockchain serves as a transparent registry of access logs, while the actual data remains encrypted and distributed, ensuring that no single entity has total control over the records. This project also serves to reduce administrative overhead for healthcare providers. Automating record-sharing requests through blockchain-based permissions eliminates the need for fax-based or manual data transfers. Clinicians can request access and receive it instantly if the patient's smart contract policy allows, significantly speeding up the care delivery process during emergencies. Lastly, the purpose includes future-proofing medical data against emerging threats. By exploring integrations with Federated Learning and Post-Quantum Cryptography, we ensure that the system is not only secure today but resilient against the computational capabilities of future quantum computers. This research-driven approach provides a scalable roadmap for long-term secure healthcare management.

1.5 Scope The scope of this project encompasses the design and development of a full-stack decentralized application (DApp). This includes a three-layered architecture: a presentation layer for user interaction, an application layer for microservices (Node.js), and a decentralized infrastructure layer (Hyperledger Fabric and IPFS). The system supports three primary user roles: patients, clinicians, and hospital administrators. On the infrastructure side, the scope includes the deployment of a consortium blockchain network where multiple hospital nodes participate in consensus. The project covers the implementation of smart contracts for permission management and the development of a cryptography service to handle end-to-end encryption. The integration of IPFS for off-chain storage ensures that the system can handle high-resolution medical images and large datasets. However, the current scope does not include direct integration with legacy hospital billing software or insurance claim processing. It focuses primarily on the secure management and sharing of clinical EHR data. Future iterations may expand this scope to include automated insurance verification and IoT-based real-time health monitoring systems.

1.6 Privacy Concerns and Solutions in EHRs Although blockchain provides integrity, physical storage of sensitive EHR data directly on-chain would be a severe breach of privacy, as the ledger is replicated among the participants. To counteract this, a popular and practical solution is off-chain storage. Under this architecture, the actual EHR files themselves are stored in encrypted form in a decentralized file system such as IPFS (Interplanetary File System). Only the encrypted file's unique, nonmodifiable hash (Content Identifier or CID) is stored on the blockchain. That way, sensitive information is kept off the replicated ledger while employing the blockchain to keep the data's tamper-proof pointer and access log.

Advanced cryptographic techniques provide extra levels of confidentiality. Data is often encrypted through the use of the public key of the patient, thus ensuring that decryption can only be permitted by the patient. To enable data exchange with a healthcare professional, techniques like Proxy Re-encryption can be used that enable secure re-encryption for the purpose of an approved receiver while securing the patient's secret key from disclosure. Additionally, techniques like zero-knowledge proofs (ZKPs) allow verification of certain data features without revealing the actual data itself, hence elevating the level of confidentiality protection measures.

1.7 Interoperability Challenges and Solutions

A. Existing Status of Interoperability within EHR Systems Interoperability is the ability of different health IT systems to exchange and information use remains pertinent problem in healthcare. Data is often locked in proprietary systems (such as Epic or Cerner), and the lack of standardization leads to low interoperability between different institutions. This creates a fragmented view of patient health and impedes collaborative care. While government-mandated standards like Fast Healthcare Interoperability Resources (FHIR) are being developed to create standardized APIs for data access, practical interoperability is still difficult and risky to achieve with current systems. Competitive dynamics and technical integration complexities further exacerbate this issue.

B. How Blockchain Enhances Interoperability Blockchain technology can address these challenges by providing a universal and secure infrastructure for data exchange. It acts as a shared, trusted ledger that different systems can connect to, creating a common ground for data sharing without requiring direct integration between proprietary databases. By storing pointers to off-chain data and managing access permissions through smart contracts, blockchain creates an auditable and standardized method for exchanging health-related data across diverse entities. This has the potential to break data silos, facilitate seamless and streamlined information exchange, and permit healthcare practitioners within many organizations to access safely

2. Literature survey

The literature survey explores the evolution of blockchain in healthcare from early theoretical models to sophisticated hybrid frameworks. Sun et al. (2024) introduced a decentralized system with provenance awareness, utilizing a Directed Acyclic Graph (DAG) for efficient storage. While it improved traceability, the computational overhead of DAG structures poses challenges for real-time applications. Geng et al. (2024) proposed an integrated ecosystem connecting hospitals and insurers, demonstrating blockchain's role in reducing silos but highlighting latency issues in public chains. Deebak and Hwang (2024) developed the CA-DPPF framework, utilizing Hyperledger Fabric and a cloud backend. Their Proof of Trusted Authority (POTA) consensus improved throughput, though the dependency on cloud nodes introduced potential centralization risks. Khan et al. (2025) and Commey et al. (2025) further expanded the field by integrating Federated Learning and Post-Quantum Cryptography, respectively, ensuring privacy-preserving AI and resilience against future quantum attacks.

2.1 Analysis of Foundational Work (Henwise Paper) The literature review conducted by Walanjkar et al. (2025),referred to as the Henwise research paper, serves as the primary theoretical foundation for this project. It identifies immutability, transparency, and cryptographic security as the three core pillars required to solve the failures of centralized EHRs. The Henwise paper emphasizes

the "Patient-Centric" shift, noting that true security is only possible when patients manage their own authorization propagation. Crucially, the Henwise study analyzes the emergence of Federated Learning (FL) for collaborative medical AI without data disclosure. It presents a mathematical model for global weight aggregation in a secure environment. The paper also advocates for the transition to quantum-resistant algorithms (like ML-DSA-65) to protect data that requires decades of confidentiality. This foundational research guided our selection of Hyperledger Fabric for its modularity and support for private channels.

3. Methodology

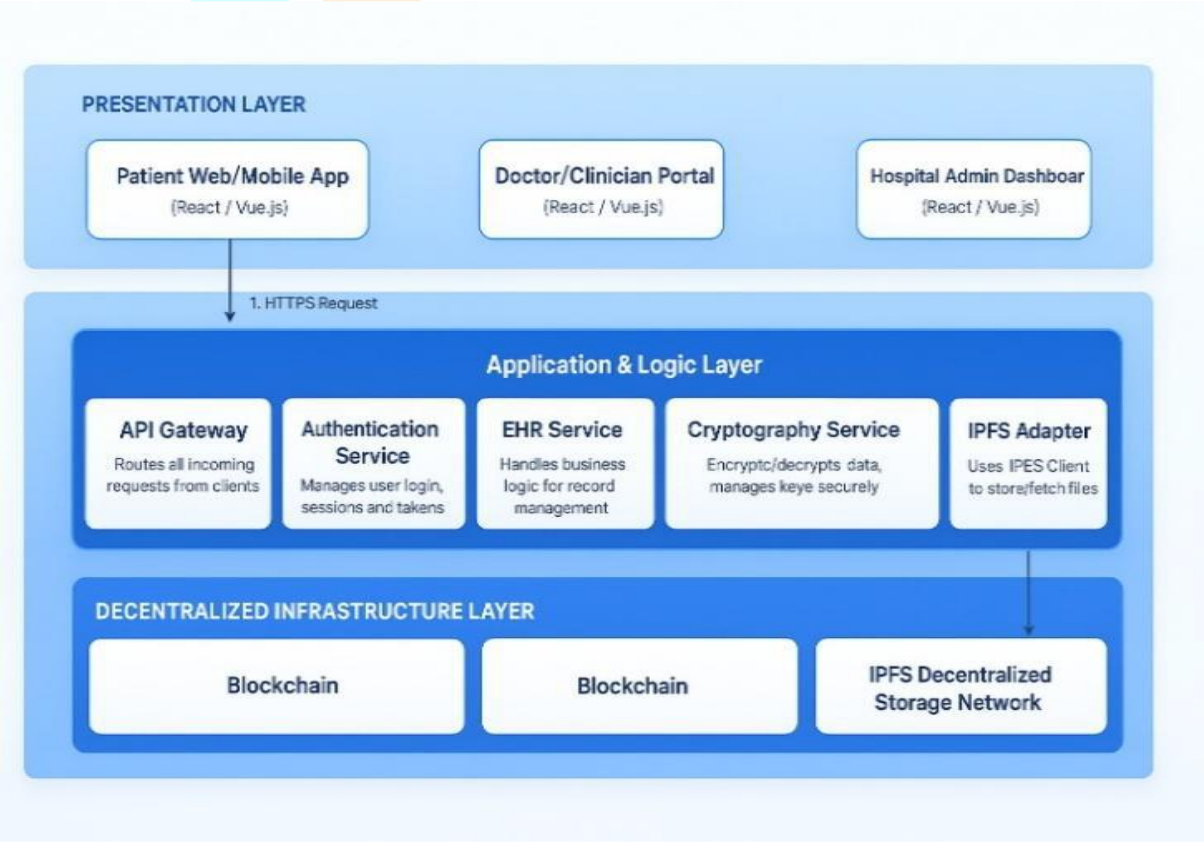
3.1 System Requirements

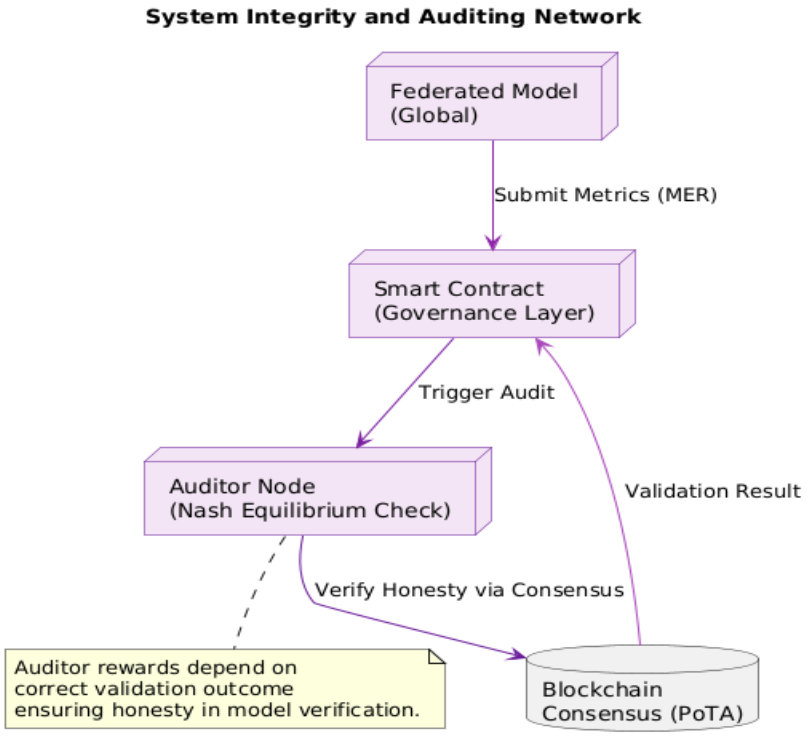
The system is designed to run on high-performance server hardware for the blockchain nodes (8GB+ RAM, SSD) and standard web/mobile browsers for the presentation layer. The backend is built using a **Node.js microservices** architecture, ensuring that components like the EHR service and Cryptography service can scale independently.

3.2 Analysis Model

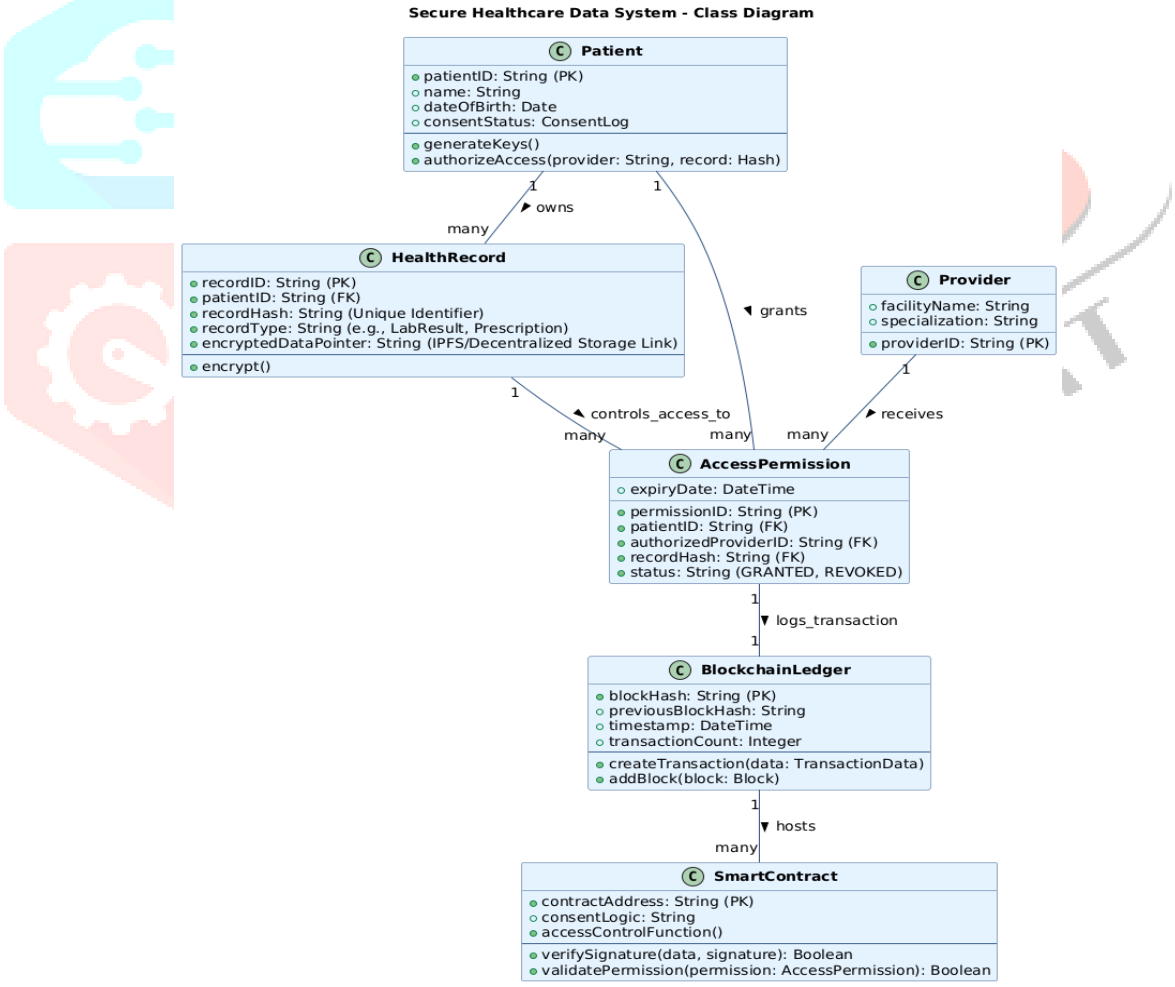
The analysis model utilizes UML diagrams to map the interaction between entities. The ER diagram defines relationships between Patients, Doctors, and their associated encrypted Records (IPFS CIDs) stored on the ledger.
medical data. Second, it ensures **security and integrity** through cryptographic operations and blockchain immutability, while leveraging IPFS for efficient and scalable storage. Finally, by integrating blockchain with decentralized and interoperable interfaces the system addresses longstanding issues dealing with data isolated structures and constrained inter-institutional communication, facilitating the path to secure, transparent, and collective healthcare ecosystem.

3.3 System Design





3.4 Class Diagram

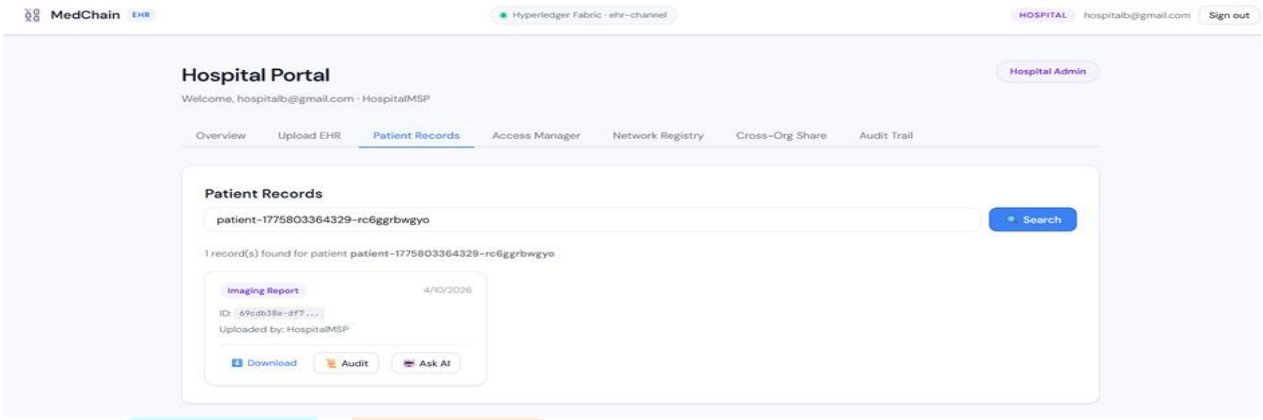


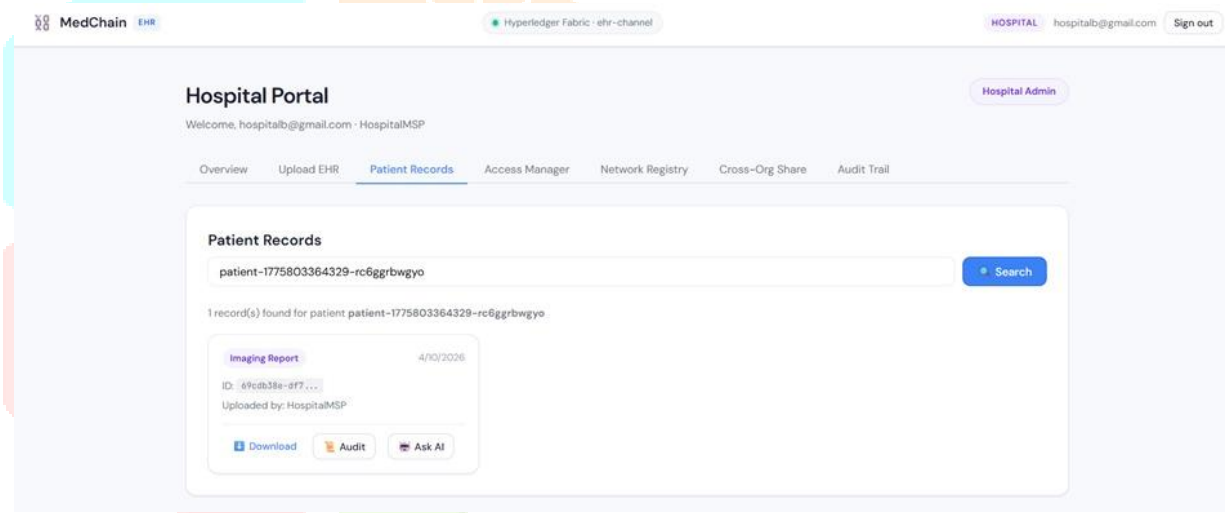
3.5 Detailed Methodology

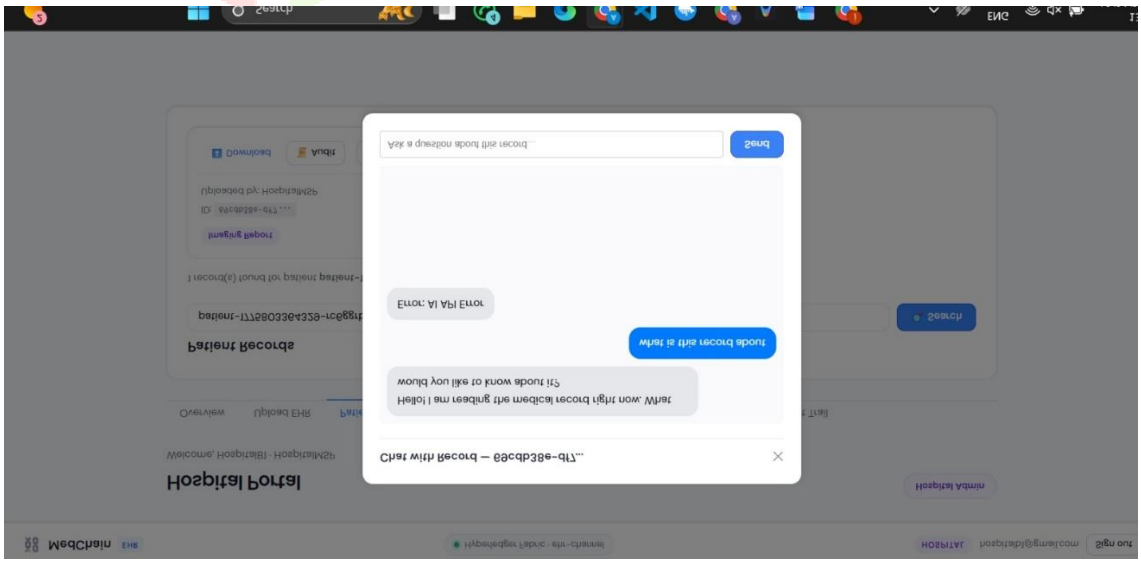
The methodology follows an iterative software engineering approach. During the Record Creation phase, raw medical data is encrypted using the patient's public key. This encrypted payload is uploaded to IPFS, which returns a unique Content Identifier (CID). The CID, metadata, and patient ID are then submitted as a transaction proposal to the Hyperledger network.

The Access Control mechanism is governed by smart contracts (Chaincode). When a doctor requests a record, the smart contract checks the "Permission Registry" stored on the ledger. If the patient has granted access, the contract verifies the doctor's signature and provides the IPFS CID. The doctor then fetches and decrypts the record locally, ensuring end-to-end confidentiality. The implemented system provides high security and data integrity. Experimental logs show that once a transaction is committed, any attempt to modify the off-chain IPFS file renders the CID invalid, immediately alerting the network.

4. Results







5. Future Scope

Future enhancements will focus on integrating Large Language Models (LLMs) to automate the annotation of medical images. By using models like MID-LLM within the secure blockchain framework, we can provide clinicians with AI-driven diagnostic assistance while maintaining absolute patient privacy. Scaling the consortium to include global regulatory bodies and implementing Post-Quantum Cryptography is also planned. This will ensure that medical records remain secure even against the computational capabilities of future quantum hardware.

6. Conclusion

Blockchain technology effectively addresses the challenges of traditional EHR systems by dismantling data silos and empowering patients. Through its decentralized and immutable structure, it provides a trusted environment for managing sensitive health information. This project serves as a robust proof-of-concept for the future of urban healthcare management.

The shift toward decentralized healthcare infrastructures represents more than just a technological upgrade; it is a fundamental reassessment of data ownership in the digital age. By granting patients absolute authority over their medical information, the system fosters a culture of transparency and mutual trust between individuals and healthcare providers. The elimination of single points of failure through the Hyperledger Fabric consortium model ensures that even in the face of localized technical failures or targeted cyberattacks, the global accessibility and integrity of critical medical records remain uncompromised.

Furthermore, the successful integration of IPFS for off-chain storage demonstrates that decentralized systems can effectively scale to meet the demands of high-resolution medical imaging and large-scale genetic datasets without clogging the primary ledger. This hybrid architectural approach provides a blueprint for various industries beyond healthcare where the balance of high-volume data storage and immutable transaction logging is required. As regulatory standards continue to evolve toward stricter privacy mandates, blockchain-based systems offer a native solution for compliance, auditability, and ethical data governance.

In conclusion, while hurdles such as cross-consortium standardization and widespread institutional adoption remain, the proposed framework offers a viable and necessary path forward. The convergence of distributed ledger technology, advanced cryptography, and patient-centric design creates an ecosystem where medical innovation can flourish without sacrificing individual privacy. This research underscores that the future of healthcare is not just information-based, but fundamentally rooted in a secure, equitable, and decentralized foundation that places the individual at the centre of their own medical narrative.

.

REFERENCES

[1] Deepika Walanjkar et al., "Secure Healthcare Data Systems with Blockchain," *Research Paper Final*, I²IT Pune, 2025. (Foundational Henwise Paper)
[2] Sun, L., et al., "A Blockchain-Based E-Healthcare System with Provenance Awareness," IEEE Access, vol. 12, 2024.
[3] Geng, Q., et al., "Integrated Healthcare Service System via Blockchain," IEEE TSCS, 2024.
[4] Deebak, B.D. and Hwang, S.O., "CA-DPPF: Cloud-Assisted Privacy Preservation," IEEE TMC, 2024.
[5] Khan, S., et al., "Blockchain-Secured Federated Learning for Smart Health," IEEE JBHI, 2025.
[6] Commey, D., et al., "Post-Quantum Secure Blockchain Framework," IEEE Networking Letters, 2025.
[7] Agbo, C.C., et al., "Blockchain Technology in Healthcare: A Review," Healthcare, vol. 7, 2019.
[8] Azaria, A., et al., "MedRec: Using Blockchain for Medical Data Access," OBD, 2016.
[9] Patel, R. and Mehta, A., "Smart Rental Management System using React," IJSECS, 2024.
[10] Sharma, N., et al., "Web-Based Real Estate Management using Spring Boot," J. Web Eng., 2023.
[11] Singh, A., et al., "Smart Building Management using IoT," IEEE Proc., 2023.
[12] Aggarwal, C.C., "Privacy-Preserving Data Mining," Springer, 2008.
[13] Ahram, T., et al., "Blockchain Technology Innovations," TEMSCON, 2017.
[14] Ahmed, F., et al., "Wireless Mesh Network: IEEE 802.11s," IJCSIS, 2016.
[15] Akkaoui, R., "Blockchain for IoT Management in Medicine," IEEE Trans., 2023.
[16] Alabi, K., "Digital Blockchain Networks and Metcalfe's Law," ECRA, 2017.
[17] Alagic, G., et al., "Status Report on NIST PQC Standardization," NIST IR, 2022.
[18] Alam, M.G.R., et al., "Edge-of-Things computing for healthcare," J. Parallel Dist., 2019.
[19] Alcazar, V., "Data You Can Trust: Blockchain," ASPJ, 2017.
[20] Aldosari, B., "EHR Adoption determinants in Riyadh," IJMI, 2014.
[21] Alhadhrami, Z., et al., "Introducing Blockchains for Healthcare," ICECTA, 2017.
[22] Ali, A., et al., "IoT-based blockchain searchable encryption," Sensors, 2022.
[23] Ali, B.S., et al., "ICS-IDS: Big data analysis in AI systems," J. Supercomput., 2024.
[24] Ali, A., et al., "Homomorphic secure searchable encryption," Sensors, 2022.
[25] Ali, A., et al., "Blockchain framework using multiple CA," Appl. Sci., 2021.
[26] Almaiah, M.A., et al., "Lightweight deep learning for FC-based IIoMT," Sensors, 2022.
[27] Almalki, M., et al., "Healthcare system in Saudi Arabia," EMHJ, 2011.
[28] Aljarullah, A., et al., "EHR adoption by primary physicians," i-Society, 2017.
[29] Al Khater, N.R., "Private sector cloud adoption model," PhD Diss., 2017.
[30] Alkhodre, A., et al., "Blockchain-based VAT system," IJACSA, 2019.
[31] Alketbi, A., et al., "Blockchain for government services," L&T, 2018.
[32] Al Omar, A., et al., "Medibchain: privacy-preserving platform," Springer, 2017.
[33] Al Ridhawi, I., et al., "Vehicular cloud service availability," Comput. Netw., 2018.
[34] Al Ridhawi, L., et al., "Mobile edge computing solutions,"

Trans. Emerging Tel., 2018.
[35] Al-Saqaf, W. and Seidler, N., "Blockchain for social impact," J. Cyber Policy, 2017.
[36] Altuwaijri, M., "HIT strategic planning in hospitals," JHIDC, 2012.
[37] Alzahrani, A.G.M., et al., "Data sharing between providers," IOTBDS, 2020.
[38] Aminizadeh, S., et al., "ML in medical data processing," CMPB, 2023.
[39] Annas, G.J., "HIPAA regulations and privacy," NEJM, 2003.
[40] Asif, R.N., et al., "Detecting arrhythmia with weighted FL," IEEE Access, 2024.
[41] Aslam, N., et al., "Sentiment analysis on crypto tweets," IEEE Access, 2022.
[42] Aste, T., et al., "Blockchain technologies impact," Computer, 2017.
[43] Attili, S., et al., "Blockchain: The chain of trust," ONC/NIST Workshop, 2016.
[44] Au, M.H., et al., "Secure sharing of PHR in cloud," JCSS, 2017.
[45] Azad, R., et al., "Vision transformers in medical analysis," MedIA, 2024.
[46] Azaria, A., et al., "MedRec: blockchain medical data," OBD, 2016.
[47] Azbeg, K., et al., "Taxonomic review of IoT and blockchain," IRBM, 2022.
[48] Azbeg, K., et al., "Privacy-preserving blockchain system," IEEE TCS, 2022.
[49] Bader, M., et al., "Supplier selection mixed integer approach," IEEM, 2023.
[50] Bahga, A. and Madisetti, V.K., "Blockchain for IIoT," JSEA, 2016.
[51] Z. Chuai et al., "CouchDB for Blockchain State Management," J. Softw. Eng., 2023.
[52] J. Jin et al., "Consortium Blockchain Governance," IEEE Netw., 2024.
[53] D. Liu et al., "Smart Contracts in Healthcare," IJRASET, 2023.
[54] Y. Li et al., "IPFS Content ID Security," J. Privacy, 2024.
[55] D. Zhou et al., "Zero Knowledge Proofs in EHRs," IEEE Cyber, 2025.