BLOCKCHAIN-DRIVEN HEALTHCARE ECOSYSTEM:
A Secure, Decentralized and Interoperable Medical Record Management Framework

Dr. Praveen Blessington Thummalakunta[1], Shrey Borkar[2], Parth Deshmukh[2], Nikita Bhande[2], Nikita Dhulgande[2].

[1]*Department of Information Technology, Zeal College of Engineering and Research (ZCOER), Pune, Maharashtra, India.*
[2]*Department of Information Technology, Zeal College of Engineering and Research (ZCOER), Pune, Maharashtra, India*

---***---

Abstract –
This Blockchain technology is driving a major transformation in the healthcare industry by providing a secure and decentralized framework for managing sensitive medical records. Unlike conventional systems that rely on centralized databases—often vulnerable to cyber-attacks and unauthorized alterations—blockchain operates on a distributed ledger where recorded data is immutable. This immutability significantly enhances data integrity and reduces the risk of security breaches. A key strength of blockchain in healthcare is its ability to ensure privacy. Through encryption and decentralized control, access to medical information is restricted to authorized users only. Additionally, blockchain enables efficient and secure data sharing among hospitals, clinics, and specialists, overcoming challenges posed by fragmented or inconsistent health records. This improves the speed and accuracy of patient care. Smart contracts further enhance the system by automating access permissions and updates based on predefined rules. These self-executing protocols minimize manual intervention, reduce administrative overhead, and lower the chance of human error. Most importantly, blockchain empowers patients by giving them full control over their personal health data. Patients can choose who accesses their records, fostering transparency and trust between healthcare providers and individuals. This patient-centric approach encourages active participation in healthcare decisions and supports a more collaborative care environment.

***Key Words*:** Blockchain Technology, Medical Records Management, Decentralized Systems, Data Privacy, Smart Contracts, Patient-Centric Healthcare, Secure Data Sharing, Interoperability, Tamper-Proof Records, Healthcare Automation, Distributed Ledger, Access Control, Digital Health Transformation

1. INTRODUCTION

1.1 Problem Statement

Despite advances in digital healthcare, several critical challenges remain. Centralized electronic health record (EHR) systems are highly vulnerable to cyberattacks, putting patient data at risk. Patients lack control over their own medical records, as access is typically managed by healthcare institutions. Additionally, poor interoperability between systems delays care and increases costs, while manual compliance processes make data security regulations difficult to maintain. Although over 80% of healthcare providers are exploring blockchain as a solution, the lack of standardized implementation frameworks hinders consistent adoption and leaves security concerns unresolved.

1.2 Proposed Solution

To overcome the limitations of centralized Electronic Health Record (EHR) systems—including data breaches, lack of interoperability, and restricted patient control—we propose Blockchain-IPFS hybrid architecture (Fig. 1). This system integrates decentralized storage, robust cryptographic mechanisms, and patient-centered access management. The solution comprises a React.js-based Decentralized Application (DApp) that supports role-specific interactions for patients, doctors, and diagnostic providers. Smart contracts deployed on the Ethereum blockchain manage access permissions and maintain immutable audit logs, while encrypted EHR files are stored off-chain using the InterPlanetary File System (IPFS), with their content hashes securely recorded on-chain. Key features include patient sovereignty through MetaMask-enabled access control, tamper-proof data verified via SHA-256 hashing, and regulatory alignment with HIPAA through AES-256 encryption and transparent audit trails. Figure 1 illustrates the architecture, highlighting the interaction between users, blockchain, and decentralized storage.

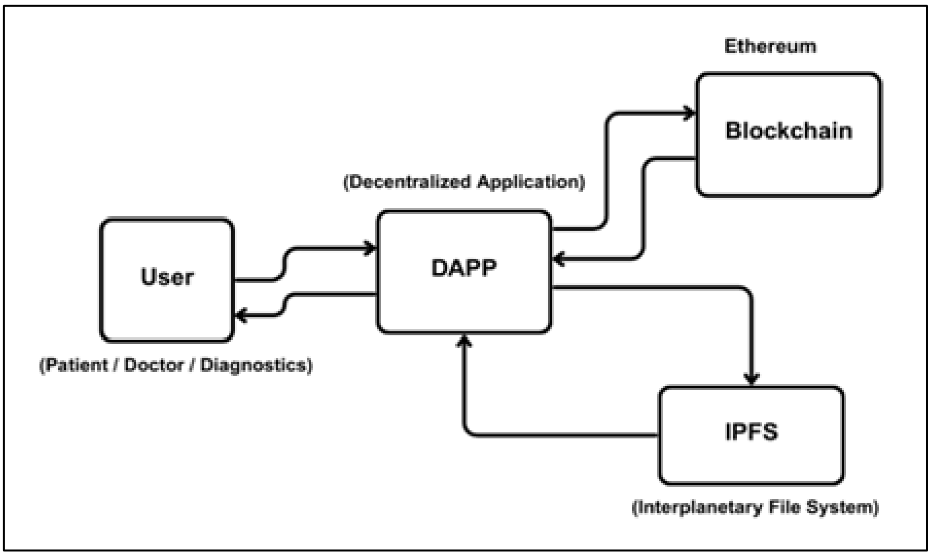

Figure 1 System Overview

2. Literature Review

a Proposed Solution

Several blockchain-based models have been proposed to enhance the integrity, privacy, and accessibility of electronic health records (EHRs). Sun et al. [1] introduced a provenance-aware blockchain framework that mitigates data silos by maintaining transparent record tracking. Similarly, Haddad et al. [2] proposed a patient-centric architecture leveraging Ethereum smart contracts and IPFS for decentralized storage, facilitating dynamic access control. A hybrid approach was explored by Sun et al. [3], where sidechain integration and optimized consensus mechanisms reduced on-chain storage overhead. Additionally, Kim et al. [4] focused on real-time patient consent mechanisms using role-based smart contracts to improve data autonomy and revocation capabilities..

b Gaps

While these models present significant contributions, they also exhibit critical limitations. The provenance-based model by Sun et al. [1] suffers from high computational costs due to unoptimized smart contract design. Haddad et al. [2] highlighted privacy risks in earlier frameworks like MedRec, and their solution faces scalability issues similar to Medchain. The hybrid blockchain model [3] improves performance but introduces trade-offs between transaction throughput and security. Kim et al. [4] encountered difficulties aligning dynamic consent features with regulatory frameworks such as HIPAA and GDPR. Moreover, none of the reviewed systems fully addressed integration with diagnostic services, efficient gas usage, or seamless patient-doctor interaction through a unified interface.

Related Work

Sun et al. [1] proposed a blockchain-based e-healthcare framework with provenance awareness to address challenges such as data silos, poor record tracking, and scalability limitations in traditional systems. However, existing blockchain EHR models still struggle with real-world usability, efficient provenance tracking, and seamless data exchange. Issues such as high computational costs, smart contract vulnerabilities, lack of robust access control, and complex user interfaces continue to limit widespread adoption. To overcome these, the proposed system incorporates secure authorization layers and advanced algorithms aimed at improving privacy, interoperability, and system efficiency.

Haddad et al. [2] focused on the evolution and challenges of blockchain in electronic health record management, particularly emphasizing patient-centered models. While early systems like MedRec utilized Ethereum smart contracts, they faced privacy issues due to reliance on external databases. Later solutions like Medchain improved data sharing but still lacked scalability and privacy strength. Recent models such as PCEHRM-SC integrate Ethereum with IPFS to enhance decentralized storage, data immutability, and overall system performance, highlighting the need for privacy-focused and scalable blockchain frameworks.

Sun et al. [3] identified weak access control and storage inefficiency as major shortcomings in existing blockchain-based medical data systems. Their proposed solution enhances these areas by incorporating a more secure architecture and optimizing system performance. Through comparative analysis of consensus mechanisms and transaction throughput, they demonstrated significant improvements in data sharing and storage management.

Kim et al. [4] explored blockchain's potential in enhancing security, privacy, and data integrity for personal health records (PHRs). The study introduced the concept of dynamic permission, empowering users with real-time control over data access. It also emphasized the importance of data standardization, legal compliance, and smooth integration with existing healthcare systems. The research outlines how emerging tools such as smart contracts and decentralized applications (dApps) can securely manage health data, laying a foundation for future blockchain-based PHR platforms.

Summary:

Several blockchain-based solutions have emerged to improve healthcare data management by ensuring traceability, decentralization, and patient-controlled access. While these systems address key challenges like data silos and access transparency, limitations remain. Common issues include high processing overhead due to complex smart contracts, scalability bottlenecks, and limited testing in real-world healthcare environments. Furthermore, many models struggle with compliance requirements and do not integrate smoothly with existing hospital IT infrastructure, indicating the need for more adaptable and secure frameworks.

3. SYSTEM ARCHITECTURE:

3.1 Technology Stack

(Refer to the figure 2)

- **Frontend:** The user interface is developed using React.js, integrated with MetaMask for secure role-based login and blockchain interactions.
- **Smart Contracts:** Core logic for user roles, access permissions, and audit trails is implemented in Solidity and deployed on the Ethereum Rinkeby test network.
- **Storage Layer:** Medical files are encrypted using AES-256, split, and uploaded to IPFS, a decentralized file system. Only the corresponding CIDs (Content Identifiers) are stored on-chain to reduce storage overhead.
- **Authentication and Interaction:** The system uses Web3.js to handle wallet-based interactions, transaction signing, and Ethereum node communication.
- **Development Tools:** Ganache provides a local blockchain environment for contract testing, while the Truffle Suite streamlines compilation, migration, and testing processes.

3.2 Workflow

- **User Registration:** Patients, doctors, and diagnostic centers register via MetaMask and are assigned roles through smart contracts.
- **Granting Access:** Patients selectively authorize access to specific doctors or diagnostic centers. This consent is recorded immutably on the blockchain.
- **Medical Record Upload:** Patients or diagnostic centers upload encrypted health records to IPFS. Each file's CID is stored on-chain to anchor it securely.
- **Data Retrieval:** Authorized users retrieve IPFS-hosted data using the stored CIDs, and decrypt the files locally using secure keys.
- **Prescription and Record Updates:** Doctors issue prescriptions or diagnoses which are linked back to the patient profile and stored securely.
- **Audit Logging:** All actions (upload, access, updates) are logged immutably on the blockchain, ensuring transparency and accountability.

4. ADVANTAGES OF THE PROPOSED SYSTEM

- **Decentralized Trust:** Eliminates centralized intermediaries, ensuring tamper-proof data storage and access.
- **Role-Based Security:** Smart contracts govern access permissions, ensuring that only verified users can access sensitive health records.
- **Patient-Centric Control:** Patients retain full authority to approve or deny access to their health data.
- **Storage Optimization:** Offloading heavy EHR files to IPFS significantly reduces the burden on the blockchain and minimizes costs.
- **Regulatory Readiness:** On-chain audit trails and encrypted off-chain storage help align with HIPAA and GDPR standards.
- **Scalability & Flexibility:** The modular design allows for easy integration with legacy systems and expansion to future health tech solutions.

5. CHALLENGES AND LIMITATIONS

- **High Gas Usage:** Operations like doctor registration and access granting consume significant gas due to authorization logic.
- **Learning Curve:** Patients and healthcare staff may require training to use wallets like MetaMask for access management.
- **Latency in IPFS Access:** Retrieval delays (~1.2s) could be problematic in time-sensitive medical scenarios.
- **Data Retention on IPFS:** Persistent availability requires active pinning, which may incur additional maintenance overhead.
- **Key Management:** Although encryption secures files, managing decryption keys externally presents a usability challenge.

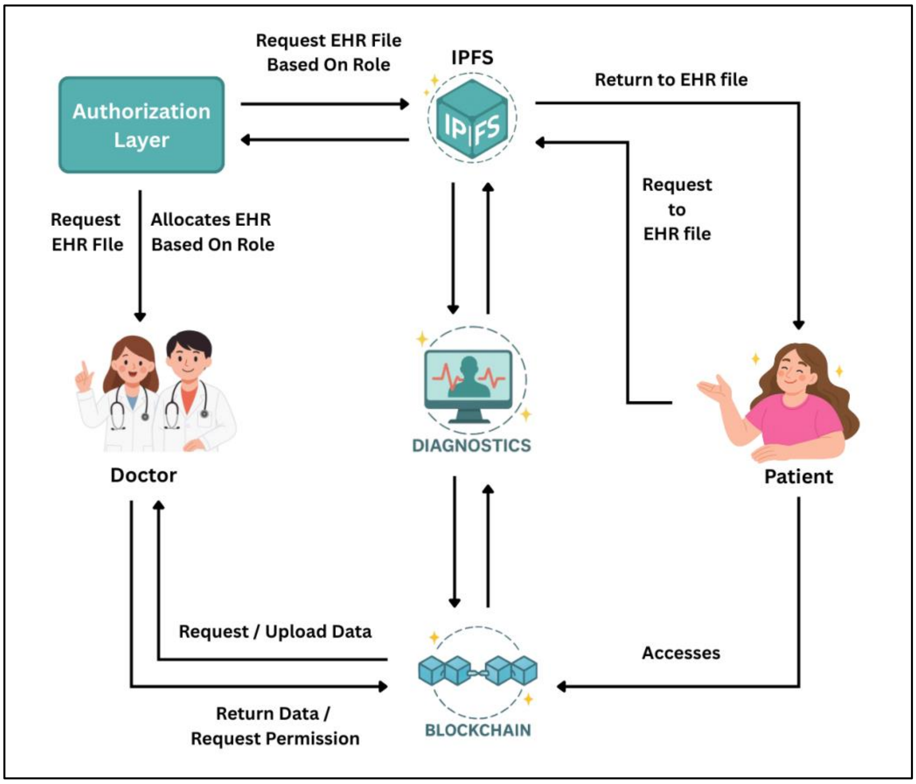

Figure 2 Proposed Architecture

6. CONCLUSIONS

The Blockchain-Based Medical Record System represents a key advancement in secure and efficient healthcare data management. By combining blockchain with technologies like IPFS, React, Ganache, and MetaMask, the system ensures data integrity, privacy, and controlled access. Role-based permissions and decentralized storage provide a reliable framework for handling sensitive medical records. The use of agile development supported continuous improvements and adaptability to healthcare needs. Moving forward, the focus will be on enhancing system interoperability, adopting advanced privacy techniques such as zero-knowledge proofs, and integrating intelligent security features powered by AI

REFERENCES

[1] Singh, P., Sagar, S., Singh, S., Haya Mesfer Alshahrani, Getahun, M., & Soufiene, B. O. (2024). Blockchain-enabled verification of medical records using soul-bound tokens and cloud computing. Scientific Reports, 14(1). https://doi.org/10.1038/s41598-024-75708-3.

[2] Vardhini B, Dass, S. N., Sahana R, & R. Chinnaiyan. (2021). A Blockchain based Electronic Medical Health Records Framework using Smart Contracts. 2022 International Conference on Computer Communication and Informatics (ICCCI), 1–4. https://doi.org/10.1109/iccci50826.2021.9402689.

[3] Bodur, H., & Al Yaseen, I. F. T. (2024). An Improved Blockchain-based secure medical record sharing scheme. Cluster Computing, 27(6), 7981–8000. https://doi.org/10.1007/s10586-024-04414-6.

[4] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain Technology in Healthcare: A Systematic Review. Healthcare, 7(2), 56–56. https://doi.org/10.3390/healthcare7020056.

[5] Haddad, A., Habaebi, M. H., Islam, M. R., & Suriza Ahmad Zabidi. (2021). Blockchain for Healthcare Medical Records Management System with Sharing Control. 30–34. https://doi.org/10.1109/icsima50015.2021.9526301.

[6] Tran, P., Nguyen, T., Chu, L., Tran, N., & Ta, H. (2024). A Solution for Commercializing, Decentralizing and Storing Electronic Medical Records by Integrating Proxy Re-Encryption, IPFS, and Blockchain. Retrieved January 30, 2025, from arXiv.org website: https://arxiv.org/abs/2402.05498.

[7] Agbeyangi, A., Oki, O., & Mgidi, A. (2024). Blockchain in Healthcare: Implementing Hyperledger Fabric for Electronic Health Records at Frere Provincial Hospital. Retrieved January 30, 2025, from arXiv.org website: https://arxiv.org/abs/2407.15876.

[8] Sun, Z., Han, D., Li, D., Wang, X., Chang, C.-C., & Wu, Z. (2022). A Blockchain-based secure storage scheme for medical information. EURASIP Journal on Wireless Communications and Networking, 2022(1). https://doi.org/10.1186/s13638-022-02122-6.

[9] Usharani Chelladurai, & Pandian, S. (2021). A novel Blockchain based electronic health record automation system for healthcare. Journal of Ambient Intelligence and Humanized Computing, 13(1), 693–703. https://doi.org/10.1007/s12652-021-03163-3.

[10] Haddad, A., Habaebi, M. H., Suliman, F. E. M., Elsheikh, E. A. A., Islam, M. R., & Zabidi, S. A.

(2023). Generic Patient-Centered Blockchain-Based EHR Management System. Applied Sciences, 13(3), 1761. https://doi.org/10.3390/app13031761.

[11] Kim, H., Lee, S., Kwon, H., & Kim, E. (2021). Design and Implementation of a Personal Health Record Platform Based on Patient-consent Blockchain Technology. KSII Transactions on Internet and Information Systems, 15(12), 4400–4419. Retrieved from https://itiis.org/digital-library/25145.

[12] Deed - Attribution-NonCommercial-NoDerivatives 4.0 International - Creative Commons. (2025). Retrieved January 30, 2025, from Creativecommons.org website: https://creativecommons.org/licenses/by-nc-nd/4.0/.

[13] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Computational and Structural Biotechnology Journal, 16, 267–278. https://doi.org/10.1016/j.csbj.2018.07.004

[14] Asaph Azaria, Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. https://doi.org/10.1109/obd.2016.11.

[15] Singh, P., Sagar, S., Singh, S., Haya Mesfer Alshahrani, Getahun, M., & Soufiene, B. O. (2024). Blockchain-enabled verification of medical records using soul-bound tokens and cloud computing. Scientific Reports, 14(1). https://doi.org/10.1038/s41598-024-75708-3

[16] Vardhini B, Dass, S. N., Sahana R, & R. Chinnaiyan. (2021). A Blockchain based Electronic Medical Health Records Framework using Smart Contracts. 2022 International Conference on Computer Communication and Informatics (ICCCI), 1–4. https://doi.org/10.1109/iccci50826.2021.9402689.

[17] Bodur, H., & Al Yaseen, I. F. T. (2024). An Improved Blockchain-based secure medical record sharing scheme. Cluster Computing, 27(6), 7981–8000. https://doi.org/10.1007/s10586-024-04414-6.

[18] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain Technology in Healthcare: A Systematic Review. Healthcare, 7(2), 56–56. https://doi.org/10.3390/healthcare7020056.

[19] Haddad, A., Habaebi, M. H., Islam, M. R., & Suriza Ahmad Zabidi. (2021). Blockchain for Healthcare Medical Records Management System with Sharing Control. 30–34. https://doi.org/10.1109/icsima50015.2021.9526301.

[20] Tran, P., Nguyen, T., Chu, L., Tran, N., & Ta, H. (2024). A Solution for Commercializing, Decentralizing and Storing Electronic Medical Records by Integrating Proxy Re-Encryption, IPFS, and Blockchain. Retrieved January 30, 2025, from arXiv.org website: https://arxiv.org/abs/2402.05498.

[21] Agbeyangi, A., Oki, O., & Mgidi, A. (2024). Blockchain in Healthcare: Implementing Hyperledger Fabric for Electronic Health Records at Frere Provincial Hospital. Retrieved January 30, 2025, from arXiv.org website: https://arxiv.org/abs/2407.15876.

[22] Sun, Z., Han, D., Li, D., Wang, X., Chang, C.-C., & Wu, Z. (2022). A Blockchain-based secure storage scheme for medical information. EURASIP Journal on Wireless Communications and Networking, 2022(1). https://doi.org/10.1186/s13638-022-02122-6.

[23] Usharani Chelladurai, & Pandian, S. (2021). A novel Blockchain based electronic health record automation system for healthcare. Journal of Ambient Intelligence and Humanized Computing, 13(1), 693–703. https://doi.org/10.1007/s12652-021-03163-3.

[24] Haddad, A., Habaebi, M. H., Suliman, F. E. M., Elsheikh, E. A. A., Islam, M. R., & Zabidi, S. A. (2023). Generic Patient-Centered Blockchain-Based EHR Management System. Applied Sciences, 13(3), 1761. https://doi.org/10.3390/app13031761.

[25] Kim, H., Lee, S., Kwon, H., & Kim, E. (2021). Design and Implementation of a Personal Health Record Platform Based on Patient-consent Blockchain Technology. KSII Transactions on Internet and Information Systems, 15(12), 4400–4419. Retrieved from https://itiis.org/digital-library/25145.

[26] Deed - Attribution-NonCommercial-NoDerivatives 4.0 International - Creative Commons. (2025). Retrieved January 30, 2025, from Creativecommons.org website: https://creativecommons.org/licenses/by-nc-nd/4.0/.

[27] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Computational and Structural Biotechnology Journal, 16, 267–278. https://doi.org/10.1016/j.csbj.2018.07.004.

[28] Asaph Azaria, Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. https://doi.org/10.1109/obd.2016.11.

[29] Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient Healthcare Data Sharing viaBlockchain. Applied Sciences, 9(6), 1207–1207. https://doi.org/10.3390/app9061207.

[30] Hussien, H. M., Yasin, S. M., Udzir, N. I., Zaidan, B. B., & Zaidan, A. A. (2019). A systematic review for enabling of develop a Blockchain technology in healthcare industry. Journal of Biomedical Informatics, 94, 103129. https://doi.org/10.1016/j.jbi.2019.103129.