IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN-DRIVEN HEALTHCARE ECOSYSTEM:

A Secure, Decentralized and Interoperable Medical Record Management Framework

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

[1] Professor, [2] Students

[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: 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.

Keywords: 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.

I. INTRODUCTION

The Growing Complexity of Medical Data Security

Modern healthcare systems face unprecedented challenges in managing sensitive patient data. The shift from paper-based to digital medical records has revolutionized care delivery but introduced critical vulnerabilities. Centralized electronic health record (EHR) systems, while efficient, are prime targets for cyber-attacks due to their single points of failure. For instance, the 2024 breach at Change Healthcare exposed 190 million records, underscoring the fragility of conventional data architectures. Concurrently, patients demand greater control over their health information, while providers struggle with interoperability and compliance burdens. Blockchain technology emerges as a transformative solution, offering decentralized, tamper-proof data

storage through cryptographic hashing and distributed consensus mechanisms. Its ability to automate access via smart contracts and maintain immutable audit trails positions it as a cornerstone for next-generation medical record systems.

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 a 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.

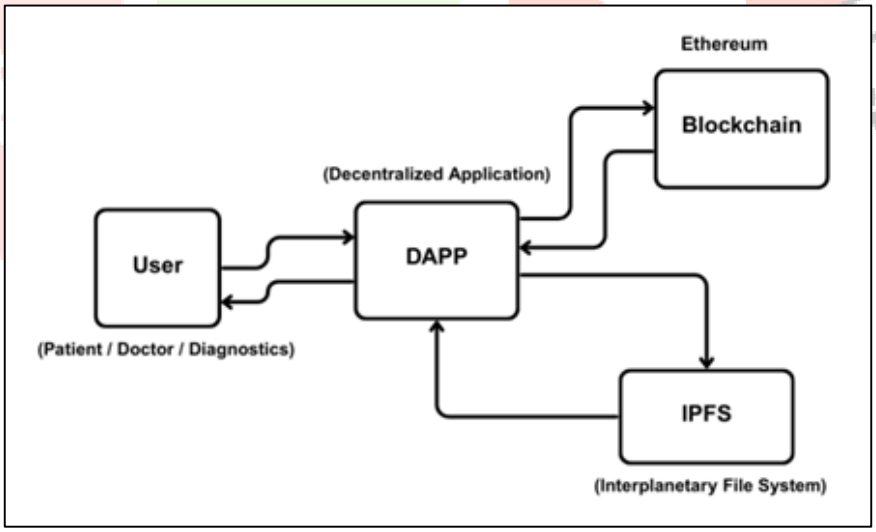

Figure 1: System Overview

1.3 Objectives

This ecosystem aims to:

1. **Evaluate** the effectiveness of blockchain in mitigating security risks associated with traditional EHR systems.
2. **Design** a decentralized, patient-centric framework for managing medical records securely and transparently.
3. **Integrate** smart contracts to automate HIPAA-compliant access control and consent management workflows.
4. **Assess** the interoperability of blockchain-based EHRs with existing healthcare IT systems.
5. **Quantify** improvements in operational efficiency, including reductions in manual audits, breach response time, and associated costs.

II. 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.

III. SYSTEM DESIGN AND ARCHITECTURE

The proposed architecture for the **Blockchain-enabled Electronic Health Record (EHR) Management System** ensures secure, decentralized handling of sensitive medical information. The architecture introduces a permissioned access model that leverages blockchain and IPFS to maintain confidentiality, authenticity, and availability of data while enabling controlled sharing among authorized participants such as patients, doctors, and diagnostic labs.

3.1 Overview:

The system is structured into distinct layers, each fulfilling a specific function within the medical data lifecycle. The architecture diagram (Figure 2) outlines how the components interact to provide a secure and transparent healthcare data exchange platform.

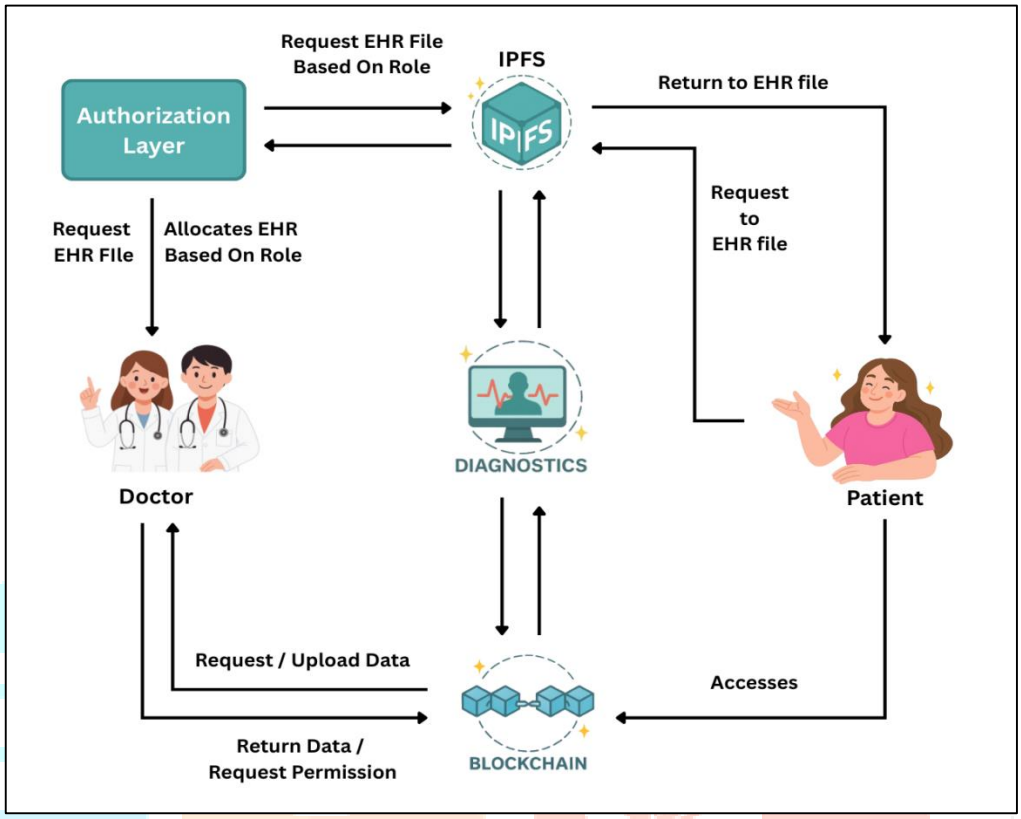

Figure 2: Proposed Architecture

1. User Interaction Layer

This layer represents the primary system users and their respective roles.

- **Actors**:
  - **Patients** – control access to their personal health records.
  - **Healthcare Providers** – request access to patient records and contribute new entries.
  - **Diagnostic Centers** – upload medical reports and test results.
- **Key Capabilities**:
  - Role-specific authentication and dashboard access.
  - Permission management for data access.
  - Upload and retrieval of medical data based on user privileges.

2. Access Control and Authorization Layer

This middleware layer governs access rights and ensures that only validated operations are allowed.

- **Functions**:
  - Validates access requests through predefined smart contract rules.
  - Interfaces with blockchain to verify the authenticity and permissions associated with each action.
  - Routes approved requests to the appropriate data storage service.

- **Technologies**:
  - Smart contracts written in Solidity.
  - Backend logic built using frameworks like Node.js or Django.

3. Decentralized Storage Layer (IPFS)

Medical documents are stored in an encrypted format within the **Inter-Planetary File System (IPFS)**, ensuring decentralized and tamper-resistant storage.

- **Features**:
  - Encrypts each file before upload using symmetric or asymmetric encryption techniques.
  - Generates a unique content identifier (CID) to track each record.
  - Enables high availability and fault tolerance across the distributed network.
- **Technology Stack**:
  - IPFS nodes (either public or private).
  - AES/RSA encryption for securing medical files.

4. Blockchain Layer

This foundational layer provides immutable, transparent, and auditable transaction logging.

- **Roles**:
  - Logs every access or update to medical records.
  - Stores access control metadata and file CIDs without revealing the actual content.
  - Ensures time-stamped, tamper-proof records to uphold data trustworthiness.
- **Technologies Used**:
  - Ethereum (private or consortium chain).
  - Smart contracts for access automation and event logging.

3.2 Workflow and Data Interaction:

The system follows a structured workflow that ensures patient consent and data integrity at each stage of interaction:

1. **System Entry**: Users (patients, doctors, or diagnostics) authenticate into the platform.
2. **Record Upload**: Diagnostic centers or doctors encrypt and upload the health record to IPFS.
3. **Permission Assignment**: Patients assign access privileges using the system dashboard.
4. **Access Request**: Doctors request patient data through smart contract calls.
5. **Authorization Check**: Blockchain validates if the requester meets the access criteria.
6. **Data Retrieval**: If approved, the file is fetched from IPFS using its CID.
7. **Audit Logging**: All operations are logged on-chain, ensuring transparency and traceability.

IV. METHODOLOGY

This system follows a decentralized approach for secure and efficient EHR management. It uses blockchain for access control and audit logs, while actual medical records are stored securely off-chain using IPFS.

4.1 System Roles:

- **Patients:** Own their health data and control who can access it.
- **Doctors:** Request access to records for consultation or updates.
- **Admin:** Manages system operations without accessing medical data.

4.2 Workflow Steps:

- **User Registration:** Patients and doctors register with the system.
- **Record Storage:** Encrypted records are uploaded to IPFS. Their hashes are saved on the blockchain**.**
- **Access Request:** Doctors request access through a smart contract**.**
- **Consent Grant:** Patients approve or deny requests via the interface.
- **Data Retrieval:** If approved, doctors fetch and decrypt records.
- **Audit Logs:** All actions are permanently logged on-chain.

4.3 Smart Contracts:

Smart contracts manage permissions with functions like:

- Granting/revoking access
- Verifying user roles
- Logging access events

These ensure that only authorized users can interact with the system.

4.4 Security Measures:

- **Data Encryption**: Records are encrypted using public-key cryptography.
- **Access Control**: Only users with granted permission can access records.
- **Auditability**: Every transaction is logged for transparency.

4.5 Tools and Platforms:

- **Blockchain:** Ethereum (prototype)
- **Smart Contracts:** Solidity
- **Storage:** IPFS
- **Frontend:** React.js
- **APIs:** Node.js with Web3.js
- **Testing:** Ganache, Remix

V. IMPLEMENTATION

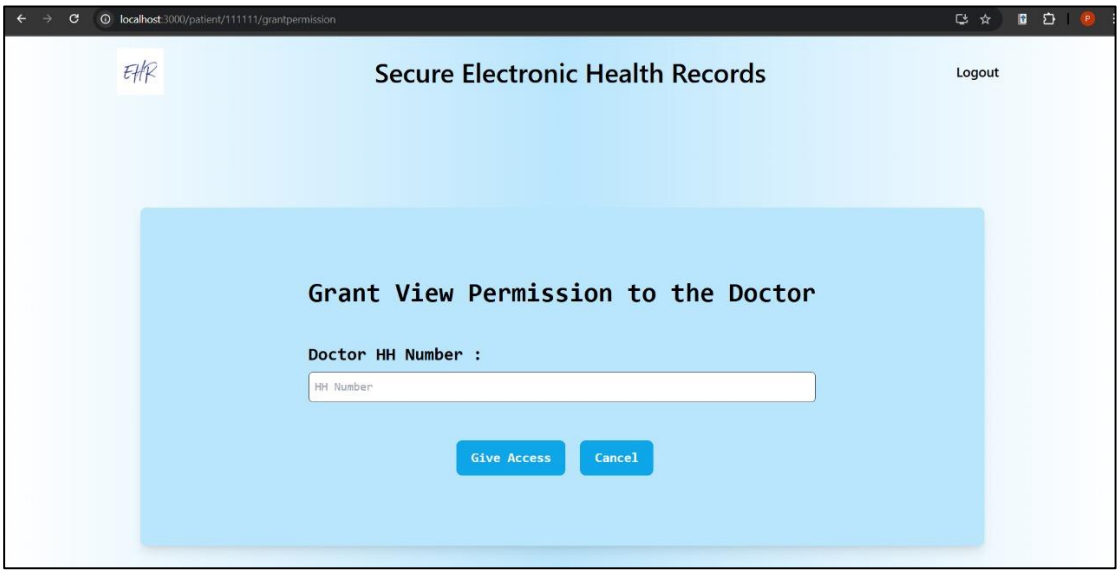

Figure 3: Patient Access Grant Interface

Figure 4: Doctor Dashboard – Access Granted Patients

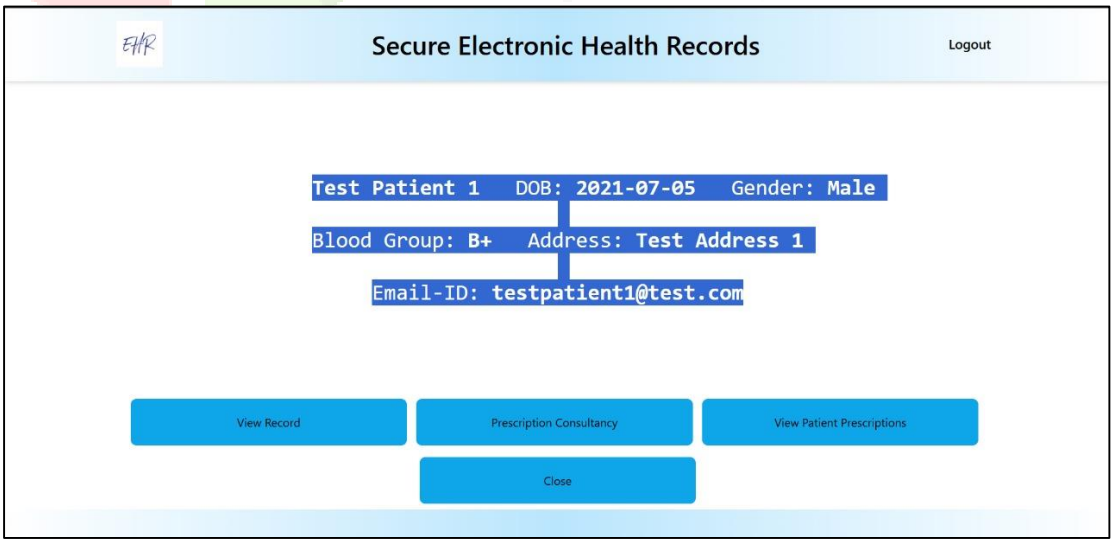

Figure 5: Patient Profile View for Authorized Doctor

Figure 6: Prescription Entry for a Specific Patient

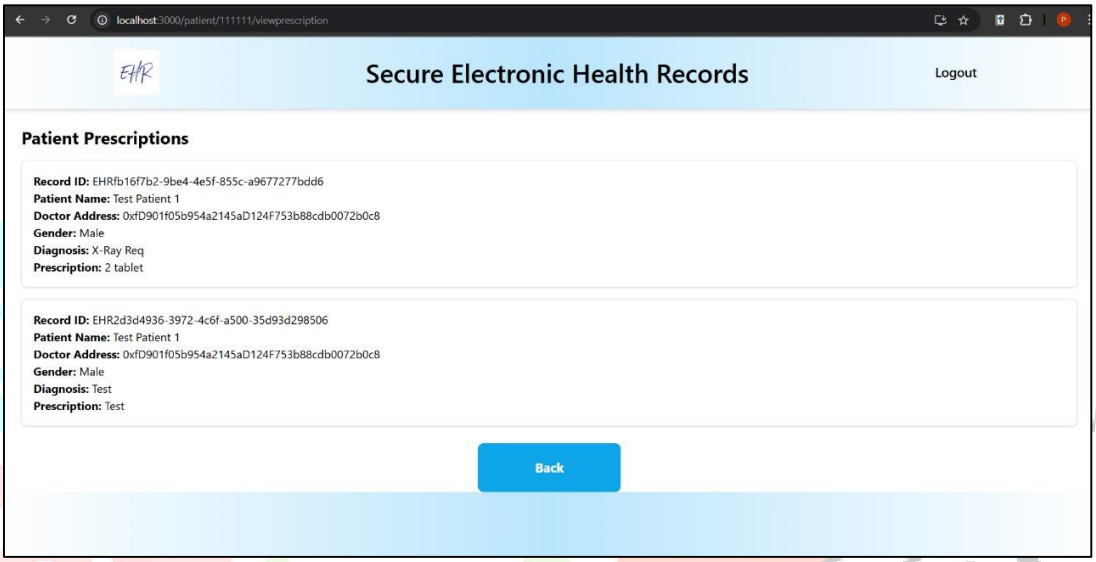

Figure 7: Patient Prescription Viewer

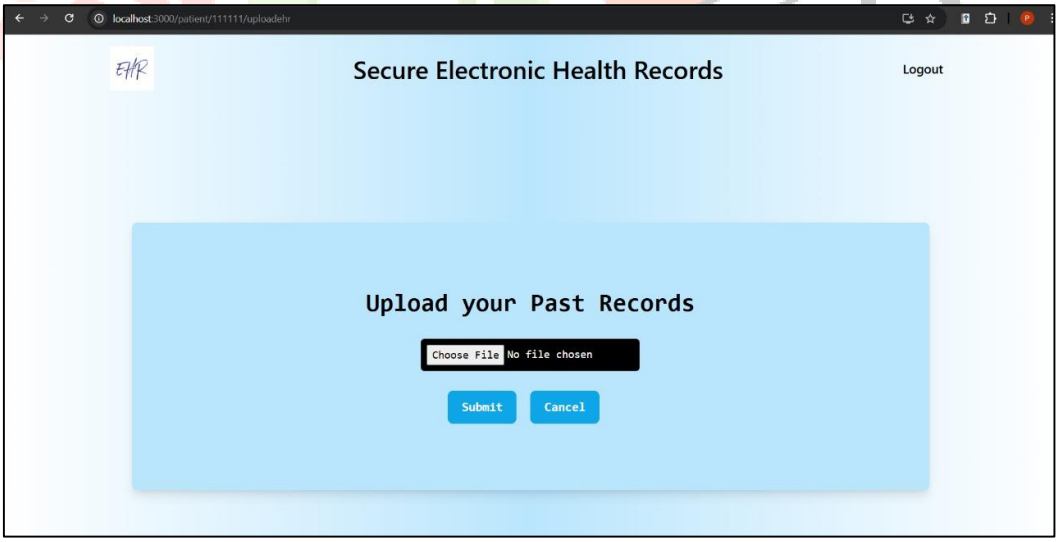

Figure 8 Patient EHR Upload Panel

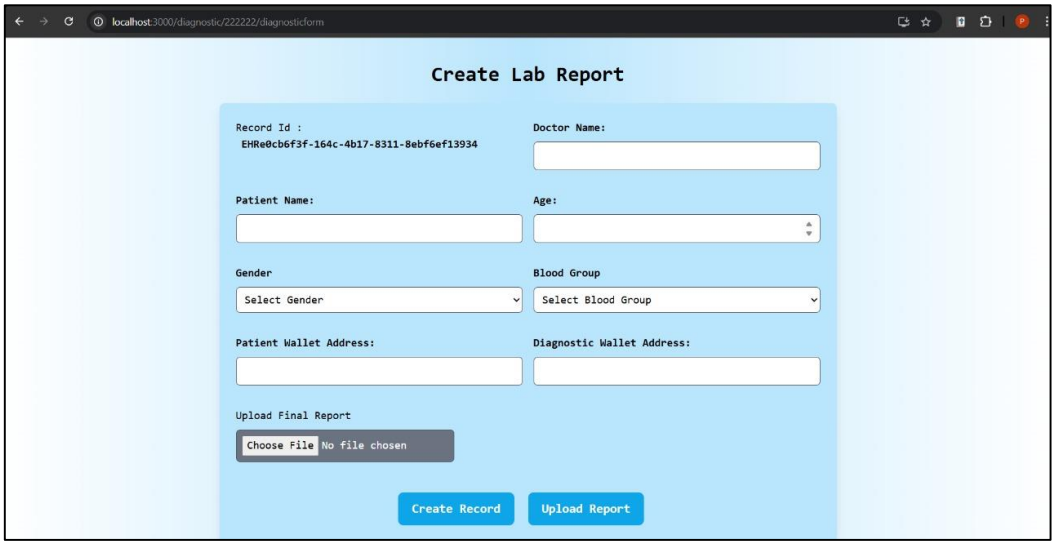

Figure 9 Diagnostic Lab Report Upload Interface

VI. RESULTS AND EVALUATION

The proposed system was evaluated on parameters such as gas usage, security, accessibility, and data integrity. Key findings are discussed below.

4.1 Gas Consumption and Efficiency

Gas usage was analysed across different modules to evaluate performance. Doctor Registration consumed the most gas due to strict verification logic, while Record Upload required the least because data is stored off-chain via IPFS.

Table 1: Gas Usage per Operation

Operation	Gas Consumption
Doctor Registration	334,710
Patient Registration	263,405
Diagnostic Registration	215,039
Patient Old Record Upload	164,545

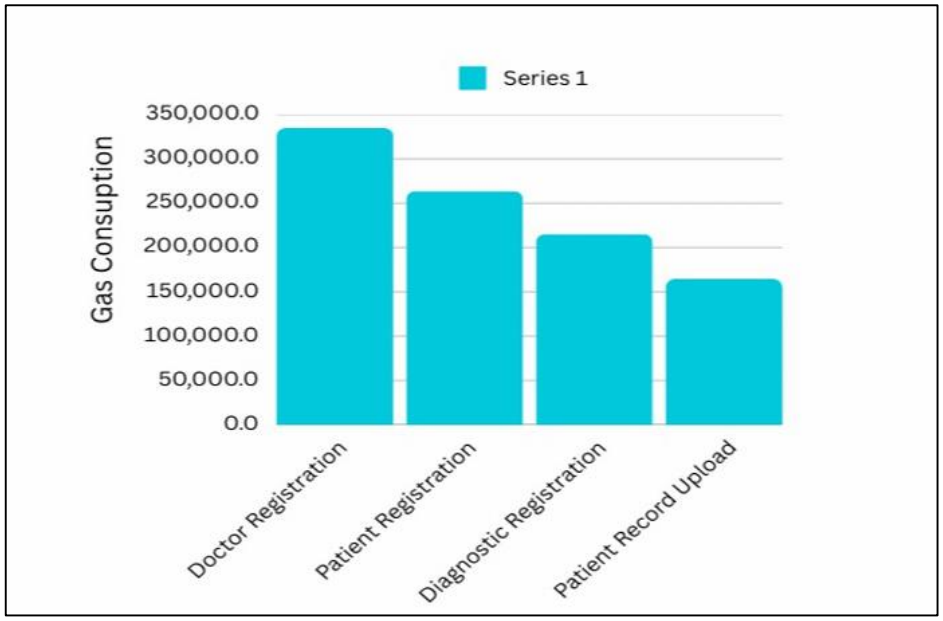

Figure 10: Gas Usage Per Module

4.2 Patient Record Accessibility and Management

The system ensures that patients retain full control over their data. Authorized users like doctors can access records through smart contract-based permissions, without compromising privacy. The use of IPFS for off-chain storage keeps uploads efficient (164,545 gas) and cost-effective.

4.3 Data Security and Integrity

Blockchain ensures all data is immutable and verifiable. IPFS enhances storage efficiency while maintaining data integrity. Every access or change request is logged and protected using cryptography, ensuring tamper-proof records.

4.4 Access Control and Authorization

Smart contracts enforce strict role-based access. Gas usage is highest during user registration, reflecting the cost of identity checks and permission setup. This ensures that only authorized parties can access or modify sensitive records, enhancing system trust and security.

VII. CONCLUSION

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.