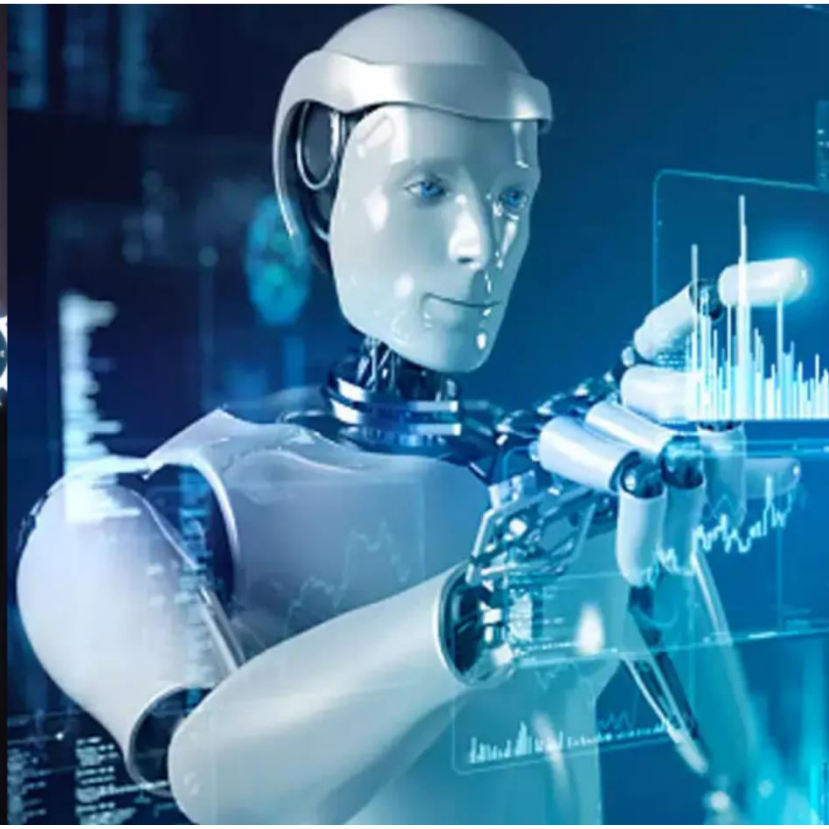
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Special Issue 1, January 2026

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

Traksh: A Blockchain-Based Secure Medical Record Management System

Shailendra Kumane[1], Krish Mishra[2], Shaswat Mishra[3], Piyush Singh[4], Shraddha Malabadi[5]

Assistant Professor, Dept. of IT, Datta Meghe College of Engineering, Airoli, Maharashtra, India[1]

UG Student, Dept. of IT, Datta Meghe College of Engineering, Airoli, Maharashtra, India[2,3,4,5]

ABSTRACT: The rapid digitization of healthcare has created a pressing need for secure, transparent, and patient-centric medical record management systems. Traditional centralized databases often face critical challenges such as unauthorized access, data tampering, lack of interoperability, and limited patient control over sensitive data. To address these issues, this paper presents Traksh, a blockchain-based decentralized medical record management system designed to ensure the security, integrity, and privacy of healthcare data. Traksh operates by interconnecting three primary entities-Patients, Doctors, and Hospitals-via smart contracts deployed on the Ethereum blockchain. The system utilizes the InterPlanetary File System (IPFS) for the secure, off-chain storage of medical reports, ensuring scalability while maintaining data integrity. Patients retain full ownership of their data; they can upload reports and manage permissions by approving or denying access requests from healthcare providers. Conversely, doctors and hospitals can request access to records, view authorized reports, and utilize an integrated referral mechanism to transfer cases seamlessly to other providers. By leveraging MetaMask for secure identity management, Ganache for blockchain simulation, and Solidity-based smart contracts, Traksh guarantees a tamper-proof, auditable, and transparent ecosystem where medical data remains under the direct control of the patient.

KEYWORDS: Blockchain, Medical Record Management, Ethereum, Smart Contracts, IPFS, MetaMask, Healthcare Security, Data Privacy, Referral System, Solidity, Tamper Proof, Data Security.

I. INTRODUCTION

The management of medical records is a critical aspect of modern healthcare, directly impacting patient care quality, data privacy, and interoperability among healthcare providers. Traditional centralized systems often face challenges such as data breaches, unauthorized access, and difficulties in seamless data sharing across multiple entities. To address these issues, blockchain technology offers a promising solution by enabling a decentralized, immutable, and transparent platform for secure medical record management.

This paper presents Traksh, a blockchain-based secure medical record management system that involves three key entities: patients, doctors, and hospitals. Leveraging Ethereum blockchain and smart contracts written in Solidity, Traksh allows patients to upload their medical reports and control access permissions effectively.
Doctors and hospitals can request access to these records, with an integrated referral mechanism enabling them to refer cases to other providers when needed. Medical reports are stored securely off-chain using IPFS, ensuring scalability and data integrity without burdening the blockchain.

The system integrates MetaMask for secure identity management and transaction authorization, while the React-based front-end provides an intuitive user interface. Using Ganache for development and testing, Traksh aims to create a secure, transparent, and patient-centric ecosystem for medical record management, addressing key challenges in healthcare data security and interoperability.

II. SYSTEM MODEL AND ASSUMPTIONS

The proposed system, Traksh, is modeled as a decentralized framework that integrates blockchain technology with distributed IPFS storage to ensure secure and patient-controlled medical record management. The system involves three primary entities—patients, doctors, and hospitals—each authenticated through a unique blockchain address using MetaMask. Patients upload medical records via the web interface, which stores the report in IPFS and returns a Content

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

Identifier (CID). This CID is recorded on the Ethereum blockchain through smart contracts such as Patient Manager and Access Manager, ensuring tamper-evident storage and transparent access governance. Doctors and hospitals interact with the system by submitting access requests, which are forwarded to the patient for approval; only after explicit consent is the CID shared, enabling authorized retrieval of the record from IPFS. A referral workflow is also embedded, allowing patient-approved delegation of access to other healthcare providers, thereby supporting practical clinical processes while maintaining strict control by the patient.

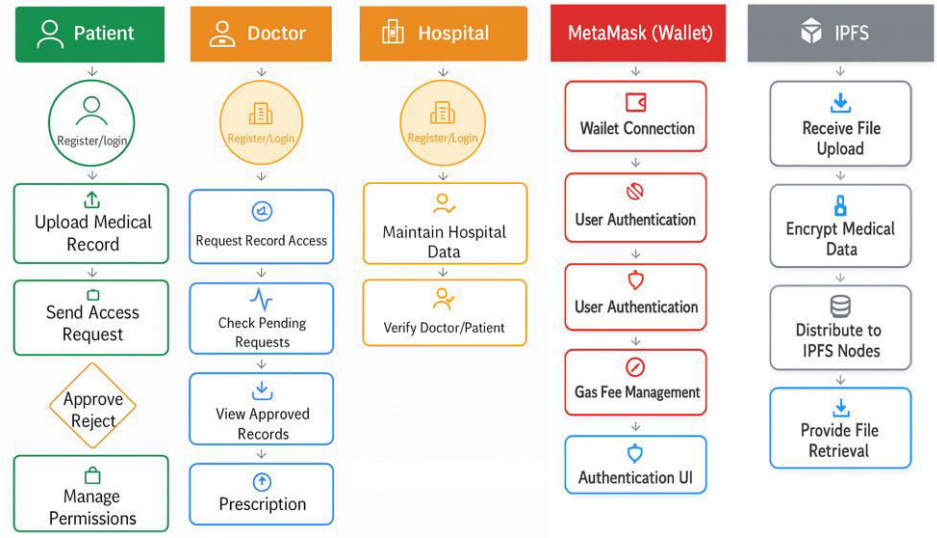


Fig. 1 System Workflow Diagram

The system assumes that all users interact through secure, verified MetaMask wallets, ensuring the authenticity of blockchain identities and preventing impersonation. The front-end interface is presumed to be trusted and free from malicious modification, and IPFS nodes are expected to remain available through appropriate pinning or replication to ensure consistent file access. Smart contracts deployed on the blockchain are considered immutable and functionally correct, as they enforce all access permissions and request handling. Additionally, it is assumed that users provide informed consent when responding to access requests and that reliable network connectivity is maintained for interactions between the blockchain, IPFS, and the web application. Under these assumptions, Traksh establishes a robust, decentralized environment that guarantees data integrity, prevents unauthorized access, and supports a secure and traceable workflow for managing electronic medical records.

III. EFFICIENT COMMUNICATION

Efficient communication within Traksh is achieved through a hybrid design that separates data storage from access governance, enabling fast, reliable, and transparent interactions among patients, doctors, hospitals, and the blockchain network. When a patient uploads a medical report through the web application, the file is stored in IPFS, and the corresponding CID is immediately recorded on the blockchain using smart contracts. This approach significantly reduces communication overhead, as only lightweight metadata is transmitted on-chain, while large files remain off-chain. Doctors and hospitals initiate access requests directly through smart contract functions, which generate on-chain events that notify the patient in real time through the application interface. Once the patient approves a request, the system securely transmits the CID to the authorized provider, allowing them to retrieve the file from IPFS without burdening the blockchain with large data transfers. This event-driven communication model ensures low latency, minimizes redundant operations, and maintains a clear and auditable flow of information between all actors.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

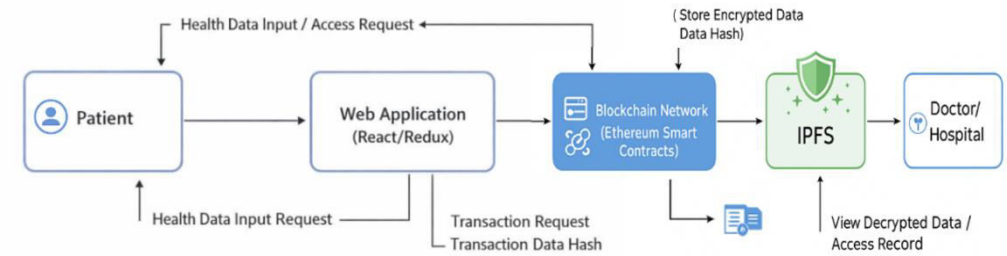


Fig. 2 Component-Based Communication Architecture

The referral mechanism further enhances communication efficiency by supporting structured delegation of access from one provider to another with explicit patient approval. Instead of re-uploading or retransmitting medical files across multiple entities, the blockchain simply updates the access permissions, enabling the newly approved doctor or hospital to retrieve the same CID from IPFS. This reduces network traffic, prevents duplication of data, and ensures synchronized access across providers. The integration of React, ethers.js, and MetaMask ensures smooth communication between the user interface and the blockchain, handling authentication, transaction signing, and state updates automatically. Together, these components form a reliable, scalable, and transparent communication framework that supports secure medical data exchange while preserving system performance and user experience.

IV. SECURITY

The security of Traksh is grounded in a decentralized architecture that ensures tamper resistance, data integrity, and strict access control throughout the medical record lifecycle. By leveraging the Ethereum blockchain, all access requests, approvals, referrals, and record-related actions are stored as immutable transactions, preventing unauthorized modifications and ensuring end-to-end auditability. Patients authenticate through MetaMask using their unique blockchain addresses, ensuring that only legitimate users can perform sensitive actions such as uploading records or granting access. Medical files themselves are never stored on the blockchain; instead, they reside on IPFS, which uses content-addressed hashing to guarantee that any modification to a stored file produces a different CID, making tampering immediately detectable. Smart contracts such as Patient Manager and Access Manager enforce fine-grained access control policies, enabling doctors and hospitals to view patient data only after explicit, on-chain patient approval.

In addition to integrity and authentication safeguards, the system protects privacy through controlled access pathways that prevent unauthorized retrieval of medical records. Even if an attacker obtains a CID, the corresponding file remains inaccessible without patient-granted permissions and proper decryption when encryption is used. The referral mechanism is similarly secured through contract-based validation, requiring patient approval before access is delegated to another provider. All actors interact through a trusted front-end that communicates with the blockchain via ethers.js, ensuring that transaction details are accurately relayed and digitally signed. Because blockchain transactions cannot be altered or erased, the system provides resilient protection against insider attacks, unauthorized access attempts, and data manipulation. Combined with IPFS redundancy and secure wallet-based authentication, Traksh establishes a comprehensive security framework that safeguards confidentiality, integrity, and accountability across all healthcare interactions.

V. RESULT AND DISCUSSION

The proposed Traksh system was implemented and tested on the Ethereum Ganache test network with full IPFS integration. The experiments verified that the platform securely handles medical record storage, access control, and permission-based sharing while keeping the patient as the central authority.

1. Experimental Setup: The system was built using React.js with ethers.js for the frontend, Solidity smart contracts deployed through Truffle/Hardhat, Ganache as the local blockchain, MetaMask for authentication and transaction signing, and IPFS for decentralize d file storage.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

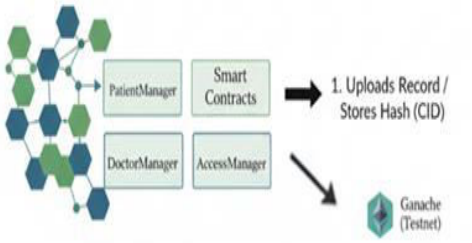


Fig. 3 Decentralized Medical Record Retrieval Process

a. Medical Record Upload: Patients successfully uploaded records, which were stored on IPFS, and the corresponding CID was saved immutably on the blockchain.

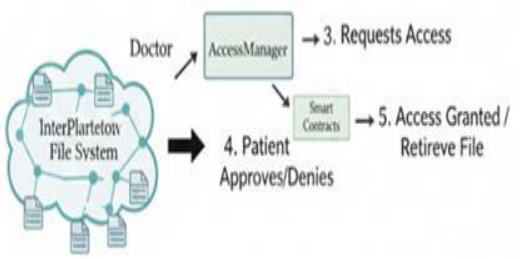


Fig. 4 Patient-Controlled Data Access Flow using IPFS and Smart Contracts

b. Access Requests & Approvals: Doctors and hospitals could request access, and patients could approve or reject these requests. Upon approval, authorized users retrieved the record via CID, while unauthorized attempts were blocked.

c. Referral Workflow: The system validated the referral mechanism, ensuring that doctors could delegate access rights only with explicit patient consent, maintaining strict patient-controlled data governance.

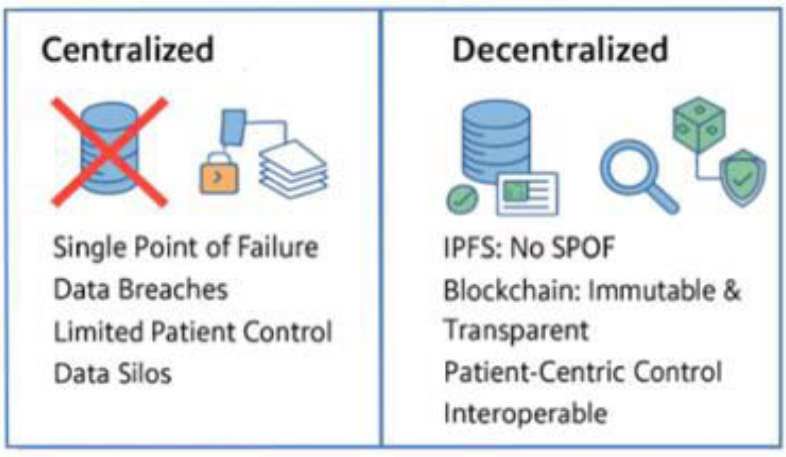


Fig. 5 Centralized vs Decentralized System

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

2. Comparative Discussion: Decentralized vs. Centralized Systems:
The Traksh decentralized architecture offers fundamental advantages over traditional centralized systems, particularly concerning data integrity and security. Unlike centralized systems that present a Single Point of Failure (SPOF) and enforce limited patient ownership, Traksh ensures data is distributed on IPFS, eliminating the SPOF, and implements Patient-Centric Control, allowing patients to retain full authority to grant or deny access. Furthermore, Traksh achieves Efficiency by storing only lightweight Content Identifiers (CIDs) on the blockchain, minimizing storage overhead and transaction costs, thereby overcoming the high-cost and data-silo issues associated with centralized databases. This structured, scalable approach, which clearly separates and manages entities (patients, doctors, and hospitals), ensures secure and traceable data sharing.

VI. CONCLUSION

The proposed system Traksh successfully demonstrates a blockchain-based secure medical record management system that ensures data privacy, security, and patient-centric control. By integrating IPFS for decentralized storage and Ethereum smart contracts for access control, the system eliminates the risks of centralized healthcare data management such as data breaches, single points of failure, and unauthorized access. Patients retain full ownership of their medical records and have the authority to grant or deny access to doc- tors and hospitals. The inclusion of a referral mechanism further enhances collaboration among healthcare providers without compromising patient consent. Experimental results confirm that Traksh effectively ad- dresses the limitations identified in previous research, particularly in terms of practical implementation, user interface design, and entity-based access control. Overall, Traksh provides a scalable, transparent, and tamper-proof solution that can significantly improve trust in electronic medical record (EMR) systems.

REFERENCES

1. S. S. Ali, S. U. Rehman, N. Javaid, M. A. Khan and M. Imran, “Blockchain-based secure data storage for healthcare systems,” IEEE Access, vol. 7, pp. 61661– 61678, 2019.
2. P. Zhang and J. White, “FHIRChain: Applying block- chain to secure and scalable sharing of healthcare data,” Computational and Structural Biotechnology Journal, vol. 16, pp. 267–278, 2018.
3. M. Azaria, A. Ekblaw, T. Vieira and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” in Proc. IEEE 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 2016, pp. 25–30.
4. M. S. Hossain, G. Muhammad, N. Guizani and A. Al- Fuqaha, “Cloud-assisted secure video transmission and sharing framework for healthcare,” IEEE Network, vol. 30, no. 1, pp. 42–49, Jan.–Feb. 2016.
5. H. Dagher, J. Mohler, M. Milojkovic and P. Babu, “An- cile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,” Sustainable Cities and Society, vol. 39, pp. 283–297, May 2018.
6. Zhaoyang Zhang, Dongsheng Cheng, Aizhu Chen, Hanyuan Hou, Kexin Mou, Zhe Jin, Renfei Wang, Lele Liu, Huaimin Pan, Ruichao Hou, Chengping Song, and Panpan Song, "Blockchain-Based Personal Health Records Sharing Scheme with Dual Access Control," Future Generation Computer Systems, vol. 128, pp. 288–299, Mar. 2022.
7. Esposito, R. De Angelis, G. Calabrò, A. Galletta and G. Nicosia, “Blockchain-based sharing and tamper-proof authentication of healthcare data,” in Proc. IEEE Inter- national Symposium on Computer-Based Medical Systems (CBMS), Karlstad, Sweden, 2019, pp. 1-6.
8. S. Roehrs, C. A. da Costa, R. da Rosa Righi, V. F. da Silva and G. B. Schmitt, “OmniPHR: A distributed architecture model to integrate personal health records,” Journal of Biomedical Informatics, vol. 71, pp. 70–81, Jul. 2017.
9. M. Al Omar, M. Z. A. Bhuiyan, A. Basu and S. Kiyomoto, “Privacy-friendly platform for healthcare data sharing using blockchain and differential pri- vacy,” Future Generation Computer Systems, vol. 95, pp. 511–521, 2019.
10. Y. Zhang, J. Ren, W. Lu, P. Zhang, J. Chen, and S. Li, "B-PHR: A Blockchain-Based Framework for Privacy-Preserving Personal Health Record Sharing with Secure Search," IEEE Access, vol. 9, pp. 12909–12921, 2021.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details