Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

A Blockchain-Based On-Chain Storage System for Electronic Health Records

Esha Malavia[1] , Aryan Patankar[2] , Heet Shah[3] , Pravin Hole[4] , Prachi Tawde[5] , Satishkumar Varma[6]

[1]Information Technology, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India
[2]Information Technology, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India
[3]Information Technology, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India
[4]Information Technology, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India
[5]Information Technology, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India
[6]Information Technology, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India

***Abstract*—Hospitals in India face major challenges in securely and efficiently sharing patient records due to centralized systems, privacy risks, and poor interoperability. MediChain offers a practical, secure, and scalable solution for healthcare data sharing tailored to Indian hospitals. Scattered medical records, poor system compatibility, and weak consent practices continue to plague hospitals in India, compromising privacy and slowing down care. This paper proposes MediChain, a blockchain-based framework to support secure, transparent, and patient-centered data sharing. Smart contracts manage user registration, access permissions, and immutable audit logs. Sensitive health information remains encrypted off-chain while blockchain anchors metadata for integrity verification. Implementation on Ethereum Sepolia using synthetic Synthea data demonstrated reliable consent management and record anchoring.**

***Index Terms*—Blockchain, Encryption, Privacy, Healthcare, Decentralized Systems, Smart Contracts**

I. Background and Survey Overview

Blockchain technology has gained prominence as a robust framework for maintaining secure, decentralized, and tamper-resistant digital records. The healthcare domain, which often suffers from fragmented data repositories and poor system interoperability, represents a critical application area for blockchain-based electronic health record (EHR) management. Conventional healthcare information systems predominantly depend on centralized databases, exposing them to risks such as data breaches, unauthorized access, and compromised data integrity. By leveraging features such as immutability, distributed consensus, and provenance tracking, blockchain enables reliable and verifiable patient record management while eliminating reliance on a single controlling authority [1]

A. *Blockchain Fundamentals*

Blockchain functions as a distributed ledger maintained across multiple network nodes, in which each block contains time-stamped transactions that are cryptographically linked to preceding blocks. The use of cryptographic hash functions ensures that any modification to stored data disrupts the integrity of the entire chain, thereby providing strong resistance to tampering. Network consensus is achieved through mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT), which enable agreement on the ledger state without reliance on a centralized authority. Owing to these characteristics, blockchain is well suited for applications that demand secure, trustless collaboration among multiple parties, including healthcare data management systems [2]

B. *Types of Blockchain*

Blockchain networks can be broadly categorized into public, private, consortium, and hybrid architectures based on their governance and access control mechanisms. Public blockchains, such as Ethereum, operate on open participation models where any user can join the network, validate transactions, and view the ledger. While this ensures high transparency and decentralization, public blockchains often face challenges related to scalability, transaction latency, and data privacy, which can limit their suitability for sensitive healthcare applications.

In contrast, private blockchains restrict network participation to authorized entities and are typically managed by a single organization. This controlled access enables higher transaction throughput, reduced latency, and stronger privacy guarantees, making private blockchains more appropriate for hospital-centric deployments where data confidentiality is critical. Consortium blockchains extend this concept by allowing multiple trusted organizations, such as hospitals or healthcare providers, to collectively manage the network. This model balances decentralization and governance, promoting

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

interoperability and shared control without exposing data to the public [1]

Hybrid blockchain systems combine elements of both public and private architectures by maintaining sensitive data and operations within permissioned environments while anchoring selected metadata or verification proofs on public blockchains. This approach enables public verifiability and auditability while preserving regulatory compliance and patient privacy. For electronic health record (EHR) management systems, private and consortium blockchains are generally preferred, as they offer better alignment with healthcare regulations, data protection requirements, and operational scalability.

II. Comparison of Frameworks

Various blockchain frameworks have been developed, each offering different performance characteristics, consensus strategies, and integration flexibility.

TABLE I
Comparison of Blockchain Frameworks

	Permission Type	Consensus Model	Healthcare Suitability
Ethereum		PoS / PoW	High
Hyperledger Fabric	Private	PBFT	High
Corda	Consortium	BFT	High
Quorum	Private	IBFT	Moderate
Polygon	Public	PoS + Layer-2	Moderate

III. On-Chain vs Off-Chain Storage Models

Existing EHR blockchain architectures use either full on-chain storage or hybrid off-chain models. On-chain storage provides maximum immutability and audit transparency but is constrained by scalability and gas cost. Off-chain storage solutions such as IPFS store patient data externally, while only hashes or metadata are stored on-chain.

TABLE II
Comparison of Storage Approaches

Feature	On-Chain Storage	Off-Chain Storage
Immutability	Very High	Moderate
Cost	High	Low
Scalability	Low	High
Security Risk	Minimal	Requires External Trust

IV. Applications of Blockchain Across Domains

Blockchain technology has been widely adopted across diverse domains including finance, digital identity management, supply chain tracking, energy trading, and government record-keeping. Its decentralized and tamper-resistant characteristics have enabled secure transaction processing, transparent auditing, and improved trust across multi-stakeholder systems [3]. Within the healthcare sector, blockchain has shown significant potential in applications such as secure electronic health record (EHR) management, automation of insurance claims, verification of pharmaceutical supply chains to prevent counterfeit drugs, and ensuring data integrity in clinical trials [4]. These practical deployments indicate the increasing maturity and technical feasibility of blockchain-based healthcare solutions. Consequently, they highlight the need for further research and development of fully on-chain EHR systems that can provide enhanced transparency, stronger data integrity guarantees, and improved patient-centric control over medical information [5] [6]

V. Literature Review

A. *Research Gaps*

Despite notable advancements in blockchain-enabled healthcare solutions, the majority of existing frameworks continue to adopt hybrid storage architectures in which sensitive patient information is stored off-chain while only hashes or metadata are anchored on the blockchain. Although this approach attempts to address scalability and storage overhead, it introduces continued reliance on centralized or semi-centralized infrastructure, thereby weakening the core decentralization guarantees of blockchain technology. Such dependencies raise concerns related to data privacy, long-term availability, and trust, particularly when off-chain storage providers become compromised or unavailable. Several studies have also highlighted that fine-grained consent enforcement and comprehensive provenance tracking are often implemented in a limited or fragmented manner, reducing transparency and accountability across the entire lifecycle of medical data [7], [8].

A substantial portion of current research emphasizes conceptual architectures or theoretical evaluations rather than fully deployable and rigorously validated systems. This has resulted in a persistent gap between academic contributions and real-world adoption within operational hospital environments [9], [10]. Moreover, experimental validation using authentic and anonymized clinical datasets remains relatively scarce, limiting the ability to assess system robustness under practical conditions. Critical performance aspects such as scalability, transaction latency, and operational cost are often evaluated in isolation and not under region-specific workloads. This limitation is particularly evident in large, heterogeneous healthcare ecosystems such as those found in India, where infrastructure constraints and high transaction volumes pose additional challenges [4], [11].

These collective limitations highlight the need for a fully on-chain, patient-centric electronic health record management solution that minimizes dependence on external infrastructure while providing strong guarantees of data integrity, traceability, and transparency [12]. Such a system should enable verifiable and decentralized access control, enforce patient consent in a systematic manner, and maintain tamper-resistant audit trails that can be independently validated by authorized stakeholders. Recent studies further emphasize that addressing interoperability barriers and deployment challenges is essential

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

for achieving large-scale adoption of blockchain-based EHR systems [6], [13]. Addressing these challenges is critical for enabling secure, efficient, and trustworthy healthcare data exchange in real-world clinical environments, thereby improving institutional workflows, strengthening patient trust, and supporting long-term healthcare digital transformation [14], [15].

B. *Conclusion on Observations*

A comparative review of existing studies indicates that blockchain technology consistently improves data integrity, immutability, and traceability within healthcare systems. At the same time, the literature highlights several practical limitations, including transaction latency, cost efficiency, and challenges related to user accessibility. [16] Many proposed solutions remain largely conceptual, with limited implementation or insufficient integration into real hospital infrastructures. These observations underline the need to balance strong technical design with practical clinical usability [17]. The proposed MediChain framework responds to these challenges by implementing a fully decentralized and provenance-aware electronic health record system on the Ethereum Sepolia network. The system is evaluated using synthetic datasets and anonymized patient records from JJ Hospital, thereby narrowing the gap between theoretical research and deployable healthcare solutions.

VI. Proposed System

A. *Research Objectives*

MediChain is a blockchain-driven electronic health record management system designed to ensure data provenance, integrity, and transparency without relying on centralized storage infrastructure. The primary objective of this research is to develop a fully on-chain e-healthcare framework that provides tamper-resistant medical data storage by leveraging the inherent immutability and cryptographic hashing mechanisms of blockchain technology. The system incorporates provenance awareness to support accountability and transparency by enabling every operation, including record creation, modification, and access, to be time-stamped and traceable to its originating entity.

The proposed framework is implemented using the Ethereum Sepolia test network in conjunction with a Next.js-based frontend, enabling seamless interaction between deployed smart contracts and the user interface. The system is evaluated using synthetic Synthea datasets as well as anonymized real-world hospital records obtained from JJ Hospital to validate design correctness and data traceability. In addition, MediChain adopts blockchain-based authentication mechanisms to achieve decentralized access control, thereby eliminating reliance on conventional username–password authentication schemes.

B. *System Architecture*

1) Frontend: The user interface of the proposed system is built using Next.js, a React-based framework that supports the development of efficient, responsive, and scalable web applications. For visual styling, Tailwind CSS is employed, enabling a consistent, flexible, and professional design while simplifying layout customization.

2) Blockchain Integration: The system is deployed and tested on the Ethereum Sepolia test network, which serves as a controlled blockchain environment for smart contract execution. Sepolia closely replicates real-world blockchain behavior while allowing experimentation and validation without the financial overhead associated with mainnet deployment.

3) Wallet Integration: MetaMask is integrated as the primary wallet interface to facilitate user authentication and transaction authorization. Through MetaMask, users can securely connect their blockchain accounts, approve transactions, and interact directly with the deployed smart contracts in a decentralized manner.

4) Smart Contracts: The smart contracts forming the core logic of the system are developed and deployed using the Remix IDE, a web-based development platform tailored for Solidity-based applications. These contracts manage healthcare record operations, enforce access control policies, and govern transaction execution, ensuring secure and reliable handling of electronic health records [18]

C. *Data Flow*

The system follows a well-defined workflow to support the secure storage, modification, and retrieval of healthcare information across the blockchain network.

1) User Interaction: Users initiate interaction with the system by connecting their MetaMask wallet, which serves as the mechanism for identity verification through blockchain credentials. Once the wallet connection is successfully established, users are granted the ability to submit new healthcare records, update existing information, or view stored medical data based on their authorized access level.

2) Data Submission: When healthcare information such as patient medical records or practitioner details is entered, the data is transmitted from the frontend interface to the blockchain layer. Each submission generates a transaction that is digitally signed using the user's wallet, ensuring authenticity, integrity, and secure transmission of the data to the network.

3) Smart Contract Execution: The signed transaction invokes the appropriate smart contract function responsible for processing the requested operation, such as record creation or modification. Upon execution, the healthcare data is recorded on the blockchain in an immutable manner, providing transparency and resistance to unauthorized alteration.

4) Data Retrieval: To access stored information, users interact with the system's frontend, which communicates with the blockchain by invoking relevant smart contract functions. The requested data is then retrieved from the blockchain and presented to the user, ensuring consistent and verifiable access to healthcare records.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

TABLE III
COMPARISON WITH EXISTING BLOCKCHAIN-BASED HEALTHCARE SYSTEMS

Reference	Focus Area	Key Contribution	Distinction from MediChain
Agnal et al., IEEE ICCCT (2025)	Decentralized EMR architecture	Presents a blockchain-driven framework for electronic medical records emphasizing data integrity and system interoperability.	The work remains primarily architecture-centric, while MediChain delivers a fully implemented on-chain system evaluated using anonymized hospital datasets.
Zilong and Alobaedy, IEEE EECT (2025)	Secure blockchain-based EHR management	Investigates security, scalability, and access control aspects of blockchain-enabled healthcare data systems.	MediChain enhances this approach by integrating complete on-chain provenance tracking and systematic consent enforcement.
Zhang et al., IEEE IoT Journal (2025)	Comprehensive survey of blockchain in healthcare	Analyzes current blockchain applications, challenges, and emerging research directions across healthcare ecosystems.	While survey-focused, MediChain directly addresses highlighted limitations through a deployable and validated on-chain implementation.
Kröckel et al., IET Blockchain (2025)	Blockchain adoption and value realization	Examines patient benefits, organizational value, and adoption barriers associated with blockchain in healthcare.	MediChain complements this perspective by concentrating on technical execution and decentralized system feasibility.
Madhumala et al., Springer IC3N (2025)	Efficient healthcare data management using blockchain	Proposes a blockchain-based healthcare framework aimed at improving data security and operational efficiency.	In contrast to hybrid storage approaches, MediChain anchors records and provenance directly on-chain without external dependencies.
Patil et al., IEEE AMATHE (2025)	Blockchain-enabled EHR security mechanisms	Implements smart contract-based authorization to enhance EHR security and stakeholder coordination.	MediChain extends this model by incorporating immutable audit trails and patient-centric consent control.

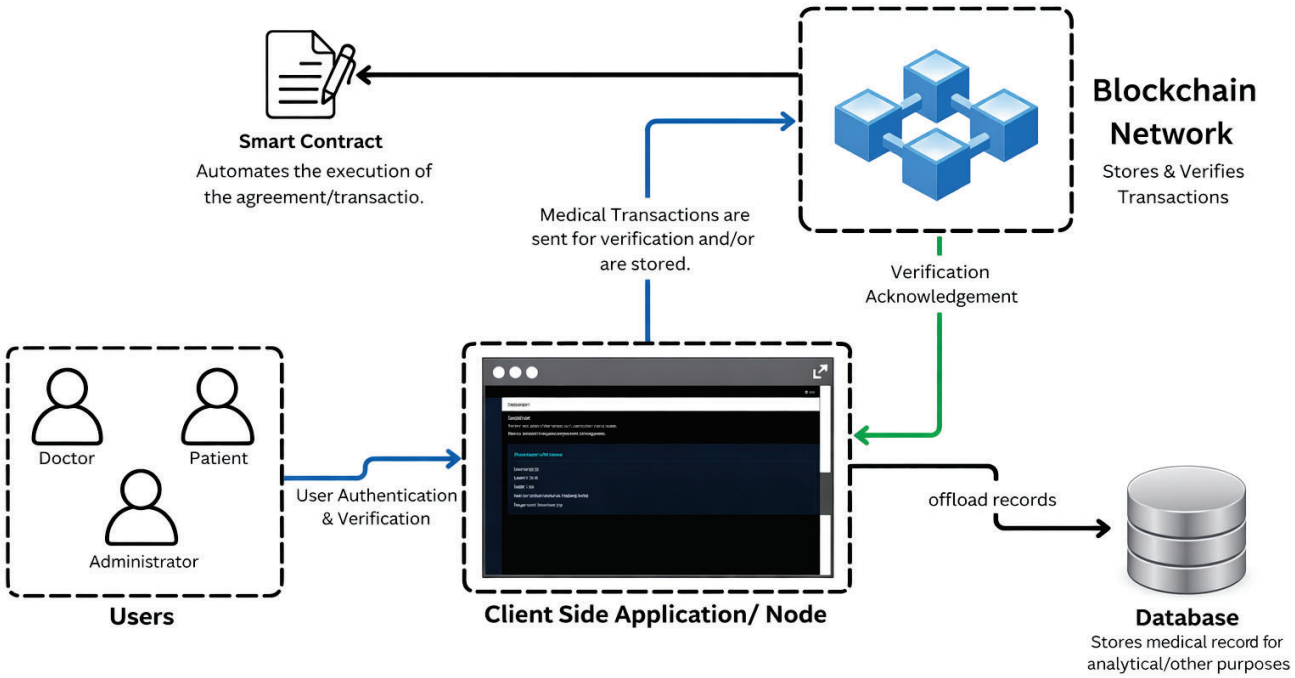

Fig. 1. Interaction between users, Next.js interface, and Ethereum smart contracts.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

D. Functionality of Smart Contracts

The MediChain architecture is derived from provenance-aware blockchain models proposed in earlier research, while simplifying the design into a single-layer, fully on-chain framework. In this architecture, both metadata and patient health records are committed directly to the Ethereum blockchain, eliminating reliance on external storage layers and ensuring consistent provenance and integrity guarantees.

1) Components:

a) User Interface Layer (Next.js Frontend): The user interface layer is implemented using Next.js 14, a React-based framework that supports server-side rendering and API integration. MetaMask is incorporated to enable cryptographic authentication and secure transaction signing. The frontend provides role-specific dashboards that allow patients to upload records and view provenance information, doctors to request and access authorized records, and administrators to perform ledger auditing and monitoring activities.

b) Blockchain Layer (Ethereum Sepolia): The blockchain layer constitutes the core logic of MediChain and is implemented through Solidity-based smart contracts deployed on the Ethereum Sepolia test network. This layer manages user role registration, health record lifecycle operations, and provenance tracking. Role mappings for patients, doctors, and administrators are maintained to enforce access control policies, while health records are created, updated, and retrieved directly on-chain. In addition, every transaction event is recorded to preserve lineage and traceability. All transactions are immutably stored on the blockchain, with data represented as key–value pairs in the form of a record identifier mapped to a hashed representation of patient data. Provenance information links each modification to its previous state using block timestamps and sender addresses, enabling complete traceability of record evolution.

c) Backend / API Layer (Next.js API Routes): The backend layer is implemented using Next.js API routes and serves as an intermediary between the frontend and the blockchain network. This layer utilizes the Ethers.js library to interact with blockchain RPC endpoints, facilitating secure read and write operations. It manages user authentication, serializes healthcare data prior to blockchain submission, and handles transaction execution. Additionally, the backend maintains provenance indexing and local caching mechanisms to improve system responsiveness during data visualization and querying.

d) Data Storage Layer (On-Chain): The data storage layer operates entirely on-chain, where hashed patient data, clinical summaries, and diagnostic results are permanently recorded on the Ethereum ledger. Prior to submission, each data element is processed using the Keccak-256 hashing algorithm to ensure immutability and resistance to tampering. Blockchain metadata, including block numbers, timestamps, and sender addresses, inherently serves as verifiable provenance evidence, allowing the origin and chronological sequence of medical records to be independently validated.

E. Testing and Network Deployment

The Ethereum Sepolia test network is utilized as a secure and cost-efficient platform for system deployment and validation. All system operations, including smart contract execution, data storage, and data retrieval processes, are extensively tested within this environment to verify functional correctness, reliability, and security prior to any consideration of mainnet deployment.

F. Datasets Used

1) Connecting the Wallet: Users gain access to the system by connecting their MetaMask wallet, which serves as the primary mechanism for authentication. The wallet integration verifies user credentials through blockchain-based identity confirmation, enabling secure interaction with the system.

2) Performing Transactions: Once authenticated, users can submit healthcare-related information, approve blockchain transactions, and securely store data on the distributed ledger. All transactions are executed through wallet authorization, ensuring integrity and non-repudiation.

3) Viewing Records: Healthcare records stored on the blockchain are retrieved through smart contract calls and presented to users in a clear and user-friendly interface. This approach ensures seamless access to information while maintaining data consistency and transparency.

4) Synthea Dataset: Synthetic healthcare data generated using the open-source Synthea simulator is utilized for system evaluation. This dataset is employed to stress-test blockchain storage mechanisms, measure transaction latency, and assess the effectiveness of provenance querying under controlled conditions.

5) Hospital Dataset: Anonymized patient records obtained from JJ Hospital, Mumbai, are used to evaluate real-world applicability of the proposed system. All personally identifiable information is removed prior to experimentation to ensure privacy compliance, allowing the dataset to be safely used for validating system integration and performance.

VII. Results

The proposed blockchain-based healthcare data management system was deployed and evaluated on the Ethereum Sepolia test network. Comprehensive testing was conducted to validate system functionality, security properties, and performance characteristics under realistic operating conditions.

A. Functional Validation

The system successfully demonstrated all essential operational capabilities required for electronic health record management. Users were able to add patient medical information, including basic medical records, health conditions, and prescribed medications, through the frontend interface. Stored healthcare records were accurately retrieved from the blockchain through smart contract interactions, ensuring consistency between submitted and fetched data. In addition, authorized users were able to modify specific record attributes, such as health status updates or medication schedules, with

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

all changes correctly reflected during subsequent retrieval operations.

B. Security Verification

Evaluation of system security confirmed the presence of strong protective mechanisms. The inherent immutability of the blockchain ensured that all healthcare records remained resistant to unauthorized modification, preserving data integrity. User authentication and transaction approvals were secured through MetaMask wallet integration, which maintained confidentiality of private keys and prevented unauthorized access. Furthermore, access control policies enforced at the smart contract level ensured that sensitive operations could only be executed by users with appropriate permissions.

C. Performance Metrics

Performance analysis conducted on the Sepolia test network indicated that the system operates within acceptable efficiency bounds for a blockchain-based healthcare application. The average transaction confirmation time was observed to be approximately 12 seconds, while typical operations incurred gas costs of around 0.00021 ETH. Network latency during peak usage periods remained minimal, generally under 2 seconds, demonstrating stable system responsiveness under testing conditions.

Acknowledgment

The authors would like to sincerely thank their project guide for his continuous guidance and support throughout the course of this work. His valuable insights and technical expertise played a significant role in the successful design, implementation, and evaluation of the blockchain-based healthcare data management system. The authors are also grateful for his consistent encouragement and constructive feedback, which were essential in addressing challenges and achieving the objectives of this project.

VIII. Conclusion

This work demonstrates the effectiveness of integrating blockchain technology into healthcare data management to enable secure, transparent, and tamper-resistant sharing of medical information. The proposed MediChain framework addresses key challenges in electronic health record systems, including data integrity, privacy preservation, and scalability, through a fully on-chain, provenance-aware design. By leveraging smart contracts, cryptographic hashing, and decentralized access control mechanisms, the system ensures reliable record management without reliance on centralized storage infrastructure.

Experimental evaluation on the Ethereum Sepolia test network confirms the feasibility of the proposed approach under realistic conditions, with acceptable transaction latency, low operational cost, and strong security guarantees. While the framework successfully validates the practicality of blockchain-based EHR management, challenges related to system interoperability, large-scale deployment, and integration with existing healthcare infrastructure remain. Future work will focus on addressing these limitations through extended real-world testing and optimization, with the objective of improving operational efficiency, enhancing patient care, and strengthening the security of sensitive medical data.

References

[1] J. Zhang *et al.*, "Blockchain empowerment in healthcare: A survey," *IEEE Internet of Things Journal*, vol. 12, no. 16, pp. 32 516–32 537, 2025.

[2] C. M. Selvamuthu, M. Salwin, D. Akshitha, S. D. Jain, V. K. Kavya, O. M. Kumar, and V. Karwa, "Transforming healthcare with blockchain: A study on its applications, benefits and barriers," *Journal of Pharmaceutical and Medical Sciences*, 2025.

[3] P. Kröckel, N. Wickramasinghe, J. van de Logt, A. Andargoli, N. Ulapane, and F. Bodendorf, "Blockchain in healthcare: Bridging the business value and patient benefit," *IET Blockchain*, 2025.

[4] B. W. Aboshosha, "Enhancing internet of things security in healthcare using a blockchain-based lightweight hashing system," *BMC Chemistry / SpringerOpen*, 2025. [Online]. Available: https://bjbas.springeropen.com/articles/10.1186/s43088-025-00644-8

[5] S. B. Othman and Others, "Leveraging blockchain and iomt for secure and interconnected healthcare systems," *Nature/IEEE Journal*, 2025.

[6] P. M. Katoon and S. Turukmane, "Interoperable blockchain network for healthcare data using cross-chain middleware architecture," *Journal Name (Springer)*, 2025, springer publication with cross-chain EHR middleware for Hyperledger and Ethereum. [Online]. Available: https://link.springer.com/article/10.1007/s44163-025-00564-7

[7] S. Agnal, V. R. C. K, D. K. S, and A. U. G, "Blockchain based electronic medical health records framework," in *2025 International Conference on Computing and Communication Technologies (ICCCT)*. Chennai, India: IEEE, 2025, pp. 1–5.

[8] S. K. Sharma and F. Parwej, "Design and implementation of a blockchain-based secure data sharing framework to enhance the healthcare system," *Blockchains*, 2025.

[9] P. L., P. G., R. Sagar, Sujay, A. S., and S. B., "Blockchain-powered electronic health record system for enhanced security," in *2025 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE)*. Shivamogga, India: IEEE, 2025, pp. 1–6.

[10] K. Danilchenko *et al.*, "Mrc: a medical-record chain system based on blockchain," *Blockchain in Healthcare Today*, 2025.

[11] K. Wang, P. Lu, and Z. Xin, "Research on blockchain privacy preservation in healthcare systems," in *2025 11th International Symposium on System Security, Safety, and Reliability (ISSSR)*. Guiyang, China: IEEE, 2025, pp. 286–290.

[12] D. Zilong and M. M. Alobaedy, "Blockchain-based healthcare data management: Analysis and evaluation of security, scalability, and compliance for electronic health records (ehrs)," in *2025 5th International Conference on Advances in Electrical, Electronics and Computing Technology (EECT)*. Guangzhou, China: IEEE, 2025, pp. 1–7.

[13] K. Li, A. Lohachab, M. Dumontier, and V. Urovi, "Privacy preservation in blockchain-based healthcare data sharing: A systematic review," *Journal Name (Springer)*, 2025. [Online]. Available: https://link.springer.com/article/10.1007/s12083-025-02148-9

[14] M. Damar, "Patient data, research, and institutional processes in blockchain healthcare," *Blockchain Healthcare Today*, 2025.

[15] A. Ullah *et al.*, "Toward blockchain based electronic health record adoption and interoperability," *Nature Reports / Scientific Journal*, 2025.

[16] A. A. Almazroi, "Innovative ai ensemble model for robust and optimized blockchain-based healthcare systems," *Network Modeling Analysis in Health Informatics and Bioinformatics*, vol. 14, no. 6, 2025.

[17] A. A. Ali, "Blockchain-enabled federated learning for privacy preservation in electronic health records," *Journal / Conference Name*, 2025.

[18] R. B. Madhumala, C. K. Samal, A. Maroju, B. Brahma, S. Aggarwal, and M. A. Parvez, "Utilization of blockchain technology in designing an efficient healthcare system," in *Proceedings of the Fourth International Conference on Computing and Communication Networks*. Springer Nature Singapore, 2025.