Surya R, 2026, 14:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Blockchain-Enabled Healthcare Data Transmission and Real-Time Patient Monitoring System

[1] Surya R , [2] Dr.R.Nagarajan Msc.,Mphil.,phd
Department of Computer Science,
Sri Ramakrishna College of Arts & Science (Formerly S.N.R. Sons College), Coimbatore – 641 006

Abstract- The Healthcare Sector Faces Major Challenges In Maintaining Secure, Private, And Real-Time Access To Patient Medical Records. Traditional Centralized Systems Are Vulnerable To Data Breaches, Unauthorized Access, And Single Points Of Failure, Which Can Critically Impact Patient Safety. To Overcome These Issues, This Paper Proposes Healthchain, A Blockchain- Enabled Healthcare Data Transmission And Real-Time Patient Monitoring System. Healthchain Employs A Python-Based Blockchain With SHA-256 Proof-Of-Work, RSA-2048 Cryptography, And AES-256 Encryption To Securely Store And Protect Patient Records On An Immutable Distributed Ledger. The System Continuously Monitors Patient Vitals Such As Heart Rate (BPM) And Blood Oxygen (Spo_2) And Updates Them In Real Time Using Websocket Communication. Critical Health Data Is Automatically Recorded On The Blockchain, While Smart Contracts Manage Emergency Access And Patient Consent. The System Is Built Using Flask, Flask-Socketio, Mongodb, And Pydantic, With A Responsive Frontend Developed Using Jinja2 Templates And Chart.Js For Real-Time Visualization. It Also Supports Role-Based Access Control For Admins, Doctors, And Patients, Along With Automated PDF Health Reports. Healthchain Demonstrates How Blockchain, Real-Time Data Monitoring, And Secure Cryptographic Techniques Can Be Integrated To Create A Tamper-Proof, Transparent, And Patient-Centric Healthcare Data Management System.

Keywords: Blockchain, Healthcare Data Management, Real-Time Monitoring, SHA-256, AES-256, RSA-2048, Smart Contracts, Role-Based Access Control, Flask, Patient Privacy

I. INTRODUCTION

The healthcare sector faces significant challenges in ensuring the security, privacy, and real-time accessibility of patient medical records. Traditional centralized Electronic Health Record (EHR) systems, while widely adopted, introduce critical vulnerabilities: they create single points of failure, expose sensitive data to breaches, and rely on the security posture of individual institutions. As ransomware attacks and data theft incidents in healthcare continue to rise globally, there is an urgent need for a structurally more resilient approach to medical data management.

Blockchain technology, originally developed as the distributed ledger underlying Bitcoin, has matured into a general-purpose infrastructure for tamper-proof, decentralized data storage. Its core properties— immutability, cryptographic integrity, and transparent audit trails—make it particularly well-suited for healthcare applications where data accuracy and accountability are paramount. When combined with modern cryptographic techniques and real-time communication protocols, blockchain can serve as the foundation for a healthcare data system that is both secure and responsive.

This paper proposes HealthChain, a blockchain-enabled system for healthcare data transmission and real-time patient monitoring. The system integrates SHA-256 Proof-of-Work blockchain, RSA-2048 asymmetric encryption, and AES-256 data protection to ensure that all patient records stored on the ledger are cryptographically secured and tamper-proof. A real-time vital monitoring module continuously streams Heart Rate and SpO_2 data to physician dashboards using WebSocket technology. Role-based access control governs system access for patients, doctors, and administrators, while smart

contract logic automates consent management and emergency access protocols.

II. LITERATURE REVIEW

Extensive research has demonstrated the inadequacy of conventional EHR architectures. Centralized storage systems such as Epic and Cerner, while standardizing clinical data exchange through HL7 and FHIR protocols, remain fundamentally susceptible to breaches and insider threats [1]. Studies have consistently identified data integrity, patient consent management, and interoperability as unresolved challenges in legacy healthcare systems [2].

Nakamoto's foundational work on distributed ledger technology established the basis for trustless record-keeping without a central authority [3]. Swan extended this framework to institutional applications, demonstrating that blockchain could serve as a general- purpose platform for social and administrative systems [4]. Christidis and Devetsikiotis showed that smart contracts could automate complex transactional workflows, a property directly applicable to healthcare consent and access management [5].

Zheng et al. provided a comprehensive analysis of blockchain architectures and consensus mechanisms suitable for enterprise deployment [6]. Healthcare-specific applications have been explored by researchers proposing blockchain for electronic medical records, drug supply chain integrity, and clinical trial data management [7], [8]. The present work builds on these contributions by proposing a complete, production- oriented architecture that integrates blockchain storage, real-time monitoring, and cryptographic access control within a single platform.

III. EXISTING SYSTEM

Centralized EHR Architecture

Current healthcare data management relies primarily on centralized EHR systems. A single institutional server or cloud service holds all patient records, creating a critical vulnerability: any breach, ransomware event, or administrative error at the central node can compromise an entire patient population's health data. Citizens and healthcare providers have no independent means of verifying that records presented to them are authentic and unmodified.

Limitations of Existing Systems

Manual and paper-based processes remain prevalent in many facilities, making patient data management slow and error-prone. Centralized databases increase the risk of unauthorized access and breaches. Patients and providers frequently face difficulty accessing accurate, up-to-date medical records. Poor integration between hospitals leads to duplicate or inconsistent patient records. Traditional systems lack advanced security mechanisms such as end-to-end encryption and distributed immutability.

IV. PROPOSED SYSTEM

HealthChain proposes a decentralized architecture that overcomes the limitations of traditional healthcare systems by integrating blockchain technology, cryptographic security, and real-time data streaming. Patient vital events and medical transactions are recorded on a custom SHA-256 Proof-of-Work blockchain, ensuring that any modification of past records becomes immediately detectable. The system continuously broadcasts Heart Rate and SpO_2 data every two seconds using Flask-SocketIO, with critical events stored on the blockchain as tamper-proof records.

Immutable Blockchain Record Storage

Every medical transaction—encompassing patient data, doctor interactions, diagnosis records, and vital sign events—is encoded as a structured block and appended to the chain. Each block carries the SHA-256 hash of the preceding block, creating an unbroken, chronologically ordered chain of custody that serves as an incontrovertible audit trail. Once written, records cannot be deleted or silently modified.

Smart Contract-Based Access Management

Patient consent and emergency access workflows are governed by smart contract logic deployed within the application. These contracts encode the conditions under which medical data may be accessed. When all preconditions are satisfied—such as a valid RSA-2048 encrypted consent token issued by the patient—the contract executes automatically, granting time-limited access without manual administrative intervention.

Role-Based Access Control

A multi-tier access control framework distinguishes between patients, doctors, and administrators. Patients access their own records and control consent settings. Doctors can view authorized patient data and monitor real-time vitals. Administrators manage user accounts and audit system activity. This segregation ensures that sensitive medical information is only accessible to verified, authorized parties.

V. METHODOLOGY

The development of HealthChain followed a structured methodology designed to ensure security, correctness, and usability at each stage of the development pipeline. The process moves from user onboarding through data submission, blockchain recording, real-time monitoring, and finally to access control and verification.

User Registration and Authentication

All participants—patients, doctors, and administrators— complete a digital onboarding process. Authentication combines email and password verification with role assignment. Upon registration, cryptographic key pairs are generated for each user: RSA-2048 public and private keys are created and stored securely using AES- 256 encryption to protect private keys at rest.

Medical Data Submission and Encryption

Patients upload medical records and health data through the web interface. The system processes this data using AES-256 encryption for storage and RSA-2048 for key exchange, ensuring that sensitive medical information remains protected both in transit and at rest. Structured forms enforce input validation to prevent malformed data from entering the system.

Blockchain Transaction Recording

Encrypted data is recorded in the blockchain ledger using SHA-256 hashing. Each new blockchain block contains the patient email, doctor email, medical record reference, previous block hash, current block hash, and a timestamp. The chaining of hashes makes retrospective modification computationally infeasible. All major system events including vitals recording, consent approval, and emergency access are logged as immutable blockchain entries.

Real-Time Vital Monitoring

The system continuously broadcasts patient vital parameters—Heart Rate (BPM) and Blood Oxygen Saturation (SpO_2)—via Flask-SocketIO WebSocket connections at two-second intervals. Doctors receive live updates on their dashboards through Chart.js visualizations. Critical threshold violations trigger automated alerts, which are simultaneously recorded on the blockchain as tamper-proof event entries.

Access Verification and Audit

Authorized users may query the blockchain at any time to retrieve current and historical records. The query interface returns cryptographically signed data that can be independently verified against the chain. All data access events are logged, ensuring a complete and transparent audit trail that supports accountability for every interaction with patient data.

VI. SYSTEM ARCHITECTURE

The HealthChain architecture comprises five integrated layers: a frontend presentation layer built with HTML5, CSS3, JavaScript, and Jinja2 templates; a backend processing layer powered by Python and the Flask framework; a real-time communication layer using Flask-SocketIO; a storage layer using MongoDB with blockchain transaction tables; and a cryptographic security layer implementing SHA-256, RSA-2048, and AES-256. Each medical event flows from the user interface through authentication, encryption, blockchain recording, and finally to

persistent storage, with all interactions logged in the immutable ledger.

VII. APPLICATIONS

Secure Patient Record Management
The primary application is the secure, tamper-proof storage and management of patient medical histories. Healthcare institutions can retire centralized record systems in favor of a distributed ledger that resists breaches and provides a complete, verifiable audit trail for every record modification.

Real-Time ICU and Remote Monitoring
The continuous vital sign monitoring module directly supports intensive care unit environments and remote patient monitoring programs. Physicians receive live Heart Rate and SpO_2 feeds with automated alerting, enabling faster clinical response to deteriorating patient conditions.

Consent and Emergency Access Management
Smart contract-driven consent management gives patients granular control over who can access their data and for how long. Emergency access protocols allow authorized physicians to obtain time-limited access to records in critical situations, with all such access events permanently logged on the blockchain for accountability.

Regulatory Compliance and Audit
The immutable blockchain audit trail supports healthcare regulatory compliance requirements. Every data access, modification, and transaction is permanently recorded with a timestamp, providing regulators and auditors with reliable evidence of data governance practices.

VIII. ADVANTAGES

Data Integrity and Tamper-Resistance
The SHA-256 cryptographic architecture makes unauthorized modification of stored records computationally infeasible. Each transaction is chained to its predecessor via hash linkage, ensuring that any attempt to alter historical data is immediately detectable.

Enhanced Patient Privacy
RSA-2048 encrypted consent tokens give patients direct control over data access. AES-256 encryption protects sensitive records at rest. Role-based access control ensures that no user can access data beyond their authorized scope.

Real-Time Clinical Intelligence
WebSocket-powered vital monitoring delivers live patient data to physicians without polling delays. Automated threshold alerts reduce response times to critical health events, directly supporting better patient outcomes.

Cost-Effective Open-Source Stack
HealthChain is built entirely on open-source technologies—Python, Flask, MongoDB, and standard cryptographic libraries—requiring no proprietary software licenses. This makes the system economically accessible to healthcare institutions of varying sizes.

IX. CHALLENGES & ETHICAL CONSIDERATIONS

Scalability and Performance
SHA-256 Proof-of-Work blockchain operations introduce computational overhead that may limit throughput under high transaction volumes. Future iterations should evaluate lighter consensus mechanisms optimized for healthcare use cases where full decentralization is less critical than performance.

Legal and Regulatory Alignment
Blockchain-recorded medical records may not currently hold equivalent legal status to traditionally certified documents in all jurisdictions. Healthcare institutions adopting this architecture should seek legal counsel regarding compliance with applicable regulations such as HIPAA and GDPR before production deployment.

Patient Digital Literacy

The system's consent management and cryptographic key infrastructure require a degree of digital literacy from patients. Effective deployment would necessitate parallel investment in patient education and accessible support pathways to ensure equitable participation across all demographics.

X. CONCLUSIONS

The system's consent management and cryptographic key infrastructure require a degree of digital literacy from patients. Effective deployment would necessitate parallel investment in patient education and accessible support pathways to ensure equitable participation across all demographics.

This paper has presented the design and implementation of HealthChain, a blockchain-enabled healthcare data transmission and real-time patient monitoring system. The motivation stems from clear and documented shortcomings in centralized EHR architectures—their susceptibility to breaches, opacity of audit trails, and inability to provide patients with meaningful control over their own data. These are not incidental problems but structural consequences of concentrating sensitive health information in single-authority systems.HealthChain addresses this gap by recording all medical transactions on an SHA-256 Proof-of-Work blockchain, protecting data with RSA-2048 and AES-256 cryptography, automating consent and access through smart contract logic, and delivering real-time vital monitoring via WebSocket communication. Together these components produce a healthcare data platform that is more resilient, more trustworthy, and more responsive than any centralized alternative. Future research should focus on scalability under high transaction volumes, integration protocols for interoperability with existing EHR systems, and advanced privacy-preserving techniques such as zero-knowledge proofs for scenarios requiring verification without disclosure of personal health information.

XI. ACKNOWLEDGEMENT

The author thanks the Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, for providing the academic infrastructure and environment that made this research possible. Special appreciation is extended to Dr. S. Mohana, Assistant Professor, for continuous guidance and support throughout the development of this project.

REFERENCES

1. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
2. M. Iansiti and K. R. Lakhani, "The Truth About Blockchain," Harvard Business Review, vol. 95, no. 1, pp. 118-127, 2017.
3. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, 2016.
4. M. Swan, Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015.
5. A. Azaria et al., "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2nd Int. Conf. on Open and Big Data, 2016.
6. Z. Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," IEEE Int. Congr. Big Data, 2017.
7. A. Ekblaw et al., "A Case Study for Blockchain in Healthcare: MedRec Prototype," IEEE Open & Big Data Conf., 2016.
8. D. Bhattacharya et al., "Blockchain-Based Healthcare Data Management," J. Medical Systems, vol. 43, no. 10, 2019.
9. A. Antonopoulos, Mastering Bitcoin. O'Reilly Media, 2nd Edition, 2017.
10. D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps. Apress, 2017.
11. W. Stallings, Cryptography and Network Security: Principles and Practice. Pearson, 7th Edition, 2017.

12. G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, 2014.