

# Jeevanlocker: A Survey on Secure Blockchain Healthcare Records

Prashanth H. S<sup>1</sup>, Mohammad Sufiyyaan Meccai<sup>2</sup>, Pranav Shastri<sup>3</sup>, Punith P<sup>4</sup>, Pranav C M<sup>5</sup>

<sup>1</sup>Assistant Professor, Department of Computer Science and Engineering,

K. S. Institute of Technology, Bengaluru, Karnataka, India

<sup>2345</sup>Department of Computer Science and Engineering,

K. S. Institute of Technology, Bengaluru, Karnataka, India

\*\*\*

**Abstract** - Healthcare institutions commonly maintain patient records in isolated databases, leading to fragmented medical information, repeated diagnostic procedures, delayed treatment, and reduced interoperability between hospitals. Traditional centralized healthcare systems are also vulnerable to unauthorized access, data tampering, and privacy breaches. This paper proposes JeevanLocker, a blockchain-based unified medical record management system designed to provide secure, patient-centric, and consent-driven healthcare data sharing. The proposed framework integrates encrypted medical record storage, blockchain-based audit logging, smart contracts, and role-based access control to improve transparency, security, and interoperability. Hospitals and doctors can access patient records only after receiving explicit patient approval, while all access requests and consent events are immutably recorded on the blockchain. The system also introduces a secure Break-Glass emergency access mechanism that allows temporary access during critical situations while maintaining complete auditability and patient notification. JeevanLocker aims to enhance healthcare efficiency, strengthen patient privacy, and establish trust between healthcare providers and patients through secure decentralized healthcare data management.

**Key Words:** Blockchain, Electronic Health Records, Healthcare Security, Smart Contracts, Medical Data Privacy, Consent-Based Access Control.

## 1. INTRODUCTION

The adoption of Electronic Health Record (EHR) systems has significantly improved digital healthcare management by enabling hospitals and healthcare providers to store patient information electronically. However, most healthcare institutions continue to maintain separate and isolated databases, resulting in fragmented medical records and limited interoperability between hospitals. Patients receiving treatment from multiple healthcare providers are often required to repeat diagnostic tests because previous

records are inaccessible, leading to increased healthcare costs and delayed treatment.

Conventional healthcare systems also face major security and privacy challenges due to centralized data storage

architectures. Medical records contain highly sensitive personal information and are vulnerable to unauthorized access, insider threats, data breaches, and accidental modification. Existing systems often fail to provide transparent patient-controlled access management, reducing trust between patients and healthcare providers.

Blockchain technology offers a secure and tamper-resistant solution for healthcare data management through decentralized transaction logging and immutable audit records. Smart contracts further enable automated consent management and secure authorization workflows. This paper proposes JeevanLocker, a blockchain-enabled unified medical record management system that provides secure, consent-based healthcare data sharing across multiple healthcare institutions.

The proposed framework stores medical records in encrypted storage while maintaining immutable blockchain logs for consent approvals, access requests, and emergency activities. The system additionally integrates role-based access control and a Break-Glass emergency access mechanism for critical medical situations. JeevanLocker aims to improve healthcare interoperability, strengthen patient privacy, and establish a secure patient-centric healthcare ecosystem.

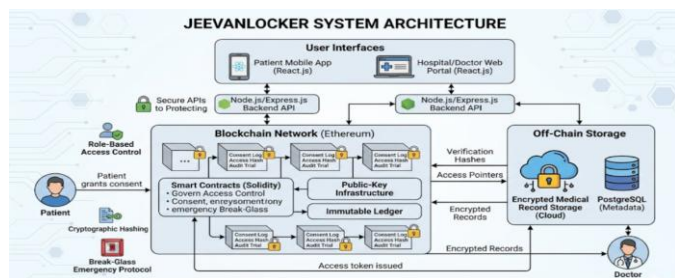


Fig1 - Proposed JeevanLocker System Architecture

## 2.LITERATURE

### SURVEY

Blockchain technology has become an important solution for improving healthcare data security, transparency, and interoperability. Several researchers have proposed blockchain-based Electronic Health Record (EHR) systems to address issues related to medical data privacy and secure healthcare information sharing.

Azaria et al. proposed MedRec, a blockchain-based framework for decentralized medical data access and permission management. The system improved transparency and patient-controlled access but faced scalability challenges in large healthcare environments.

Chenthara et al. introduced HealthChain, which combined encrypted off-chain storage with blockchain audit logging to improve confidentiality and reduce storage overhead. However, interoperability and emergency access handling remained limited.

Dubovitskaya et al. developed ACTION-EHR, a patient-centric healthcare data management system for secure medical information sharing between institutions. Although the framework improved security and transparency, transaction latency remained a challenge.

Shahnaz et al. proposed a blockchain-enabled EHR system focused on improving medical data integrity through decentralized verification and cryptographic hashing. The framework strengthened audit transparency but lacked detailed patient consent management.

Yaqub et al. introduced a blockchain-enabled policy-based access control mechanism using smart contracts for flexible healthcare authorization and improved privacy management.

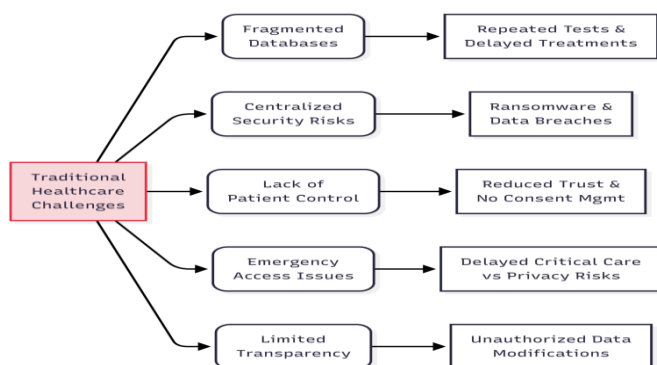
Recent research indicates that hybrid architectures combining encrypted cloud storage with blockchain-based

audit logging provide better scalability, transparency, and interoperability for healthcare systems. However, challenges such as scalability limitations, emergency access management, and interoperability with existing hospital systems still remain unresolved.

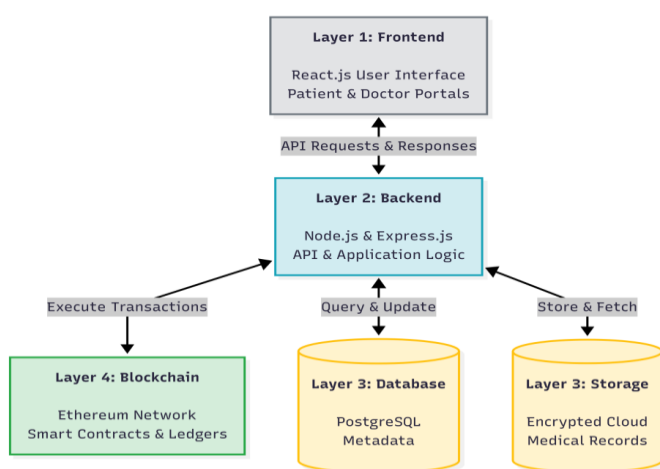
The proposed JeevanLocker framework addresses these limitations through encrypted medical record storage, consent-driven access control, blockchain-based immutable audit logging, role-based authorization, and a secure Break-Glass emergency access mechanism. The system aims to provide a secure, transparent, and patient-centric healthcare management solution.

### 3. PROBLEM STATEMENT

Healthcare institutions currently maintain patient records in isolated databases managed independently by hospitals, clinics, and diagnostic centers. This fragmented approach creates challenges in healthcare interoperability, leading to repeated medical tests, delayed treatments, increased healthcare costs, and inefficient patient management. Traditional healthcare systems also face serious security and privacy concerns due to centralized data storage. Medical records are vulnerable to unauthorized access, insider threats, ransomware attacks, and data breaches. Existing systems often fail to provide transparent patient-controlled access management, reducing trust between patients and healthcare providers. Another major challenge is the lack of secure emergency access mechanisms. During critical medical situations, healthcare providers require immediate access to patient information, but existing systems struggle to balance emergency accessibility with accountability and privacy protection. Conventional healthcare systems also provide limited transparency regarding healthcare access activities, increasing the risk of unauthorized data modification and misuse. To address these issues, there is a need for a secure, transparent, and patient-centric healthcare management framework that supports consent-driven access control, encrypted medical record storage, immutable audit logging, and secure emergency access management. The proposed JeevanLocker framework addresses these limitations using blockchain technology, smart contracts, encrypted storage, and role-based authorization within a unified healthcare ecosystem.



**Fig2** - Challenges in traditional healthcare record management systems.



**Fig3** - Overall architecture of the proposed JeevanLocker system

#### 4. PROPOSED SYSTEM

The proposed JeevanLocker system is a blockchain-based unified medical record management framework designed to provide secure and patient-centric healthcare data sharing across multiple healthcare institutions. The system integrates blockchain technology, encrypted medical record storage, smart contracts, and role-based access control to establish a secure healthcare ecosystem.

The framework enables patients to maintain ownership and control over their medical records while allowing hospitals and doctors to access information only after receiving patient consent. Unlike traditional healthcare systems that rely on isolated databases, JeevanLocker provides a unified platform for secure healthcare data sharing.

The system follows a consent-driven access model where healthcare providers must request permission before accessing patient records. Once approved by the patient, the

access activity is recorded on the blockchain using smart contracts to ensure transparency and tamper-resistant audit logging.

Medical records are stored in encrypted cloud-based storage, while cryptographic hashes and access logs are maintained on the blockchain. This hybrid architecture improves scalability and reduces blockchain storage overhead while preserving data integrity and confidentiality.

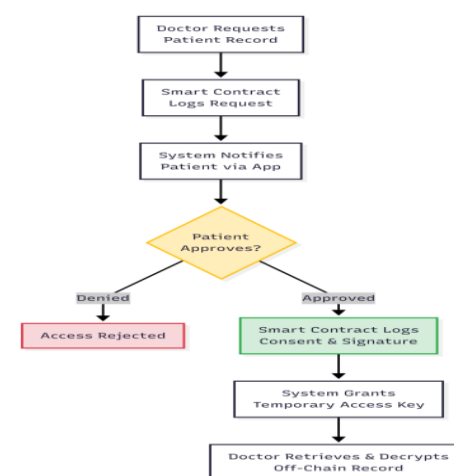
The proposed framework also implements Role-Based Access Control (RBAC) to restrict functionalities according to user roles such as patient, doctor, and administrator.

To support emergency situations, the system includes a Break-Glass emergency access mechanism that allows verified healthcare professionals to temporarily access patient records during critical medical conditions. All emergency access activities are logged on the blockchain and later notified to the patient.

The system architecture consists of four layers:

- Frontend Layer using React.js
- Backend Layer using Node.js and Express.js
- Database Layer using PostgreSQL and encrypted storage
- Blockchain Layer using Ethereum smart contracts

The proposed JeevanLocker framework aims to improve healthcare interoperability, strengthen medical data security, and establish transparent healthcare data management.



**Fig4** - Consent-based healthcare record access workflow

## 5. SYSTEM ARCHITECTURE

The JeevanLocker framework follows a layered architecture designed to provide secure, scalable, and transparent healthcare record management. The system integrates frontend services, backend processing, encrypted storage, and blockchain-based audit logging.

The architecture consists of four major layers:

### 1. User Interface Layer

The frontend is developed using React.js and provides separate interfaces for patients, doctors, hospitals, and administrators. Patients can upload records, approve access requests, and monitor healthcare activities, while doctors and hospitals can request and access authorized medical information.

### 2. Backend Layer

The backend is implemented using Node.js and Express.js. It manages authentication, authorization, consent verification, API communication, and blockchain interaction. JWT-based authentication and Role-Based Access Control (RBAC) are used to secure system operations.

### 3. Database and Storage Layer

PostgreSQL is used for storing metadata and healthcare information, while encrypted cloud storage is used for maintaining medical records securely. The system follows a hybrid storage model where medical files are stored off-chain and cryptographic hashes are stored on the blockchain.

### 4. Blockchain Layer

The blockchain layer uses Ethereum smart contracts written in Solidity to maintain immutable logs for consent approvals, healthcare access requests, and emergency activities. This ensures transparency, tamper resistance, and secure audit tracking.

The working process of the system includes patient registration, medical record upload, consent request handling, blockchain logging, and authorized healthcare access. In emergency situations, verified doctors can temporarily access patient records through the Break-Glass mechanism while maintaining complete auditability.

The proposed architecture improves healthcare interoperability, strengthens medical data security, and ensures patient-centric healthcare management.

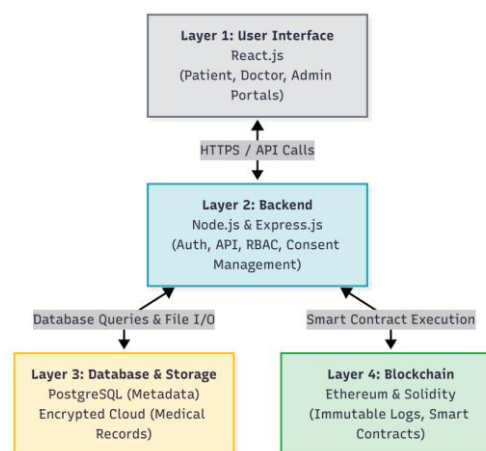


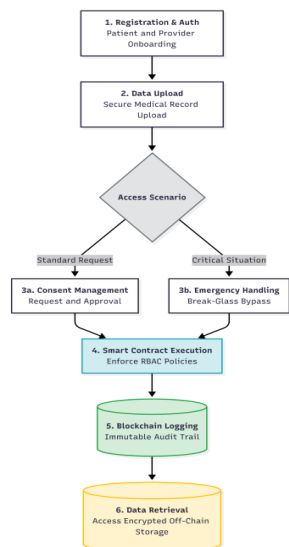
Fig5 - Layered architecture of the JeevanLocker system.

## 6. METHODOLOGY

The JeevanLocker framework is developed using a blockchain-integrated methodology designed to provide secure healthcare data management, consent-driven access control, and transparent audit logging. The system is developed using React.js for the frontend, Node.js and Express.js for backend services, PostgreSQL for database management, and Ethereum smart contracts for blockchain integration. The methodology includes the following steps:

- Patient registration and authentication.
- Secure medical record upload.
- Consent request and approval management.
- Blockchain-based audit logging.
- Encrypted healthcare data storage.
- Emergency Break-Glass access handling.

Medical records are stored in encrypted off-chain storage, while cryptographic hashes and access logs are maintained on the blockchain to ensure integrity and transparency. The system follows a consent-based workflow where hospitals and doctors must obtain patient approval before accessing healthcare records. Smart contracts record all consent approvals and access activities on the blockchain. Role-Based Access Control (RBAC) is implemented to restrict system functionalities according to user roles such as patient, doctor, and administrator. The proposed framework also includes a Break-Glass emergency mechanism that allows temporary healthcare access during critical situations while maintaining auditability and patient notification. Testing was performed to validate authentication security, consent enforcement, blockchain logging, and secure healthcare data access.



**Fig6 -** Methodology workflow of the JeevanLocker system.

## 9. CONCLUSION

The JeevanLocker framework presents a secure and patient-centric approach for healthcare record management using blockchain technology, encrypted storage, and consent-driven access control. The proposed system addresses major challenges in traditional healthcare systems, including fragmented medical records, unauthorized data access, lack of interoperability, and insufficient audit transparency. By integrating blockchain-based immutable logging with encrypted off-chain storage, the system improves healthcare data security, transparency, and confidentiality while reducing blockchain storage overhead. Smart contracts automate consent verification and healthcare authorization processes, ensuring secure patient-controlled access to medical records. The framework also introduces a Break-Glass emergency access mechanism that enables temporary healthcare access during critical situations while maintaining accountability through blockchain audit logging. The proposed system improves healthcare interoperability, strengthens patient privacy, and establishes transparent healthcare data management. Future enhancements may include advanced encryption techniques, AI-assisted healthcare analytics, and large-scale healthcare deployment. Overall, JeevanLocker provides a secure, scalable, and transparent healthcare management solution capable of supporting modern digital healthcare requirements.

## REFERENCES

1. Ravi Sekaran, "A Blockchain Based Framework for Securing Electronic Medical Records," International Journal of Applied Mathematics, Vol-38, Issue-35, 2025.
2. A. Ullah et al., "Toward Blockchain Based Electronic Health Record Management with Fine-Grained Attribute-Based Encryption and Decentralized Storage Mechanisms," Scientific Reports, 2025.
3. M. Shaikh et al., "A Systematic Literature Review for Blockchain-Based Healthcare Implementations," Journal of Medical Internet Research, 2025.
4. A. A. Ali et al., "Securing Electronic Health Records Using Blockchain-Enabled Federated Learning Framework," Results in Engineering, vol. 25, 2025.
5. R. Naga Priyadarsini et al., "Blockchain-Based Electronic Health Record System," IETE Journal of Research, 2025.
6. G. N. Brijwani et al., "Revolutionizing Healthcare Record Management: Secure Documentation Storage and Access through Advanced Blockchain Solutions," arXiv, 2025.