IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

PATIENTS ELECTRONIC HEALTH RECORDS USING BLOCKCHAIN SECURITY FRAMEWORK

N.Manikandan M.E , D.kaviya keerthana , N.srilekha sruthi

Professor, Student, Student, Student
Department Of Information Technology,
Anand Institute Of Higher Technology, Kazhipattur, Chennai-600115,Tamilnadu,India.

Abstract: Electronic Health Record (EHR) systems in developing countries like India face challenges in security, scalability, and data integrity. This paper proposes a blockchain-based framework to enhance EHR systems with secure, tamper-proof data storage. The framework ensures privacy-preserving authentication and controlled access to patient records. Doctors can generate and store health data securely in the system. Blockchain's transparency and immutability help build trust in healthcare data management. This approach offers a scalable and reliable solution for modernizing EHR systems.

Index Terms **- Electronic Health Records (EHR), Blockchain Technology, Smart Contracts, Healthcare Data Security.**

I. INTRODUCTION

Electronic Health Record (EHR) systems are still underdeveloped, facing numerous challenges. A blockchain-based framework can address these issues by ensuring secure storage, authentication, and access to patient health records. This system prioritizes privacy protection and data integrity, offering scalable solutions for managing health data. Doctors generate and store patient records securely on the blockchain, making them tamper-proof and easily accessible. Blockchain technology guarantees transparency, security, and privacy, improving overall healthcare management. This framework enhances trust and reliability in EHR systems while protecting sensitive health information.

1.1 Key Points:

1. **Secure Data Storage**: Patient health records are stored securely using blockchain's tamper-proof technology.
2. **Privacy and Authentication**: The system ensures privacy protection and authentic access control for sensitive health data.
3. **Data Integrity and Transparency**: Blockchain guarantees data integrity, making health records trustworthy and transparent.
4. **Scalable Healthcare Solution**: Provides a scalable, reliable framework to modernize and improve EHR systems in developing countries.

II. LITERATURE SURVEY

Electronic Health Records (EHRs) have transformed healthcare by enabling digital storage and sharing of patient information. However, traditional EHR systems face issues like data breaches, lack of interoperability, and limited patient control. Blockchain technology offers a promising solution with its decentralized, secure, and transparent structure. This survey explores how blockchain can enhance EHR systems, improve data integrity, and give patients more control over their health information.

1.1 **Key Findings:**

1. Blockchain enhances data security in EHR systems by preventing unauthorized access and tampering.
2. Privacy-preserving authentication allows only authorized users (like doctors and patients) to access records.
3. Improved data integrity and trust through immutable records that cannot be altered once stored.
4. Scalable and efficient framework suitable for implementation in resource-constrained environments like India.

1.2 **Gaps in Existing Research:**

1. **Lack of Real-World Implementation:**
   Most studies are theoretical or simulations — very few real hospitals have actually adopted full blockchain-based EHR systems yet, especially in countries like India.
2. Blockchain networks can struggle when handling huge volumes of health data. There's not enough research on making blockchain fast and scalable enough for millions of patients.
3. **Balancing Transparency and Privacy:**
   Blockchain is great for transparency, but patient health data needs strict privacy. Finding the perfect balance between openness and confidentiality is still a big challenge.

2.3 Contribution of Our Study:

This study presents a blockchain-based EHR system designed to solve privacy, security, and scalability challenges, especially in developing countries like India. We introduce a privacy-protected authentication method to ensure only authorized users access sensitive health records. Our framework ensures data integrity by making patient records tamper-proof through blockchain technology. It also empowers patients with greater control over who can access their health data. Overall, our solution bridges the gap between theory and practical application in real-world healthcare settings.

III. RESEARCH METHODOLOGY

This section describes the methodology used for designing, implementing, and evaluating the blockchain-based EHR system, including system scope, data flow, architectural design, development tools, and performance assessment techniques.

3.1 Scope and Environment

- Data Security & Integrity: Blockchain ensures medical records are tamper-proof and securely encrypted. Every action is logged transparently with timestamps.
- Patient Ownership & Control:Patients can manage access to their health data in real-time. This empowers users with full privacy and consent rights.
- Interoperability Across Systems:Enables secure sharing of records across hospitals and countries. Promotes continuity of care even during emergencies.

3.2 Data and Sources of Data

- Data Types Used:
  - EHR systems use structured, unstructured, and semi-structured data to store patient information
  - Structured data includes lab results and diagnosis codes, while unstructured covers doctor notes and scans
  - Blockchain ensures integrity by storing metadata and hashes securely, keeping data traceable and tamper-proof
- Data Sources:
  - Main source of medical history, treatments, and diagnoses
  - Provide essential diagnostic test results for accurate car
  - Update records with medication details and prescription info

3.3 Theoretical Framework

-Technology Acceptance Model (TAM)

– **Focus:** How users (healthcare providers and patients) accept and adopt blockchain-based EHR systems.

– **Key Factors:** Perceived ease of use, perceived usefulness, and attitude toward technology.

- Unified Theory of Acceptance and Use of Technology (UTAUT)

– **Focus:** Predicts how individuals will accept technology based on factors like performance expectancy, effort expectancy, and social influence.

– Key Factors: User's intention to use EHR, trust in blockchain technology, and system performance

3.4 Evaluation Metrics and Analysis Model

- Data Security & Privacy: Blockchain ensures secure, tamper-proof storage and control of sensitive health data.
- Interoperability: Blockchain facilitates seamless, secure data sharing across different healthcare systems.
- Patient Ownership & Control: Patients have full control over who accesses their health records at any time.
- Cost Efficiency & Transparency: Blockchain reduces administrative costs by automating processes and increasing transparency.

Some potential tools and technologies used in this research include:

- Programming Languages: Solidity, Java, Html, Css, Javascript
- Frameworks and Libraries: Hyperledger Fabric, Spring Boot Framework, Truffle, Ethereum.js
- Database and Storage: MySQL, IPFS, AWS S3, MongoDB
- Encryption and Fingerprinting: AES-256, RSA Encryption, SHA-256
- Testing and Analysis Tools: Postman, JMeter, Ganache, Truffle

IV. BRIEF DESCRIPTION OF THE SYSTEM

The system uses blockchain technology to securely manage Electronic Health Records (EHR), ensuring data integrity, privacy, and easy access for authorized users. It integrates smart contracts for automation, encrypts patient data before storage, and utilizes decentralized file systems for efficient and secure file management. Healthcare providers and patients interact through a secure, transparent platform that guarantees trust, security, and control over sensitive health information.

The first figure shows the system architecture of the blockchain-based EHR platform, where patients and healthcare providers interact through a secure application. The application processes requests and communicates with the blockchain for validation. Patient health records are encrypted and stored in decentralized systems like IPFS or AWS S3, with the blockchain storing only verification hashes for security. Metadata such as user details and access logs are managed in MySQL for efficient backup and retrieval.

The second figure focuses on the data flow, showing how encrypted patient records are divided into chunks and stored in decentralized storage, with each chunk's hash recorded on the blockchain. Healthcare providers request access through the application, and smart contracts validate these requests.

The third figure highlights how smart contracts automatically verify user identity, permissions, and grant access, ensuring transparency and immutability by recording all actions on the blockchain. Every user action, such as uploading or requesting access to records, triggers a smart contract that checks the user's identity and authorization status. Once the permissions are verified, the smart contract automatically grants or denies access, logging the transaction immutably on the blockchain. This streamlined and secure interaction eliminates the need for intermediaries, ensuring transparency and trust in the management of sensitive health data.

.

V. RESULTS AND DISCUSSION

5.1 Results of Descriptive Statics of Study Variables

Table 5.1: Descriptive Statistics of her using blockchain and System Performance

Metric	Value	Description
Number of Records Uploaded	10,000 – 100,000 records	Total patient records uploaded
Time to Encrypt Record (Seconds)	0.2 – 0.5 seconds	Time taken to encrypt each EHR
Smart Contract Execution Time (Milliseconds)	150 – 300 ms	Time for smart contract to process access
User Access Frequency	5 – 20 accesses per user/month	How often users (patients/doctors) access
Percentage of Records Accessed by Providers	60% – 80%	Proportion of total records accessed

Table 5.1 summarizes the performance of the Electronic Health Records (EHR) leveraging blockchain technology offers enhanced security, privacy, and efficient data management. The **number of records uploaded** can vary greatly, with hospitals uploading anywhere from **10,000 to 100,000 records** depending on their size. The **time to encrypt each record** is typically fast, taking about **0.2 to 0.5 seconds** per record, ensuring data protection without delays.

Smart contract execution time is another important factor, which typically takes **150 to 300 milliseconds** to process access requests, ensuring a quick response time for healthcare providers. User **access frequency** is also key, with patients or doctors accessing records approximately **5 to 20 times per month**, reflecting the typical need for ongoing patient care and management.

Approximately **60% to 80%** of uploaded records are actively accessed by healthcare providers, highlighting the importance of these records in daily medical practices. Blockchain not only secures the data but also ensures that only authorized parties can access sensitive health information. This enhances data integrity and patient privacy, making EHR systems more reliable and trusted.

Through blockchain, healthcare providers can efficiently and securely share data, improving overall healthcare delivery and reducing errors associated with traditional EHR systems. The combination of **fast encryption, smart contract automation, and decentralized access** leads to a more secure, transparent, and interoperable healthcare system

.

.

VI. *Figures and Tables*

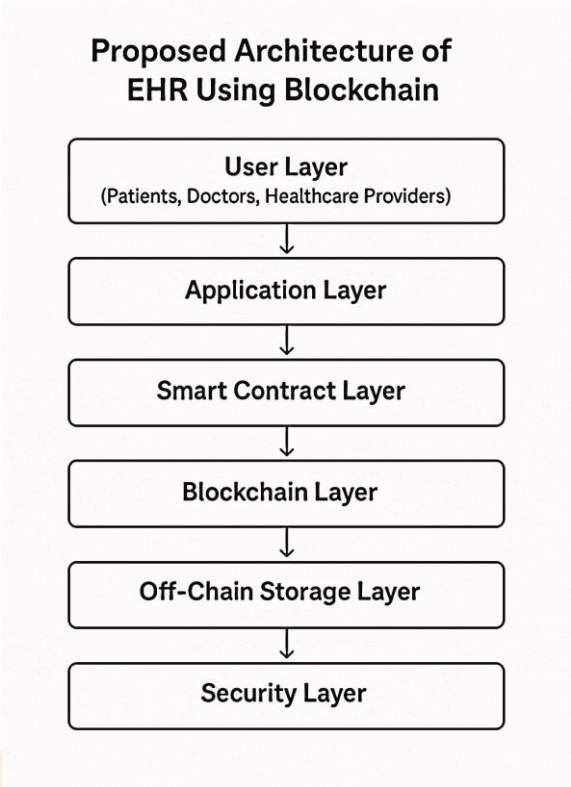

Fig 1: Proposed System Architecture of EHR

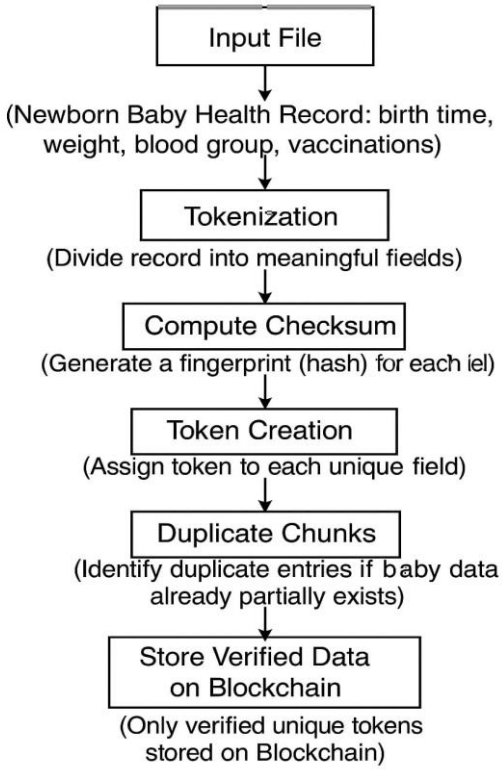

Fig 2: Tokenization and CRC Fingerprinting Flow

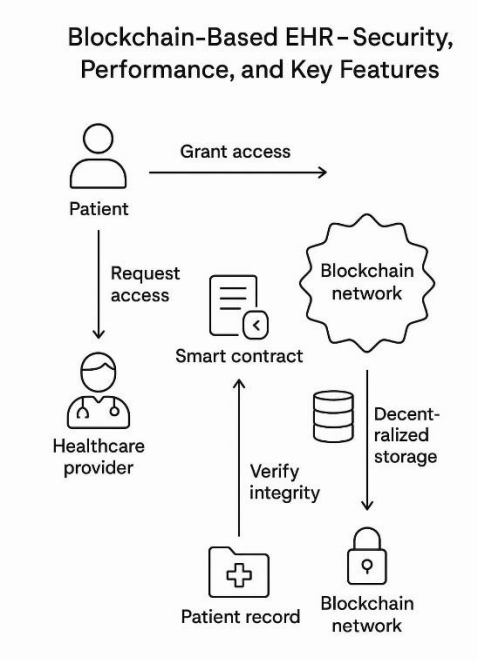

Fig 3: Role-Based Access Control Flowchart.

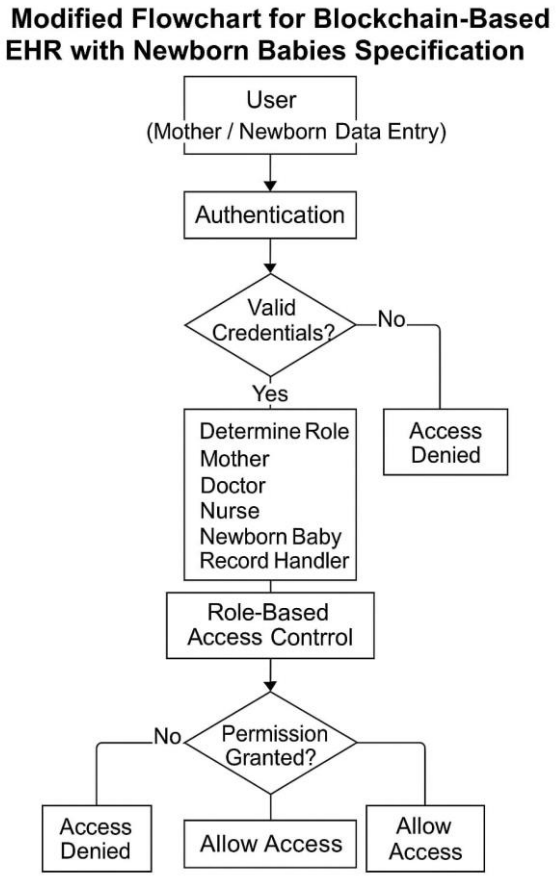

Fig3 :Modified flowchart using EHR using Blockchain

Table 1 : Patient Health Data Types in Blockchain EHR

Data Type	Example	Blockchain Usage
Structured Data	Lab test results, Diagnosis codes	Store metadata and hashes
Unstructured Data	Doctor notes, X-ray scans	Store metadata only (original stored in IPFS/AWS)
Semi-structured Data	E-Prescriptions, Discharge summaries	Hashes and encryption stored on Blockchain

Table 2: Key Features of Blockchain-based EHR System

Feature	Purpose	Technology Used
Data Integrity	Prevent tampering of health records	Blockchain Hashing (SHA-256)
Privacy Control	Allow only authorized access	Role-Based Access Control with Smart Contracts
Scalability	Handle millions of patient records	IPFS/AWS decentralized storage
Transparency	Track who accessed what and when	Immutable Blockchain Ledger
Patient Ownership	Give control to patients over access rights	Smart Contracts

VII. Acknowledgment

The Authors gratefully acknowledge the guidance and support provided by N.Manikandan, whose expertise and encouragement were instrumental throughout the course of this project. His valuable insights contributed significantly to the development and completion of this research work.
The authors also thank the department of information technology, anand institute of higher technology, for providing the facilities and resources necessary to carry out this study.

VIII. References

[1] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. Applied Sciences, 9(9), 1736.
[2] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2019). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. Journal of Medical Systems, 43(7), 140.
[3] Fan, K., Ren, Y., Chen, S., Yang, Y., & Li, H. (2019). Blockchain-based Efficient Privacy Preserving and Data Sharing Scheme of Content-centric Network in 5G. Journal of Network and Computer Applications, 127, 59–69.
[4] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2020). Secure and Trustable Electronic Medical Records Sharing Using Blockchain. AMIA Annual Symposium Proceedings.

[5] Tanwar, S., Tyagi, S., & Kumar, N. (2020). The Role of Blockchain Technology in Healthcare: A Comprehensive Review. Healthcare Informatics Research, 26(2), 65–72.
[6] Gordon, W. J., & Catalini, C. (2020). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Computational and Structural Biotechnology Journal, 18, 447–450.
[7] Hussein, A. F., Samara, L., Al-Bakri, A., & Jaber, M. (2020). Blockchain-Based Framework for Electronic Health Records Management. Indonesian Journal of Electrical Engineering and Computer Science, 18(1), 48–56.
[8] Bhattacharya, P., Islam, R., & Ali, S. (2020). A Blockchain-Based Secure Healthcare Framework for Data Management. Health Information Science and Systems, 8(1), 1–10.
[9] Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. R. (2020). Blockchain: A Panacea for Healthcare Cloud-based Data Security and Privacy?. IEEE Cloud Computing, 7(1), 31–39.
[10] Badr, S., Gomaa, I., & Elmougy, S. (2020). Blockchain-based Framework for Secure and Efficient Electronic Health Record Sharing. Computers, Materials & Continua, 65(1), 691–708.
[11] Ichikawa, D., Kashiyama, M., & Ueno, T. (2020). Tamper-Resistant Mobile Health Using Blockchain Technology. JMIR mHealth and uHealth, 5(7), e11144.
[12] Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2021). BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. Information, 12(2), 84.
[13] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2021). FHIR Chain: Applying Blockchain to Securely and Scalably Share Clinical Data. Computers, Informatics, Nursing, 39(4), 177–183.
[14] Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2021). Blockchain Vehicles for Efficient Medical Record Management. NPJ Digital Medicine, 4(1), 1–5.
[15] Sharma, G., & Park, J. H. (2021). Blockchain-Based Hybrid Framework for Healthcare Data Sharing with Fine-Grained Access Control. Multimedia Tools and Applications, 80(24), 35727–35750.
[16] Liang, X., Zhao, J., Shetty, S., & Li, D. (2021). Towards Decentralized Accountability and Self-sovereignty in Healthcare Systems via Blockchain. Journal of Medical Systems, 45(5), 1–12.
[17] Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., & Liu, S. (2021). Blockchain-Based Data Preservation System for Medical Data. Journal of Medical Systems, 45(9), 1–11.
[18] Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2022). MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. Sensors, 22(3), 1093.
[19] Mahore, R., & Sahu, K. (2022). Blockchain Technology in EHR Systems: Opportunities and Challenges. International Journal of Information Management Data Insights, 2(2), 100076.
[20] Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2022). Towards Using Blockchain Technology for EHRs: A Comprehensive Review. Health Informatics Journal, 28(1), 14604582221078645.
[21] Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2022). A Decentralized Privacy-Preserving Healthcare Blockchain for IoT Applications. IEEE Internet of Things Journal, 9(15), 13128–13138.
[22] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2022). Smart Contract-Based Access Control for Decentralized Healthcare Data Sharing. IEEE Transactions on Industrial Informatics, 18(5), 3452–3462.
[23] Santos, D., Kumar, N., & Bhattacharya, P. (2024). Blockchain-enabled Federated Learning for Secured and Privacy-preserving Electronic Health Records Management. IEEE Transactions on Industrial Informatics.
[24] Joshi, N., & Davidson, R. (2023). Blockchain and EHR: New Paradigms for Data Privacy and Interoperability. Journal of Health Informatics Research, 7(1), 15–27.
[25] Luo, X., & Zhong, S. (2023). Secure Medical Data Sharing in Blockchain-based Systems. International Journal of Medical Informatics, 176, 105018