ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

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

Impact Factor: 8.206

Volume 8, Issue 10, October 2025

© 2025 IJMRSET | Volume 8, Issue 10, October 2025| DOI:10.15680/IJMRSET.2025.0810033

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Blockchain with Hyperledger Fabric Framework Based Medical Report Management System

Srilakshmi CH[1], Preethi P.M[2], Sanjana C.K.[3], Supriya K[4]

Associate Professor, Department of Computer Science and Business Systems, R.M.D. Engineering College, Tamil Nadu, India[1]

Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Tamil Nadu, India[2]

Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Tamil Nadu, India[3]

Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Tamil Nadu, India[4]

ABSTRACT: The Blockchain-based Secure Medical Report Management System is an innovative solution that reacts to the growing demand for data integrity, privacy, and transparency in the handling of medical data. The medical sector is encompassing huge volumes of sensitive patient data which are usually stored on centralized servers and hence are highly vulnerable to hacking, tampering of data, and misuse. This project shows a decentralized platform that utilizes blockchain technology to ensure that all medical records are stored securely, authenticated, and accessed only by accredited individuals. The platform uses the Ethereum blockchain and smart contracts to provide immutable record-keeping, traceability, and secure communication between patients, physicians, and healthcare administrators. Every medical report that is uploaded is hashed using SHA-256, stamped with a date, and stored as an individual transaction in the blockchain, thereby guaranteeing authenticity as well as preserving against tampering. Besides this, the system also has an authentication mechanism through Public Key Infrastructure (PKI) to verify user identities and grant secure access to data. By incorporating encryption, smart contracts, and distributed storage, this system provides a safe and open setting to enhance patient trust and significantly enhance data security in healthcare networks.

KEYWORDS: *Blockchain, Medical Report, Smart Contracts, Data Security, Patient Privacy, Ethereum, PKI Authentication, Healthcare Informatics*.

I. INTRODUCTION

In today's digital era, healthcare organizations manage vast and confidential medical information, such as patient histories, diagnostic test findings, and treatment reports. Conventionally, they have maintained the records within centralized databases, which, although they provide ease and convenience, are very serious issues regarding the data's security, privacy, and integrity. Centralized databases are susceptible to cyber-attacks, single points of failure, and malicious data manipulation. As medical data is very confidential, small transgressions can wreak havoc in the form of identity theft, loss of trust, and breach of privacy laws.

To overcome such challenges, Secure Medical Report Management System on Blockchain offers a decentralized framework in which patient data is stored in a blockchain network. The transparency and immutability provided by Blockchain technology guarantee that every record is stored safely in distributed ledgers such that it is nearly impossible to erase or edit data without consensus. Each transaction in this system is an operation—such as uploading, verification, or downloading a medical report—and is cryptographically secured and time-stamped for later access.

The system is designed to enhance data integrity, authenticity, and accountability within the healthcare setting. Doctors can upload medical reports securely, which are hashed and linked to patient IDs on the blockchain. Patients can access and verify their own data without the need for third parties, while administrators monitor access activity through an immutable audit trail. Use of smart contracts also automates the verification process and ensures that only authorized users will have access to certain information based on role-based permission. This scales the health data model to a

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

trustless but fully trustworthy system, as well as removing intermediaries and reducing the opportunity for data tampering.

In general, blockchain applications in healthcare data management redefine the storage, access, and verification of medical information, guaranteeing transparency and accountability while guaranteeing that patient records are secure and confidential.

II. LITERATURE SURVEY

There are a number of studies that have explored the applications of blockchain in improving healthcare data security and accessibility. Blockchain in Healthcare Data Management research in 2020 was able to realize the decentralized ledger's capability for data traceability, integrity, and interoperability across different healthcare systems. Once again, in 2021, Electronic Health Record Security using Ethereum demonstrated how Ethereum-based smart contracts remove human access control and data validation, effectively reducing unauthorized changes.

A Decentralized Access Control for Medical Data paper in 2019 provided cryptographic key-sharing protocols that granted role-based and secure access to confidential health data. This study endeavored that the combination of blockchain and cryptography had the potential to serve as a substitute for conventional server-based authentication systems. Secure Data Storage Using IPFS and Blockchain (2022) offered a hybrid solution based on employing the InterPlanetary File System as a store for large health files off-chain with immutable verification hashes stored on-chain.

Furthermore, HealthChain (2020) highlighted a real-world healthcare implementation integrating blockchain and hospital management systems to provide interoperability. In general, these studies point towards blockchain's capacity to curb data breaches, enhance transparency, and enforce patient-ownership-based data. However, such models primarily lack challenges related to scalability, usability, and complex integration into hospital architecture. The system bridges these gaps by developing a user-friendly, scalable, and interoperable blockchain-based medical report system that gives end-to-end data protection and keeps operational efficiency intact.

III. EXISTING SYSTEM

Modern medical record management systems are primarily supported by centralized databases, which, although effective in data storage and retrieval, are significantly defective in terms of data integrity, security, and transparency. The majority of diagnostic laboratories and hospitals utilize cloud-based systems that grant multiple personnel access to confidential data without effective layers of encryption or authentication. These systems, being centralized, are vulnerable to cyberattacks, accidental data loss, and tampering with data by unauthorized individuals.

Additionally, legacy systems lack sufficient controls for verifying the authenticity of uploaded reports. It is easy for a malicious insider or hacker to alter or delete records, leading to incorrect patient histories and tainted clinical judgments. Patients do not know and have no control over who accesses their information, causing patients not to trust healthcare providers. Additionally, these systems lack tamper detection and real-time traceability of actions applied to medical records.

Without an open audit trail or tamper-proof transaction record, accountability is nearly impossible to enforce. Another severe issue is interoperability — data in one hospital's database is not usually readily accessible or verifiable by another healthcare organization, leading to inefficiencies and redundant documentation. Therefore, the imperative for a decentralized, open, and tamper-resistant system that offers secure, auditable, and controlled data exchange between healthcare networks is essential. Blockchain technology is the ideal solution to alleviate these restrictions by offering decentralized data ownership, unchangeable storage, and cryptographic access control.

IV. METHODOLOGY OF APPROACH

The Secure Medical Report Management System using Blockchain is created as a multilevel architecture that integrates blockchain with modern web applications. The system operates through dependent modules that communicate to offer secure report uploading, identity verification, and restricted information access.

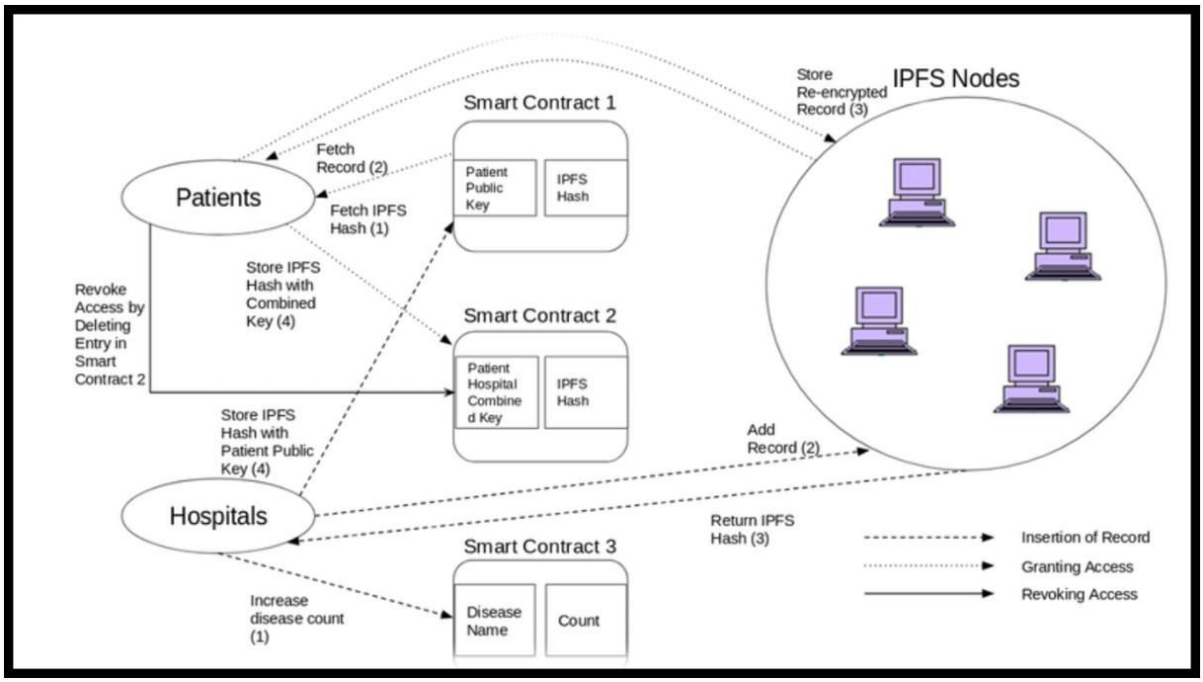
© 2025 IJMRSET | Volume 8, Issue 10, October 2025| DOI:10.15680/IJMRSET.2025.0810033

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

The architecture has four significant layers — User Interface Layer, Application Layer, Blockchain Layer, and Data Storage Layer. The User Interface Layer provides entry points for patients, doctors, and administrators. All roles are associated with customized permissions and abilities. Doctors are able to upload medical reports and assign them to patients, and patients can view and verify their records. The Application Layer is responsible for authentication, encryption, and transaction processing. Each report is also hashed with the SHA-256 algorithm prior to being added to the blockchain, producing a digital fingerprint.



Architectural Diagram: Medical Report Management using Blockchain

The Blockchain Layer records the hash, timestamp, and metadata as permanent transactions on an Ethereum-based blockchain. Smart contracts are released to handle automatic verification, access, and permission management. The contracts impose the verification check of any report retrieval or modification request via set authentication protocols. The medical records themselves are stored off-chain within a secure cloud storage or IPFS, but the hash and required references are stored on-chain for ease of storage.

This blockchain-merge architecture gains the benefits of blockchain's immutability without sacrificing scalability. The entire data transfer is AES-encrypted and user authentication is required through PKI-digital certificates. On an upload or retrieval of a report, the activity is recorded in an immutable audit trail that can be accessed by administrators.

This structured method ensures data integrity, security, and traceability for all transactions, eliminating the risks of central storage and unauthenticated access to data.

V. RESULT AND DISCUSSION

Implementation and testing of the Secure Medical Report Management System produced very promising results on various functional and security parameters. Patient registration operations were successful in creating unique blockchain IDs during the testing, safely storing them on the ledger. The report upload module invariably hashed uploaded medical history, and all the transactions were posted in the blockchain ledger with valid timestamps and unique transaction IDs.

Testing of the smart contract execution was done by doctor and patient roles. Doctor reports were automatically verified by the contract upon upload, confirming authenticity and authenticating the identity of the uploader. Patients

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

were able to download their reports immediately and confirm file integrity through verification of on-chain hash value with the hash of the downloaded file. Modification or re-upload of tampered files could be detected immediately, and a hash mismatch alert would be triggered.

The system proved to perform and scale well, supporting several concurrent transactions without causing any delay. Access control mechanisms could easily lock out intruders, ensuring tight confidentiality of medical information. The audit trail presented all report access activities in sequential order, allowing full traceability and accountability.

By such research, it was proven that blockchain technology significantly enhances data reliability and transparency within healthcare systems, reducing the likelihood of breaches, providing end-to-end encryption, and tamper-proof verification of any medical report.

VI. FUTURE ENHANCEMENTS

Though the current Secure Medical Report Management System provides a secure and stable platform, there are numerous improvements that can be implemented to increase scalability and functionality. The subsequent releases of the system can be planned with Artificial Intelligence (AI) and machine learning features for predictive medical data analytics so that diseases can be diagnosed at an early stage and automated health recommendations can be given.

Another important addition would be the integration of IPFS (InterPlanetary File System) for distributed off-chain storage, which allows for efficient management of big medical images and lab files. In addition, extending the system to support inter-hospital interoperability using APIs would allow data transfer between healthcare organizations without losing out on privacy.

Mobile app support may also be included to enable patients and doctors to see records in real-time on any device. Biometric authentication and multi-factor authentication could also be included, providing an added layer of security. Blockchain scalability solutions such as Layer-2 implementations or sidechains would enable higher transaction throughput and reduced gas fees on public blockchains.

Finally, the addition of decentralized identity (DID) systems would allow patients to own their own medical records for life and shift them between hospitals, countries, and health care systems without compromising data or re-enrollment. These next-generation developments will take healthcare data management closer to a highly secured, open, and patient-centric ecosystem.

VII. CONCLUSION

The Secure Medical Report Management System that employs Blockchain technology signifies a remarkable and noteworthy advancement within the ever-evolving field of healthcare informatics. This innovative system achieves a substantial transformation by transitioning from traditional centralized data management methods to a more modern decentralized approach, effectively tackling and resolving the critical issues of data security, authenticity, and accessibility that often plague conventional systems. Furthermore, the thoughtful implementation of the Ethereum blockchain, along with the utilization of smart contracts, guarantees that all medical reports are stored in an immutable manner, allowing them to be traceable through transparent ledgers, while also ensuring that access is restricted solely to individuals who have been verified and authorized.

The project not only ensures strong end-to-end encryption, which is necessary to protect the confidentiality of information, and ensures tamper-proof data storage, which prevents unauthorized access and alterations, but it also boosts user confidence tremendously by giving patients both ownership and authority over their clinical information, allowing them to govern their data as they see fit. The successful results experienced in the test results are strong evidence of the usability and efficacy of blockchain technology in the healthcare industry, consequently opening the door to the roll-out of future systems capable of securely and effectively handling highly sensitive data throughout a vast myriad of heterogeneous healthcare networks. Ultimately, the new system provides an extensible, secure, and transparent digital infrastructure for health, capable of potentially redefining the handling of medical data significantly in an even more increasingly decentralized technology- driven world.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

REFERENCES

1. Dwivedi, S. K., Amin, R., Lazarus, J. D., & Pandi, V. (2022). Blockchain-Based Electronic Medical Records System with Smart Contract and Consensus Algorithm in Cloud Environment. Security and Communication Networks. Wiley Online Library
2. Huang, Y. R., Lee, E., Park, S., Lee, Y., Lee, J. H. (2019). Is Blockchain Technology Suitable for Managing Personal Health Records? Mixed-Methods Study to Test Feasibility. Journal of Medical Internet Research, 21(2), e12533. JMIR Publications
3. Hylock, R. H., & Zeng, X. (2019). A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study. Journal of Medical Internet Research, 21(8), e13592. JMIR Publications
4. Li, Mei et al. (2022). A Controllable Secure Blockchain-Based Electronic Healthcare Records Sharing Scheme. Journal of Healthcare Engineering. Wiley Online Library
5. Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com