IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, June 2026
Impact Factor: 8.2

Securing Healthcare Privacy Using Blockchain Technology

Dr. R. G. Raut[1], Gaurav Kajabe[2], Prem Kusmude[3], Gaurav Nawale[4], Rohan Raysing[5]
[1]Prof. and [2,3,4,5]Students of Department of Information Technology,
Dr VitthalraoVikhe Patil College of Engineering, Ahilyanagar, Maharashtra
Savitribai Phule Pune University, Pune

Abstract: *With the growing integration of digital technologies in healthcare, medical services have become faster and more accessible. Yet, this progress has also increased the exposure of confidential patient records to cyber threats and data misuse. This project introduces a blockchain-driven framework designed to secure, streamline, and decentralise the management of healthcare data. The proposed system safeguards electronic health records through a distributed architecture, cryptographic encryption, and automated smart contracts, enabling authorized communication among patients, hospitals, and insurance providers while maintaining data accuracy and confidentiality. Each healthcare transaction is permanently registered on the blockchain ledger, ensuring traceability, immutability, and prevention of unauthorized alterations. By removing intermediaries, the system accelerates claim validation, enhances transparency, and ensures compliance with essential healthcare privacy frameworks such as HIPAA and GDPR. Unlike traditional centralized databases, the proposed model significantly reduces the chances of data fraud, improves coordination among different healthcare platforms, and fosters greater reliability and confidence within the digital medical ecosystem. Ultimately, the project highlights how blockchain technology can redefine healthcare privacy management, building a secure, efficient, and reliable digital health infrastructure.*

Keywords: Blockchain Technology, Healthcare Data Security, Electronic Health Records, Smart Contracts, Decentralized Systems, Data Privacy, Telemedicine, HIPAA Compliance, GDPR Compliance, Digital Healthcare, etc.

I. INTRODUCTION

Healthcare systems across the world are rapidly adopting digital technologies to improve the efficiency, accessibility, and quality of medical services. The widespread use of electronic health records, cloud-based platforms, and telemedicine has enabled faster diagnosis, remote consultation, and seamless data sharing among healthcare providers. However, this digital transformation has also introduced serious challenges related to data privacy, security, and trust. Sensitive patient information is increasingly exposed to cyberattacks, unauthorized access, data tampering, and misuse, especially in centralized healthcare systems.

Traditional healthcare data management systems rely heavily on centralized databases and trusted third parties to store and control patient records. Such architectures create single points of failure and limit transparency, making them vulnerable to insider threats and large-scale data breaches. Moreover, managing access permissions among multiple stakeholders such as hospitals, doctors, laboratories, and insurance providers becomes complex and inefficient. Recent research in blockchain technology, cryptography, and distributed systems has shown that decentralized solutions can significantly enhance data integrity, transparency, and trust in sensitive data environments.

Blockchain technology has emerged as a promising solution for secure and tamper-resistant data management due to its decentralized ledger, immutability, and traceability features. When combined with cryptographic encryption and smart contracts, blockchain can automate access control and verification processes while eliminating the need for intermediaries. These capabilities make blockchain particularly suitable for healthcare systems where data accuracy, confidentiality, and accountability are critical.

DOI: 10.48175/IJARSCT-36416

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, June 2026
Impact Factor: 8.2

The primary objective of this project is to develop a blockchain-based healthcare data management framework that ensures secure storage, controlled access, and transparent sharing of electronic health records. The proposed system leverages distributed architecture, cryptographic encryption, and automated smart contracts to enable authorized communication among patients, healthcare providers, and insurance entities. By integrating blockchain technology into healthcare workflows, the project aims to reduce data fraud, enhance coordination across platforms, and establish a secure, reliable, and privacy-preserving digital healthcare ecosystem.

II. PROBLEM STATEMENT

The rapid digitization of healthcare systems has led to widespread use of electronic health records and cloud-based medical platforms. However, most existing healthcare data management systems rely on centralized architectures, making them vulnerable to data breaches, unauthorized access, record manipulation, and lack of transparency. Sensitive patient information is often stored and managed by third-party intermediaries, increasing the risk of data misuse and single points of failure. Additionally, inefficient access control mechanisms make it difficult to securely share medical data among hospitals, doctors, and insurance providers while maintaining privacy and regulatory compliance. Therefore, there is a critical need for a secure, decentralized, and transparent healthcare data management system that ensures data integrity, controlled access, and trust across all healthcare stakeholders.

III. MATERIALS AND METHODS

The goal of this project is to design and implement a blockchain-based healthcare data management system that ensures secure, transparent, and privacy-preserving handling of medical records. The system is developed as a software-based framework that integrates blockchain technology, cryptographic encryption, and smart contracts to manage healthcare data in a decentralized manner. The materials utilized and the methods employed focus on safeguarding electronic health records, enabling controlled data access, and maintaining data integrity across healthcare stakeholders. The proposed approach supports secure data sharing among patients, hospitals, and insurance providers while eliminating dependency on centralized authorities. This methodology ensures transparency, traceability, and resistance to unauthorized data modification in digital healthcare environments.

•Materials Used

The system is developed using Java for backend processing and Java web technologies such as JSP and Servlets for implementing the web-based healthcare application. Blockchain technology is used to create a decentralized and immutable ledger for recording healthcare transactions. Cryptographic techniques, including hashing and encryption algorithms, are employed to secure electronic health records and generate unique identifiers for data integrity verification. Smart contracts are used to automate access control, authorization, and transaction validation. A cloud storage environment is utilized for storing encrypted medical records, while blockchain nodes maintain transaction metadata and access logs. Standard computing systems with internet connectivity are used for system deployment and testing.

•Methods Followed

Initially, patients, hospitals, and authorized healthcare entities are registered into the system through secure authentication mechanisms. Patient medical records are encrypted and uploaded to cloud storage, and corresponding hash values are generated for each record. These hash values, along with transaction details, are stored on the blockchain as immutable blocks to ensure data integrity and traceability.

When healthcare providers or insurance entities request access to medical records, smart contracts automatically verify predefined access policies and authorization conditions. Upon successful validation, controlled access to the encrypted data is granted without exposing sensitive information on the blockchain. Each data access and modification request is permanently logged, ensuring transparency and preventing unauthorized alterations. Continuous testing and validation are performed to enhance system reliability, security, and performance, ensuring a secure and efficient healthcare data management framework.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, June 2026
Impact Factor: 8.2

IV.RESULTS

The implemented blockchain-based healthcare system enables secure and reliable management of electronic health records through a decentralized architecture. The use of cryptographic encryption ensures that patient data remains confidential, while blockchain technology successfully records each healthcare transaction as an immutable and traceable entry. The system effectively prevents unauthorized modification of medical records and ensures data integrity across all participating entities.

Authorized hospitals, doctors, and insurance providers are able to securely access patient records through smart contract–based validation. Access requests are processed efficiently, and only users satisfying predefined authorization conditions are granted controlled access to encrypted data. Test observations indicate that the decentralized approach improves transparency and trust while reducing dependency on centralized intermediaries. The permanent logging of transactions enhances auditability and accountability, allowing healthcare stakeholders to verify data authenticity and history. Overall, the system demonstrates dependable performance in securing healthcare data, supporting transparent data sharing, and improving coordination within digital healthcare environments.

Key Results

Secure storage of electronic health records using blockchain-based immutable ledger.
Accurate enforcement of access control through smart contracts and authorization policies.
Tamper-proof recording of healthcare transactions ensuring data integrity and traceability.
Improved transparency, trust, and secure data sharing among patients, hospitals, and insurance providers.

V. DISCUSSION

The proposed system architecture effectively demonstrates how blockchain technology can be utilized to secure and manage healthcare data in a decentralized environment. The interaction between patients, hospitals, multi-authority entities, smart contracts, and the peer-to-peer blockchain network ensures that sensitive medical information is processed, stored, and accessed in a secure and transparent manner. By integrating smart contracts with a distributed ledger, the system successfully enforces access control policies and automates transaction validation without relying on a centralized authority.

The architecture highlights the role of cryptographic hash generation and mining in maintaining data integrity and immutability. Each healthcare transaction, including patient data submission and hospital report uploads, is validated and committed to the blockchain, preventing unauthorized modification or data tampering. The validation and recovery mechanisms further enhance system reliability by ensuring blockchain consistency even in the presence of node failures or malicious attempts.

The inclusion of multi-authority access control strengthens privacy protection by distributing trust among multiple entities rather than a single controlling authority. Hospitals can securely upload and retrieve historical patient records, while authorized users can generate reports and access verified data through controlled requests. The peer-to-peer blockchain network ensures transparency, traceability, and consensus among participating nodes, improving trust across healthcare stakeholders.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, June 2026
Impact Factor: 8.2

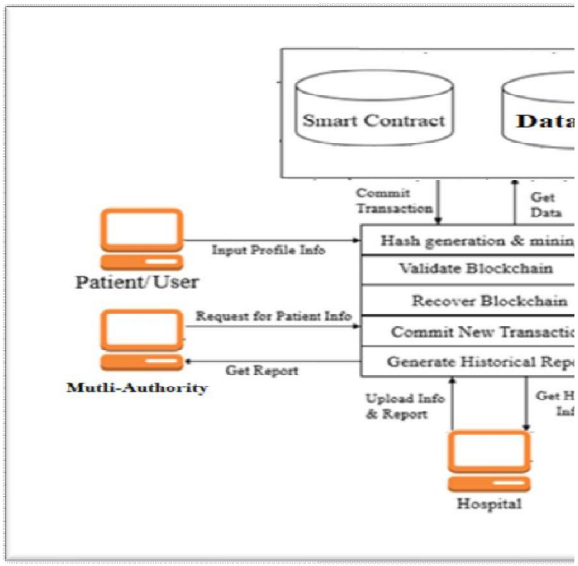

Fig.1: System Architecture Design

Overall, the system architecture demonstrates a scalable, secure, and future-ready healthcare data management solution. The clear separation of modules and well-defined data flow enable ease of maintenance, extensibility, and real-world deployment. The design effectively addresses major challenges such as data privacy, unauthorized access, and lack of transparency in traditional healthcare systems, validating the practical applicability of blockchain technology in digital healthcare environments.

VI. CONCLUSION

The findings of this project demonstrate that blockchain technology can significantly enhance the security, privacy, and transparency of healthcare data management systems. The effective integration of decentralized ledger technology, cryptographic encryption, and smart contracts ensures that electronic health records are stored and shared in a secure and tamper-proof manner. This approach reduces reliance on centralized authorities while maintaining data integrity and controlled access among healthcare stakeholders.

The results further indicate that decentralized access control and immutable transaction logging provide a reliable solution to critical challenges such as unauthorized data modification, data breaches, and lack of trust in traditional healthcare systems. By enabling secure data sharing among patients, hospitals, and insurance providers, the proposed system improves coordination and accountability within digital healthcare environments. Overall, the study highlights the potential of blockchain-based architectures to build secure, efficient, and trustworthy healthcare infrastructures that support modern telemedicine and future digital health applications.

ACKNOWLEGEMENT

We sincerely acknowledge the researchers and publishers whose valuable contributions and resources supported this work. We extend our heartfelt appreciation to our project guide for their continuous guidance, support, and motivation. We also thank the college management for providing the essential facilities and institutional support throughout the completion of this project.

REFERENCES

1. G. Verma, “Blockchain-based privacy preservation framework for healthcare data in cloud environment,” Journal of Experimental & Theoretical Artificial Intelligence, vol. 36, no. 1, pp. 147–160, 2024..
2. K. Azbeg, O. Ouchetto, and S. J. Andaloussi, “Access control and privacy-preserving blockchain-based system for diseases management,” IEEE Transactions on Computational Social Systems, vol. 10, no. 4, pp.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, June 2026
Impact Factor: 8.2

1515–1527, 2022.

3. M. Qi et al., "Privacy protection for blockchain-based healthcare IoT systems: A survey," IEEE/CAA Journal of Automatica Sinica, 2022.
4. Healthcare Engineering Journal, "SmartMedChain: A blockchain-based privacy-preserving smart healthcare framework," Article ID 9791481, 2023.
5. A.G. de Moraes Rossetto, C. Sega, and V. R. Q. Leithardt, "An architecture for managing data privacy in healthcare with blockchain," Sensors, vol. 22, no. 21, Art. no. 8292, 2022
6. R. Zhang, R. Xue, and L. Liu, "Security and privacy for healthcare blockchains," IEEE Transactions on Services Computing, vol. 15, no. 6, pp. 3668–3686, 2021.
7. M. K. Hasan et al., "Blockchain technology on smart grid, energy trading, and big data: Security issues, challenges, and recommendations," Wireless Communications and Mobile Computing, vol. 2022, Article ID 9065768, 2022.
8. A. Abdelzahir et al., "Blockchain for IoT applications: Taxonomy, platforms, recent advances, challenges and future research directions," Electronics, vol. 11, no. 4, Art. no. 630, 2022.
9. Raja Santhi and P. Muthuswamy, "Influence of blockchain technology in manufacturing supply chain and logistics," Logistics, vol. 6, no. 1, Art. no. 15, 2022.
10. Zaabar et al., "HealthBlock: A secure blockchain-based healthcare data management system," Computer Networks, vol. 200, Art. no. 108500, 2021.