STM JOURNALS

Journal of
Network Security

ISSN: 2395-6739 (Online)
ISSN: 2321-8517 (Print)
Volume 13, Issue 3, 2025
September–December
DOI (Journal): 10.37591/JoNS

https://journals.stmjournals.com/jons

Research JoNS

Blockchain Enabled Security Framework: Smart Healthcare

Rakeshram S.[1,*], Muthu Kumar B.[1], Ranjith S.[1], Vivek R.[1], Banu Priya M.[2], Jermina F.[2]

Abstract

To explores the transformative potential of blockchain technology in managing, securing, and ensuring the integrity of Electronic Health Records (EHRs). EHRs, which store vital patient information such as medical histories, diagnoses, prescriptions, and imaging results, are essential for enhancing healthcare delivery. Conventional centralized Electronic Health Record (EHR) systems encounter issues such as susceptibility to single points of failure, security risks, and constraints in maintaining data integrity. By leveraging blockchain's inherent properties like security, privacy, decentralization, and transparency, this research proposes a robust framework for blockchain integration into EHR systems. The framework addresses the limitations of centralized models, enabling interoperable, secure, and connected health records. Key benefits include enhanced data privacy, system transparency, improved interoperability, and automation through smart contracts. The implementation on the Ethereum blockchain showcases a practical, scalable solution that is cost-effective and adaptable for both permissioned and permissionless networks, demonstrating its potential for wide adoption in modern healthcare systems.

Keywords: Smart contracts, smart healthcare, blockchain, electronic health record

INTRODUCTION

Blockchain is a decentralized and distributed ledger system that operates across a network of computers. It securely stores data electronically, best known for its role in cryptocurrencies like Bitcoin, maintaining a trusted and decentralized records of transactions without requiring a central authority. While primarily used for recording digital asset transactions, such as cryptocurrencies, blockchain also supports other applications like contracts, medical records, and voting results. It maintains the features like: Security to data and making it difficult for hackers to tamper, Transparency in transactions and reducing fraud and corruption, Efficient use of transaction and settlements, and maintain the trust to enable the self-executing smart contracts, fostering trust between unfamiliar parties [1]. This innovative technology ensures data integrity and reliability while offering diverse applications and benefits.

***Author for Correspondence**
Rakeshram S.
E-mail: rakeshramsingaram@gmail.com

[1]Student, Department of Computer Science and Engineering (Cyber Security), Karpagam College of Engineering, Coimbatore, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science and Engineering (Cyber Security), Karpagam College of Engineering, Coimbatore, Tamil Nadu, India

Received Date: March 10, 2025
Accepted Date: July 20, 2025
Published Date: September 17, 2025

Citation: Rakeshram S., Muthu Kumar B., Ranjith S., Vivek R., Banu Priya M., Jermina F. Blockchain Enabled Security Framework: Smart Healthcare. Journal of Network Security. 2025; 13(3): 11–17p.

Motivation

Cyberattacks threaten intellectual property, personal information, financial data, and sensitive records, causing significant harm to an organization's reputation. The impact becomes critical when such attacks target smart healthcare systems, a vital component of modern healthcare [2]. Healthcare systems are expected to function continuously, providing uninterrupted services to patients, relatives and staff. To ensure the resilience smart healthcare, a robust security mechanism is essential. Blockchain's features can enhance security, making it a suitable foundation for a framework to safeguard electronic health monitoring systems [3].

Study Outline

We integrate decentralized blockchain technology into the proposed framework to alleviate the single-point-of-failure feature of the existing centralized EHR frameworks. A smart contract is developed to improve the management and sharing of patient EHRs while preserving patients' control over their personal health data [4]. It offers improved data privacy and security of EHRs by storing them on the immutable ledger of the blockchain.

BLOCKCHAIN TECHNOLOGY BASED HEALTHCARE APPLICATIONS

Today, numerous innovative solutions have emerged for the effective management of healthcare data, improved patient access to their information, and streamlined sharing of essential medical details. These advancements have been made possible through the development of digital health records, cloud-based data systems, and strengthened health information privacy regulations [5]. Blockchain-powered applications in this domain include mobile health apps, secure data exchange platforms, privacy-focused systems, financial solutions, and PSN-based healthcare frameworks, all of which are outlined in the sections below.

EHR Management System

There are a number of difficulties in managing Electronic Health Records (EHRs) under the current system. Many medical facilities handle patient data as administrators or custodians, which frequently leads to inefficiencies and treatment delays. Treatment might be delayed, for example, if medical information from one healthcare professional is not promptly shared with another [6]. Blockchain technology combines smart contracts, distributed ledgers, and encrypted identity management to provide a decentralized method of administering EHRs.

A self-executing protocol called a smart contract is made to validate, enforce, or automate transactions without requiring the assistance of a third party. Smart contracts can be used in EHR systems to perform prescribed tasks, including providing access or changing information, in response to predetermined criteria. Blockchain technology and smart contracts allow healthcare providers to uphold trust, security, and transparency.

Data Sharing System

The rapid advancement of mobile computing, smart wearable technologies, and wireless sensing has led to widespread use of various mobile and wearable devices, like smartphones, tablets, smartwatches, fitness bands, and smart glasses.

These devices support a broad spectrum of healthcare applications, including telemedicine, disease tracking, remote diagnostics, healthcare supply chain oversight, and elderly care. Large amounts of personal healthcare data are produced by these kinds of services, and all of this data is useful for scientific research and commercial healthcare service applications [7]. All parties involved: app owners, patients, research scientists, organizations, and the public healthcare system as a whole, would benefit from the appropriate interchange of patient health data.

Financial System

Blockchain technology makes it possible for several parties to exchange medical data securely and in a decentralized manner, which enhances healthcare applications. To enable real-time changes to healthcare platforms that link all stakeholders involved in a patient's care lifecycle, patient data is kept as distinct entries in files. Through the integration of payers, service providers, and users, this technology guarantees a patient payment ledger that is both secure and easily accessible [8–11]. Blockchain technology was first investigated and applied in the financial technology (FinTech) industry, which generally refers to developments in economic services. FinTech was one of the first sectors to use blockchain's potential for safe and transparent transactions to test it in conventional markets. Building upon this framework, FinTech entrepreneurs keep creating ground-breaking technologies that upend traditional financial systems and bring about revolutionary changes.

PRIOR RELATED WORK

The proposed methodology integrates blockchain and smart contract technologies with modern development frameworks to create a secure, decentralized healthcare application. The backend utilizes Solidity, a specialized programming language used to develop smart contracts on the Ethereum blockchain platform. Using features like mappings, structs, and modular smart contracts that handle data storage, access control, and business logic directly on the blockchain.

Working Mechanisms

Solidity ensures efficient organization and restricted access to sensitive patient data. Patient records are stored securely using the Inter Planetary File System (IPFS), which decentralizes data storage by storing file hashes on the blockchain, reducing costs while maintaining data integrity and security. Tools like Ganache, a personal Ethereum blockchain, and MetaMask, a browser wallet extension, facilitate local testing and user authentication. The frontend is built with Next.js, a framework recognized for its support of server-side rendering (SSR) and static site generation (SSG), which enhances performance, improves SEO, and delivers a responsive user experience [12–17]. Integration with the Ethereum blockchain is achieved using Web3.js, which provides tools for seamless interaction with smart contracts, account management, and transaction handling. The frontend connects to the blockchain via providers like HTTP or WebSocket, enabling real-time communication and enhanced user experience. Together, this methodology ensures a secure, scalable, and user-friendly healthcare decentralized application (DApp). Figure 1 shows the diagram of Ethereum blockchain.

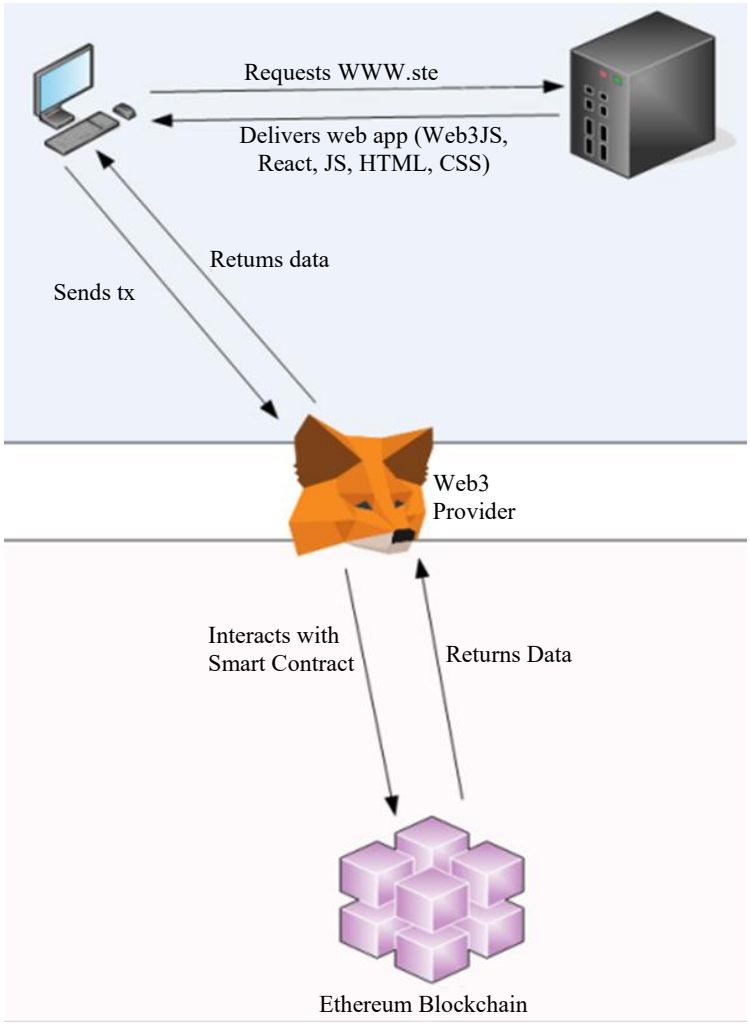

Figure 1. Workflow diagram.

Table 1 shows the comparison between traditional healthcare data systems, and the improvement highlights substantial advancements in security, efficiency, and patient empowerment.

Figure 2 illustrates the integration of blockchain technology for secure healthcare data management, focusing on transparency, patient control, and trust. Figure 2 shows the workflow diagram of Hospital/Patient Registration.

Figure 3 illustrates the network structure of the proposed framework which shows a blockchain-based healthcare data management framework that integrates hospitals, patients, decentralized storage (IPFS), and blockchain nodes to ensure secure, transparent, and patient-centric data handling.

DISCUSSION

Healthcare data holds immense value, making it a prime target for vulnerabilities and breaches. The healthcare sector stands at the forefront of transformative change, with blockchain technology poised to revolutionize the medical care landscape. Key advancements include securing electronic health records (EHRs) and preserving medical historiography. Blockchain brings all valuable healthcare data onto a unified platform, allowing authorized parties to access and modify records transparently. Any change made by one participant becomes immediately visible to all others within the framework. This integration of blockchain with healthcare infrastructure leverages core blockchain features: decentralization, immutability, and security, to address critical challenges facing the sector. Reports indicate an alarming rate of data breaches, with approximately 1.4 incidents occurring daily in 2019. Enhancing the security of electronic medical records (EMRs) for Saudi Arabian healthcare organizations has become a primary focus for researchers. This paper serves as an initial milestone in exploring blockchain as a robust security solution for healthcare systems. It evaluates the methodology's effectiveness from a data security perspective, offering a comprehensive pathway for security experts to implement blockchain-based solutions [18–25]. To validate the computational feasibility of blockchain, this study adopts a multi-criteria decision-making (MCDM) method that integrates the Fuzzy Analytic Hierarchy Process (F-AHP) with the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS). This simulation quantitatively assesses the impact of identified criteria, providing empirical evidence of blockchain's potential. The study's findings highlight both the advantages and limitations of the proposed methodology, offering valuable insights for future advancements in secure healthcare systems [26].

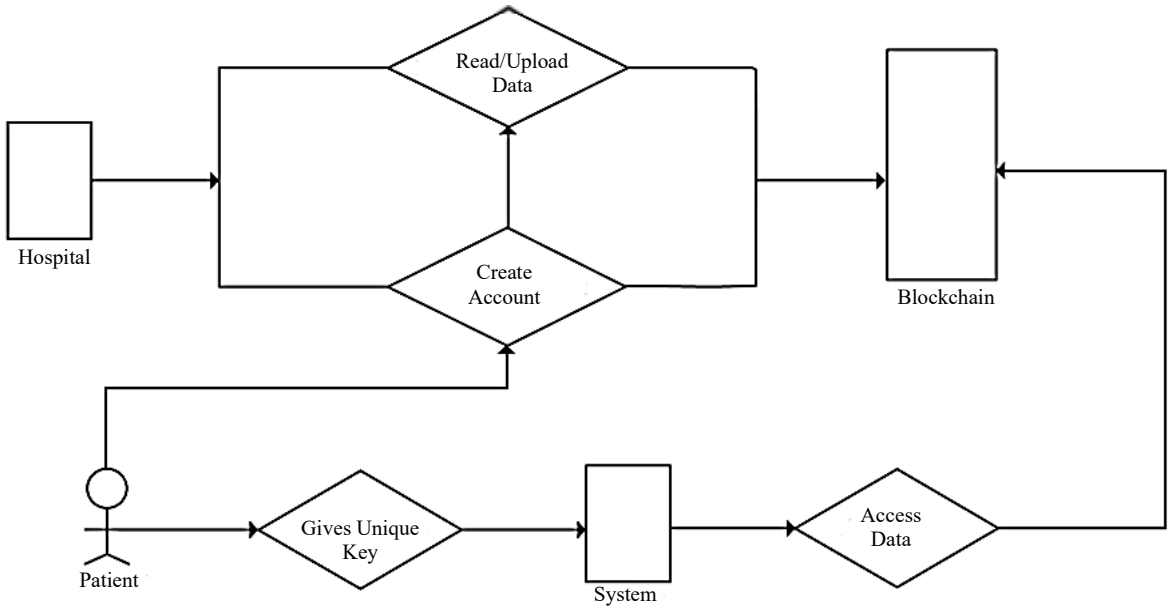

Figure 2. Hospital/patient registration.

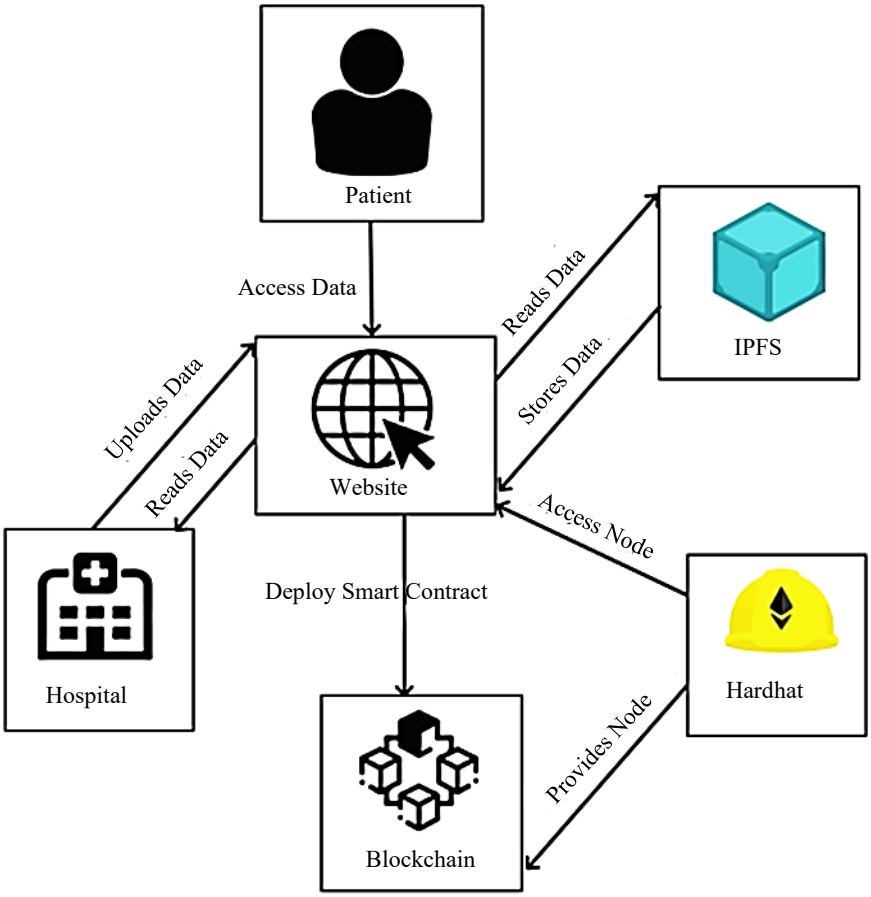

Figure 3. Network structure of proposed framework.

Table 1. Statistical comparison of blockchain and traditional system.

Metric	Analysis		
	Parameter	***Traditional System***	***Improvement***
Data Security	Data breach occurrences (year)	25 breaches (2)	92%
Patient Data Ownership	Patient control over records (%)	40%	45%
Fraud Detection	Success rate	60% (95)	35%
Cost Efficiency	Data Management	$0.15	67%

Pros

The main benefit of this study is its recommendation and focus on simulation, which could serve as a significant step in using blockchain technology to secure and protect the privacy and integrity of healthcare data in Saudi Arabia.

Limitations

Given the intricate nature of healthcare services, blockchain technology remains in its early stages within this sector. Therefore, additional empirical research is necessary to draw strong and definitive conclusions about the proposed framework. Numerous other MCDM (Multi-Criteria Decision-Making) methods exist, and their impact through various integration techniques has yet to be thoroughly explored.

CONCLUSION

We have effectively created and deployed a blockchain-based healthcare security framework that uses cutting-edge cryptographic approaches for safe data processing and Solidity for smart contract

execution. The architecture preserves accessibility and transparency while guaranteeing strong protection for patient medical records. Adopting essential features like mapping, ECC encryption, and modifiers provide a solid basis for user authentication, data integrity, and privacy. The ability to retrieve and manage patient records efficiently while preventing unauthorized access underscores the system's potential to enhance trust and collaboration within the healthcare ecosystem.

REFERENCES

1. Gorodnichev M, Kukharenko A, Kukharenko E, Salutina T. Methods of developing systems based on bockchain. In Conference of Open Innovation Association, FRUCT 24. 2019 Apr 8; 613–618.
2. Nugent T, Upton D, Cimpoesu M. Improving data transparency in clinical trials using blockchain smart contracts. F1000Research. 2016 Oct 20; 5: 2541.
3. Crosby M, Pattanayak P, Verma S, Kalyanaraman V. Blockchain technology: Beyond bitcoin. Applied Innovation. 2016 Jun; 2(6–10): 71.
4. Zheng Z, Xie S, Dai HN, Chen X, Wang H. Blockchain challenges and opportunities: A survey. Int J Web Grid Serv. 2018; 14(4): 352–75.
5. Andoni M, Robu V, Flynn D, Abram S, Geach D, Jenkins D, McCallum P, Peacock A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew Sustain Energy Rev. 2019 Feb 1; 100: 143–74.
6. Teufel B, Sentic A, Barmet M. Blockchain energy: Blockchain in future energy systems. J Electron Sci Technol. 2019 Dec 1; 17(4): 100011.
7. Li M, Shao S, Ye Q, Xu G, Huang GQ. Blockchain-enabled logistics finance execution platform for capital-constrained E-commerce retail. Robot Comput-Integr Manuf. 2020 Oct 1; 65: 101962.
8. Damico F. How technology is reshaping financial services: Blockchain use cases in the banking industry. Doctoral dissertation. Italy: Politecnico di Torino; 2020.
9. Ølnes S, Ubacht J, Janssen M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Gov Inf Q. 2017 Sep 1; 34(3): 355–64.
10. Zhang P, Boulos MN. Blockchain solutions for healthcare. In Precision medicine for investigators, practitioners and providers. Academic Press; Massachusetts. 2020 Jan 1; 519–524.
11. Ray PP, Dash D, Salah K, Kumar N. Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. IEEE Syst J. 2020 Jan 22; 15(1): 85–94.
12. Alammary A, Alhazmi S, Almasri M, Gillani S. Blockchain-based applications in education: A systematic review. Appl Sci. 2019 Jun 13; 9(12): 2400.
13. Xiong H, Dalhaus T, Wang P, Huang J. Blockchain technology for agriculture: applications and rationale. Front Blockchain. 2020 Feb 21; 3: 7.
14. Bhuiyan MZ, Zaman A, Wang T, Wang G, Tao H, Hassan MM. Blockchain and big data to transform the healthcare. In Proceedings of the international conference on data processing and applications. 2018 May 12; 62–68.
15. Mandl KD, Markwell D, MacDonald R, Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ. 2001 Feb 3; 322(7281): 283–7.
16. Arsene C. The global “Blockchain in healthcare” report: the 2021 ultimate quide for every executive. Healthcare Weekly. 2020.
17. Kumar R, Pandey AK, Baz A, Alhakami H, Alhakami W, Agrawal A, Khan RA. Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security. Symmetry. 2020 Apr 22; 12(4): 664.
18. Abusaaq H. Kingdom of Saudi Arabia 2020 budget report. KPMG Professional Services; Amstelveen, Netherlands. 2019.
19. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst. 2016 Oct; 40(10): 218.
20. Kumar R, Khan AI, Abushark YB, Alam MM, Agrawal A, Khan RA. An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications. IEEE Access. 2020 Jan 29; 8: 50944–57.

21. Ertuğrul İ, Karakaşoğlu N. Comparison of fuzzy AHP and fuzzy TOPSIS methods for facility location selection. Int J Adv Manuf Technol. 2008 Nov; 39(7): 783–95.
22. Liang X, Zhao J, Shetty S, Liu J, Li D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC). 2017 Oct 8; 1–5.
23. Zheng X, Vieira Campos A, Ordieres-Meré J, Balseiro J, Labrador Marcos S, Aladro Y. Continuous monitoring of essential tremor using a portable system based on smartwatch. Front Neurol. 2017 Mar 15; 8: 96.
24. Malina L, Hajny J, Dzurenda P, Ricci S. Lightweight Ring Signatures for Decentralized Privacy-preserving Transactions. In ICETE. 2018 Jul 26; 692–697.
25. Till BM, Peters AW, Afshar S, Meara JG. From blockchain technology to global health equity: can cryptocurrencies finance universal health coverage?. BMJ Glob Health. 2017 Nov 10; 2(4): e000570.
26. Huang J, Wang H, Wu Q, Yin J, Zhou H, He Y. Clinical research on neurological and psychiatric diagnosis and monitoring using wearable devices: A literature review. Interdiscip Med. 2024 Oct; 2(4): e20230037.

