Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 3
Open Access

Revolutionizing Healthcare Security: A Comprehensive Exploration of Blockchain-Based Medical Data Protection

[1]Kapil Netaji Vhatkar, [2]Atul B.Kathole,[3]Dipmala Salunke,[4]Jayesh Mohanrao Sarwade
[5] Nisarg Gandhewar
[1]Department of Computer Engineering,
Dr. D. Y. Patil Institute of Technology, Pimpri, Pune-411018
kapilnv@gmail.com
https://orcid.org/0000-0003-4629-107X
[2]Department of Computer Engineering,
Dr. D. Y. Patil Institute of Technology, Pimpri, Pune-411018
atul.kathole1910@gmail.com
[3]Department of Information Technology,
JSPM's RajarshiShahu College of Engineering,
Pune-411033
dtsalunke_it@jspmrscoe.edu.in
[4]Department of Information Technology,
JSPM's RajarshiShahu College of Engineering, Pune-411033
jayesh.sarwade@gmail.com
https://orcid.org/0000-0003-1815-5484
[5]Assistant Professor,
Shri Ramdeobaba College of Engineering & Management, Ramdeobaba University, Nagpur
nisarg.gandhewar@gmail.com

Cite this paper as: Kapil Netaji Vhatkar, Atul B.Kathole,Dipmala Salunke,Jayesh Mohanrao Sarwade Nisarg Gandhewar (2024) Revolutionizing Healthcare Security: A Comprehensive Exploration of Blockchain-Based Medical Data Protection. *Frontiers in Health Informatics, 13* (3), 2521-2529.

Abstract: *Healthcare organizations struggle with electronic health records (EHRs) because they digitize medical data. Doctors and patients spend a lot of time accessing EHRs for information, but if the data isn't relevant, access can be blocked. Sharing and retaining medical records is crucial to healthcare. Losing patients' privacy and correct medical information would be terrible. It is one of the main reasons electronic health records must be secure. Modern healthcare infrastructure is notoriously inefficient in data integrity, security, and privacy. However, well-managed and monitored EHRs may reduce security and complexity difficulties. The blockchain's decentralization and trustworthiness make this possible in healthcare. The healthcare delivery system has inherent data management and validation and dissemination issues. Blockchain technology improves access to drugs, hospital assets, drug systems, patient data, and more for healthcare data management. Blockchain technology could improve healthcare by giving doctors rapid access to their patients' medical histories, which is essential for prescription drugs. Thus, a blockchain-based medical record verification and security solution is essential. This article focuses on building a permissioned blockchain-based Ciphertext Policy-Attribute encryption system to protect personal data and restrict medical record access. When all qualities are fine-tuned during encryption, the meta-heuristic model improves. Optimization reduces ciphertext size, encryption costs, and communication costs. Finally, the performance evaluation shows that the proposed method is as reliable and robust as state-of-the-art designs.*

Keywords- *Healthcare, HER,Security, Privacy , blockchain*.

1. Introduction

The healthcare industry is undergoing a transformative shift towards digitization, with the adoption of Electronic Health Records (EHRs) and other health information technologies. While these advancements offer numerous benefits, they also bring about concerns regarding the security and privacy of sensitive medical data [1]. This is majorly due to cyber threats, data leakage, and unauthorised access are one of the major threats to the patients data [3]. Blockchain seems to be the best solution for these issues since it implements distributed, safe, and open approaches for processing medical information. This approach not only increases the protection of patient records but also provides data accountability, audi trial, and patient control over personal information [3].

1.1 Key Components of a Blockchain-Based Approach:

Decentralized Data Storage:

• Objective: Reduce dependency on a single point of failure and intruder breach [4].

Immutable Record Keeping:

• Objective: Protect data relevancy, data consistency and also to maintain the check and balance of medical information [5].

Patient-Controlled Access and Consent:

• Objective: Health information should be in control of the patients [6].

Interoperability and Data Exchange:

• Objective: Ensure that health statistics information can move freely and safely from one healthcare provider to another [7].

Secure Identity Management:

• Objective: Minimise on the cases of identity theft and other cases of unlawful intrusion into the houses of patients records [10].

Auditable Access Logs:

• Objective: To increase accountability and traceability of accessed data in the observed protocols..

1.2 Objective of work:

- Implement blockchain to provide an immutable and tamper-proof ledger for storing medical data [10].
- Ensure that once medical data is recorded on the blockchain, it cannot be altered or deleted, maintaining the integrity of patient records.
- Utilize smart contracts to establish access controls that allow patients to control who can access their medical records [11].
- Empower patients to grant or revoke access permissions, ensuring that only authorized healthcare providers can view specific aspects of their health information.
- Enable healthcare organizations and regulatory bodies to audit and trace access to patient records, ensuring accountability and aiding in investigations.
- Implement monitoring tools and processes to continuously assess the security posture of the blockchain-based medical data system [12].
- Proactively identify and address potential security vulnerabilities, ensuring ongoing improvement and adaptability to emerging threats.

By defining and pursuing these objectives, a blockchain-based approach to ensuring the security of medical data can effectively address key challenges, empower patients, and create a resilient and trustworthy healthcare information ecosystem [13].

2. Related work:

What has prompted interest in a blockchain solution to the system interoperability, privacy, and data integrity problems in healthcare settings is the fragility of patient medical data. Here are some synopses of relevant studies and works in this field: The [1] The paper notes that the comprehensive review explores numerous innovations of the blockchain in healthcare. It expounds on security as provided by blockchain through data authenticity, patient centred approach and interconnection issues. The paper outlines past and identified current issues and proposes possibilities for future studies.

This [2] brings a discussion of how EHRs can be protected by the use of blockchain technology. It underlines the stability and openness characteristics of blockchain to increase the reliability of the patient's records. This paper explains how a system based on the blockchain can be protected against attempts at alteration or additional unauthorized access.

The paper [3] proposes a distributed framework to securely and privately share EHRs using blockchain. Despite the use of smart contracts to facilitate the access controls, the authors explain that patients have more control over the access of their personal records. It is crucial to maintain the confidentiality of the information in health care facilities as postulated by the work. Special attention is paid to the application of blockchain in the pharmaceutical supply chain, and the work investigates how to identify counterfeit drugs using this technology. The study highlights that blockchain's application in the supply of drugs has the power of guaranteeing the originality and security of the product [4].

Finally in [5] this paper presents a systematic review of security concerns and the solutions to the use of blockchain in health care. It comprehensively includes coverage of such areas as data privacy, access control, and networks. In the paper, the author gives an overview of contemporary issues for medical data that are addressed by blockchain and possibilities of solutions.

Whereas in paper [7] case use of smart contracts for e-Health record (EHR) based on blockchain technology is discussed. The authors explain how the notion of smart contracts can be leveraged to improve the objective of making records transparent, secure, and controlled by the patient. Taken together, these works as a whole represent an important contribution to the question of how exactly blockchain technology can be used to properly protect medical information [8]. As discussed above it tackles challenges concerning data authenticity, patient's privacy, and the extent of which the system is open and transparent and thus the possible implications of blockchain in changing the face of H Im [9].

3. Proposed work flow:

Explaining how to assure the security of the medical data using blockchain approach it is possible to define the flowchart for the phases and interactions of the system. The suggested method is illustrated by the following simple flowchart: This flowchart outlines the main steps in the process [10]:

1. Start the process.

2. Will be given/transmitted a new transaction t = (sender, recipient, data) [1].

3. Wonder if the necessary fields are missing from the transaction.

4. The new block contains the transaction: make a new block.

5. Make a proof of work to the search for the new proof.

6. Make new block append to the blockchain [11].

7. Answer to facts regarding the mined block.

8. Optionally, we can see the whole blockchain.

9. End the process.

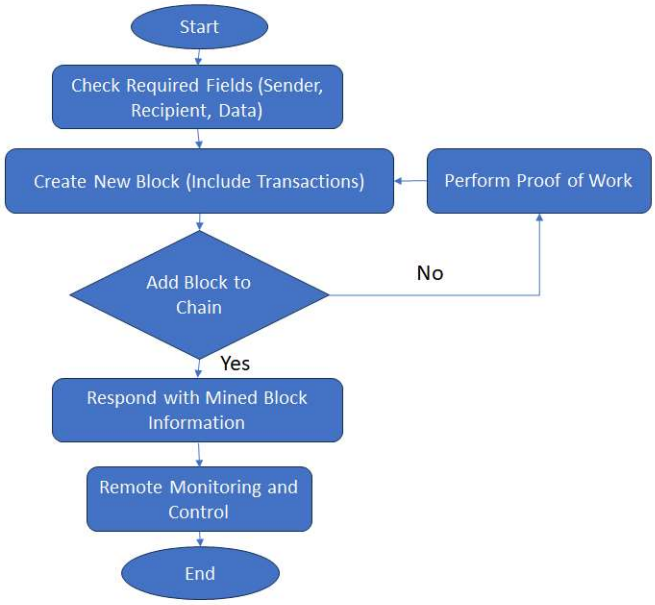

Figure 01: Flow of Proposed Approach

However, it has to be noted that the flowchart is intentionally kept simple for instructional presentation only [12]. Moreover, in a real-world context [9], other features such as security or encryption and adherence to relevant regulations governing the healthcare industry, would have to be implemented as well [3].

3. Discussion and flow of implementation:

Secure medical data using blockchain is achieved through coming up with a blockchain, proper encryption of data, and deployment of access control smart contracts[11].

The blow is a raw proposal of a simplified approach using python: It should also be noted, however, that this is just an example and in a real-world application a seemly professionally oriented approach would be needed [13].

Step 1: Install Required Libraries pip install Flask pip install Flask-SocketIO pip install cryptography

Step 2: Blockchain Class

```
import hashlib
import json
from time import time
from uuid import uuid4
from flask import Flask, jsonify, request
from hashlib import sha256

class Blockchain:
    def __init__(self):
        self.chain = []
        self.current_transactions = []
        self.nodes = set()

        # Genesis block
        self.new_block(previous_hash='1', proof=100)

    def new_block(self, proof, previous_hash=None):
        block = {
            'index': len(self.chain) + 1,
            'timestamp': time(),
            'transactions': self.current_transactions,
            'proof': proof,
            'previous_hash': previous_hash or self.hash(self.chain[-1]),
        }

        # Reset current list of transactions
        self.current_transactions = []

        # Append the block to the chain
        self.chain.append(block)
        return block
```

Step 3: Introducing the End User to the Blockchain

curl -X GET http://localhost:5000/mine

curl -X GET http://localhost:5000/chain

On a production system other factors like data encryption, access control, and adherence to healthcare standards are other factors that should be put into consideration [11]. Also, it is recommended to extend the used frameworks like Flask-RESTful and Flask-RESTful-reqparse for the API request handling [14].

3. Application of Working Approach:

This has the benefit of making public health surveillance systems work better.

• It makes sense to store genomic data on a blockchain to protect personal data and guarantee their authenticity.care use cases [12]. Here are some specific applications of blockchain in securing medical data [16]:

• Storing patient health records on a blockchain ensures immutability, transparency, and secure sharing. Patients can control access to their data through smart contracts, enhancing privacy and security.

• Using blockchain to record the journey of drugs from manufacturing to distribution ensures authenticity and prevents the entry of counterfeit drugs. Each transaction is recorded on the blockchain, providing a transparent and tamper-proof history.

• Storing research data on a blockchain ensures data integrity and prevents manipulation. Smart contracts can facilitate transparent and automated processes for data sharing and consent management among research collaborators [17].

• Integrating blockchain for secure device communication and data exchange. Each device interaction is recorded on the blockchain, reducing the risk of unauthorized access or manipulation of health-related data.

• Issuing and managing cryptographic identities on the blockchain enhances security. Smart contracts control access permissions, ensuring that only authorized entities can access sensitive medical data.

• Utilizing blockchain to record and verify patient data collected through remote monitoring devices. Smart contracts can facilitate secure and transparent data sharing between healthcare providers and patients.

• Recording epidemiological data, vaccination records, and health statistics on a blockchain ensures accuracy and transparency. This can improve the efficiency of public health surveillance efforts [11].

• Storing genomic data on a blockchain ensures the integrity and privacy of sensitive genetic information. By applying blockchain erasing technologies, authorization control to patient's genomic information can be given within the patient's mobile device [12].

These applications show that by incorporating a blockchain, the framework can strengthen the security, privacy, and openness of the medical data in the overall health care system. The implementation should take cognizance of the need and the legal factors that may apply to each use case [9].

4. Advantages and Disadvantages of Proposed System

Transparency, decentralization, changelessness, and stronger security from cryptographic solutions make a blockchain framework suitable for medical data preservation. Security is inherent in blockchain by design because patient data can only be stored and entered into the database and cannot be changed or deleted. This includes medical data [10].

By dispensing with the need for a centralized control, decentralization enhances system reliability by having multiple locations of control and thus less vulnerability to a point of failure. A main benefit is transparency because all participants in the network have access to all the data present in the whole blockchain [15]. To avoid situations when unauthorized individuals intercept personal health information, cryptographic methods are applied to data storage and exchange [4].

Furthermore, by including smart contracts, in a healthcare system based on blockchain, it is easier to implement and monitor access controls automatically. This also implies that only those who have been privileged to do so by smart contracts can access certain medical data giving unique control over the data's privacy and security [16]. It guarantees an auditable and traceable record of medical data transactions flow and also supports application, including drug traceability for ascertaining the legitimacy and quality of drugs in the market. As well, the use of consent mechanisms enables the patient gain more control of his/her data by giving or denying access as he/she deems fit [5].

The one that stand out is the regulatory risks, especially in such areas as healthcare and emerging Blockchain technology that brings in regulatory risks and compliance, which one needs to adapt to, in order to meet emerging regulations.. Implementing blockchain together with existing and future HCITs is a challenging task that requires appropriate interdisciplinary mapping and assessment of interfaces based on HL7 FHIR.

Protecting data is important and responding to this challenge may entail for example encoding and privacy preservation mechanisms [8].

6.1 Advantages

- The parties involved in the network have full view over the entire blockchain thus encouraging for transparency [11].
- This is because in every transaction, the previous data is pulled in and the end result added to the history of medical data.
- Patients are also the actors in consent mechanisms and therefore have more control over patient data [12].
- Each transaction is linked to the previous one, creating an auditable and traceable history of medical data.

6.2 Disadvantages

• Consequently, as the content of the blockchain continues to expand with height, it is bound to face a problem that relates to the issue of scalability, which is likely to reduce its performance.

• Some bases of consensus like the proof-of work model utilized by many blockchain systems could be power hungry [13].

• Implications of Distributed Ledger Technology for Healthcare: Sometimes, logistics of incorporating blockchain into current healthcare information technology architecture could be challenging.

• There are no global best practices for implementation healthcare blockchains [14].

• The various stakeholders such as the users – clinicians and patients may require training on the block chain solutions. work consensus mechanisms, as used in many blockchains, can be energy-intensive.

• Integrating blockchain with existing healthcare IT systems can be complex.

• Lack of standardized protocols and frameworks for healthcare blockchains can hinder interoperability.

• Users, including healthcare professionals and patients, may need education on blockchain technology and its implications [15].

It is also important to realize that the benefit and the risk may be different for each implementation and for the business which uses it. Solving these problems presupposes thoughtful planning [10], cooperation, and the constant development of new technologies related to the application of the blockchain in healthcare.

5. Conclusion:

Therefore, it is promising to develop a blockchain-based system that is aimed at safeguarding medical data since it can bring about transformation of healthcare industry. Some of the attributes that make blockchain technology include changelessness, structure, transparency, and security form the major challenges associated with data accuracy, privacy, and compatibility in a healthcare setting. This approach offers a secure and efficient method of Cryptographic techniques and Smart Contracts for protect health data, give back Control over the data to the patients and automated access management. Even generally applied advantages of blockchain technology, like the traceability and the making of a genesis history of medical transactions impossible to forge, are usable for objectives like drug identification and patient record.

The ability to improve operations, accuracy, and decrease fraud risk associated with operations in healthcare justify the use of blockchain. Nevertheless, it necessary to mention the difficulties and concerns encountered in the application of blockchain in the healthcare industry. Impediments significantly include scaling issues, the environmental impacts likely to be caused by some energy demanding consensus algorithms, legal frameworks and the issue of compatibility with current systems. It is important for industry players,

policymakers, and technology gurus to come up with a common goal of how to get over these hurdles. In the context of the path toward a blockchain healthcare system, there is a need to focus on user adoption, the proper explanation of the principles of blockchain in healthcare to different classes of users. Also, following the changes in regulations, creating the set of common rules for the integration of blockchain technologies into the healthcare system is critical.

Therefore, although a blockchain-based approach offers new concepts to increase the safety and reliability of medical records, its efficient adoption depends on the holism and dynamism of the strategy. Here, the future of the healthcare industry is discussed together with the ways that accepting the innovative tools such as blockchain could transform the system and make it more effective, safe, and focused on patients.

References:

[1] SD Patil, AB Kathole, S Kumbhare, K Vhatkar, "A Blockchain-Based Approach to Ensuring the Security of Electronic Data", International Journal of Intelligent Systems and Applications in Engineering,2024.
[2] Taherdoost, H. Blockchain-Based Internet of Medical Things. *Appl. Sci.* **2023**, *13*, 1287.
[3] Busayatananphon, C.; Boonchieng, E. Financial technology DeFi protocol: A review. In Proceedings of the 2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), Chiang Rai, Thailand, 26–28 January 2022; pp. 267–272.
[4] Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R.; Khan, S. A review of Blockchain Technology applications for financial services. BenchCouncil Trans. Benchmarks Stand. Eval. 2022, 2, 100073.
[5] Anwar, M.R.; Apriani, D.; Adianita, I.R. Hash Algorithm In Verification Of Certificate Data Integrity And Security. Aptisi Trans. Technopreneurship (ATT) 2021, 3, 181–188.
[6] K. N. Vhatkar and G. P. Bhole, "Optimal container resource allocation in cloud architecture : A new hybrid model," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 5, pp. 1906–1918, 2022, doi: 10.1016/j.jksuci.2019.10.009.
[7] K. N. Vhatkar and G. P. Bhole, "Particle swarm optimisation with grey wolf optimisation for optimal container resource allocation in cloud," IET Networks, vol. 9, no. 4, pp. 189–199, 2020, doi: 10.1049/iet-net.2019.0157.
[8] Al Omar, I. Rahman, and A. Kamsin ," Blockchain-Based Solutions for Healthcare Data Management: A Review", Journal of King Saud University - Computer and Information Sciences, 2020.
[9] K. O. Acheampong et al," Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention", PLOS ONE, 2020.
[10] Y. Zhang, S. Wen, Y. Yu, and T. J. O. Dickson," A Survey of Blockchain Security Issues and Solutions for Healthcare", Journal of Network and Computer Applications, 2019.
[11] K. N. Vhatkar and G. P. Bhole, "Improved rider optimization for optimal container resource allocation in cloud with security assurance," International Journal of Pervasive Computing and Communications, vol. 16, no. 3, pp. 235–258, 2020, doi: 10.1108/IJPCC-12-2019-0094.
[12] K. N. Vhatkar and G. P. Bhole, "A comprehensive survey on container resource allocation approaches in cloud computing: State-of-the-art and research challenges," Web Intelligence, vol. 19, no. 4, pp. 295–316, 2021, doi: 10.3233/WEB-210474.
[13] K. M. Gadd, K. A. Valdez, and J. E. Brenner," Blockchain for Health Data and Its Potential Use in Health Professions Education", Academic Medicine, 2019
[14] M. Y. Kan, K. Y. Lam, and K. L. Li," Blockchain for Securing Sustainable Internet of Things: Recent Advances and Opportunities", IEEE Internet of Things Journal, 2019.

[15] Atul B Kathole, Dr.Dinesh N.Chaudhari, "Pros & Cons of Machine learning and Security Methods, "2019.http://gujaratresearchsociety.in/index.php/ JGRS, ISSN: 0374-8588, Volume 21 Issue 4

[16] Atul B Kathole, Dr.Prasad S Halgaonkar, Ashvini Nikhade, " Machine Learning & its Classification Techniques, "International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-9S3, July 2019.

[17] M. L. R. Baars et al.," Blockchain-Based Electronic Health Record: A Case Study of Smart Contracts", Studies in Health Technology and Informatics, 2018.