Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 7, pp. 2191–2206
DOI : 10.47974/JDMSC-2091

A blockchain-based encrypted method for obtaining and storing EHRs

Vimmi Malhotra *
Sandeep Joshi †
Varun Tiwari §
School of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

A revolutionary technology called blockchain is being applied to many different areas of healthcare. Numerous enhanced outcomes in the medical sector have been demonstrated by it. Blockchain is still used in modern EHRs despite its improved performance in addressing data quality, availability, confidentiality, and interoperability concerns. This paper focuses on discovering the potential of blockchain technology in transforming EHR systems and providing a potential solution to these problems. We put up a framework that might be applied to adopting electronic health records in the blockchain industry. Our suggested framework aims to do two things: first, it will enable EHRs to incorporate blockchain technology; second, it will give its customers safe electronic record storage by establishing Algorand. In addition, this framework addresses the issue of scalability that blockchain technology, in general, faces by utilizing Algorand record storage, which covers both off-chain and on-chain storage. The scalability, security, and integration of a blockchain-based solution are advantages that this framework offers the EHR system.

Subject Classification: *Primary 68M12, Secondary 90B18.*

Keywords: *Algorand, P-POS, Scalability, Decentralization, EHRs, Security*

* *E-mail:* **malhotra.vimmi22@gmail.com (Corresponding Author)**
† *E-mail:* **sandeep.joshi@jaipur.manipal.edu**
§ *E-mail:* **varun.tiwari@jaipur.manipal.edu**

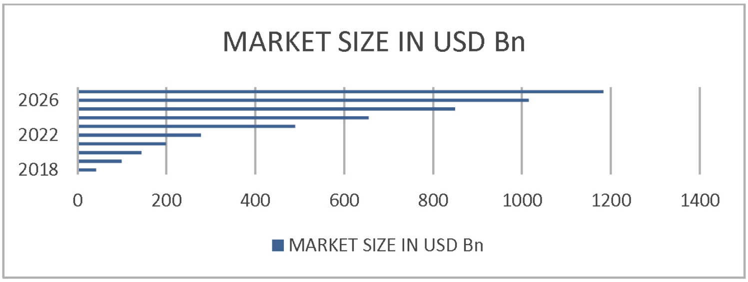

Figure 1

Digital Transformation in Healthcare Market [8]

1. Introduction

The distributed and decentralized [1] environment made possible by blockchain [2] technology eliminates the need for a solo power foundation. Due to its ability to connect disparate systems, enhance the quality of electronic medical records, and change the way healthcare is provided, blockchain technology has the most potential in the healthcare industry [3] [4], which further helps in producing a more patient-centric perspective.

The digital transformation and adoption of data in the healthcare market are shown in Figure 1. [8] A growing number of individuals have observed in recent years that blockchain technology has the potential to accelerate the digitization of health and medical systems. [5] [6] Many academics are interested in blockchain because it is a breakthrough decentralized information technology with a lot of potential applications in the medical and healthcare sectors [4], specifically in the progress and application of EHRs. [7]

The famous Electronic Health records (EHRs) [2] are like digital libraries for patient health information. They store an all-inclusive record of a patient's medical history in a secure electronic format, including their diagnoses, treatments, medications, and test results. EHRs have revolutionized healthcare providers' management of patient information, moving from traditional paper-based systems to streamlined, efficient digital platforms.

The main benefits of using Blockchain technology in healthcare [9] [10] are improving the following trilemma: healthcare data security, user scalability, and other aspects such as better treatment, availability of hospitals nearby and instant reports available on patient mobile. Earlier, these advantages are covered by Electronic Health Record (EHR) [11] and Electronic Medical Record (EMR) machines or servers. However, they silent face some concerns regarding the security of medical records, user ownership of data, data integrity, etc., which are discussed in the upcoming section.

1.1 *ISSUES in Current EHR*

Electronic Health Records (EHR) [2] [12] have revolutionized how healthcare providers manage patient information, but they are not without challenges. Here are some common issues that occur in EHR systems:

a) **Interoperability Problems:** Lack of platform compatibility is one of the main issues EHR systems have to deal with. Different EHR systems [2] that healthcare providers frequently use might not be able to communicate with one another well. This may result in fragmented patient data, jeopardizing patient safety and making it more difficult to coordinate care effectively.

b) **User Interface Complexity:** The intricate user interfaces of EHR systems are frequently criticized for being challenging to use and navigate. Healthcare workers [13] [14] who are too busy to search for information rapidly may become frustrated and make mistakes in their documentation.

c) **Data Security Concerns:** Health records are becoming more digital, which increases the probability of data breaches [15] and illegal access. Keeping private patient data safe from online attacks is a never-ending task for healthcare institutions. The supplier may have financial, legal, and reputational consequences if strong security measures aren't implemented. [13]

d) **Data Entry Burden:** In order to spend more time with patients, healthcare providers frequently have to spend a lot of time entering data into EHR systems. The burden of documentation can lead to physician burnout and reduced job satisfaction. Additionally, manual data entry increases the risk of errors and inconsistencies in the patient record. [9]

e) **Alert Fatigue:** Many alerts and notifications are frequently generated by EHR systems for a variety of clinical events, such as drug interactions or unusual test findings. On the other hand, an overwhelming quantity of notifications may cause alert fatigue in healthcare personnel. Alerts may grow boring to providers, and they can overlook important information in the commotion.

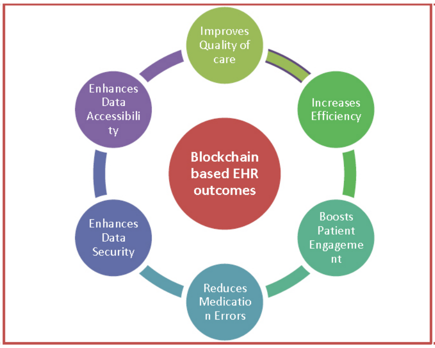

Figure 2

Healthcare Outcomes Using Blockchain Technology

Healthcare providers, technology companies, legislators, and regulatory agencies must work together to address these problems. Stakeholders can cooperate to maximize the potential benefits of EHR systems while minimizing their negatives by emphasizing interoperability, upgrading data security measures, improving user interface design, and lowering documentation burdens. Thus, blockchain technology has made a lot of sense for the healthcare industry, and it has been in the news lately. [13]

All things considered, blockchain [16] can enhance EHR interoperability [9] by facilitating safe and easy data interchange between healthcare systems and providers. With blockchain technology, patients can give particular healthcare providers access to their data and maintain more control over their health information. This may result in less redundant testing, better healthcare outcomes, and more integrated care. These results are shown in Figure 2.

In summary, healthcare data management's security, interoperability, and effectiveness could be greatly enhanced by integrating blockchain technology into Electronic Health Records (EHRs). Blockchain's revolutionary features can be leveraged to make EHRs more transparent, secure, and patient-focused. In the end, this shift will completely change the way healthcare is provided and experienced by both doctors and patients. [17]

Below is the structure of this paper: In this paper, section 2, we provide an overview of the fundamentals of blockchain technology, including how hash value is computed and how it depends on the current design. It also describes the related work that has been done in this field. With several blockchain structure tiers and data storage, Section 3 describes the system architecture and design of the suggested work. The framework's suggested paradigm is explained in Section 4, along with how smart contracts and the Algorand consensus process in the relevant healthcare blockchain lead to better data storage. Concluding remarks and references are given in the final section.

2. About Blockchain Technology

Through a network of computers, safe and transparent transactions may be carried out thanks to a distributed ledger system known as blockchain technology. Although it's frequently linked to cryptocurrencies like Bitcoin, [18] its possible uses go much beyond virtual money. [9] Blockchain technology has become a game-changer in many different fields. Beyond cryptocurrencies such as bitcoin, [19] its reach affects a wide range of sectors, including supply chain management, healthcare, and banking. One of the main advantages is improved security through unchangeable records, more transparency [20] through distributed ledgers, immediate asset tracking, financial savings, and the possibility of innovation through smart contracts and decentralized apps. [21] Blockchain continues to be a potent instrument for changing how we handle data and transactions as businesses strive for efficiency, transparency, and trust.

2.1 *Architecture*

The cooperation of several crucial elements allows blockchain architecture to have its decentralized and secure features. In essence, a blockchain is a distributed ledger that records transactions throughout a node—a computer network—network. Each block in the chain consists of a batch of transactions that are cryptographically linked to the previous block and timestamped, resulting in an immutable record that is arranged chronologically. This comprehensive breakdown of the primary components of blockchain architecture is provided in Figure 3 below. To ensure trust and immutability, decentralized nodes in blockchain architecture use a consensus method to validate and record transactions in a distributed ledger. This ledger, which is organized as a series of cryptographically connected blocks, supports decentralized apps and smart contracts for a range of use cases, providing security and transparency.

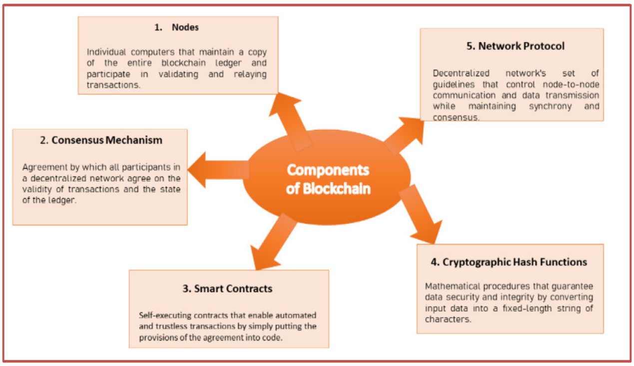

Figure 3

Primary Components of Blockchain Architecture

Figure 4 [7] presents a condensed perspective of a blockchain network block, highlighting the many characteristics of the block. A safe and unchangeable chain of records is created by each block, comprising a batch of transactions that are cryptographically connected to the previous block. Cryptographic hash functions [16] guarantee the integrity and security of the data kept on the blockchain, while smart contracts on the blockchain allow for programmable and automated transactions. The network protocol makes the blockchain'S distributed and decentralized structure possible, making it easier for nodes to interact and communicate with one another.

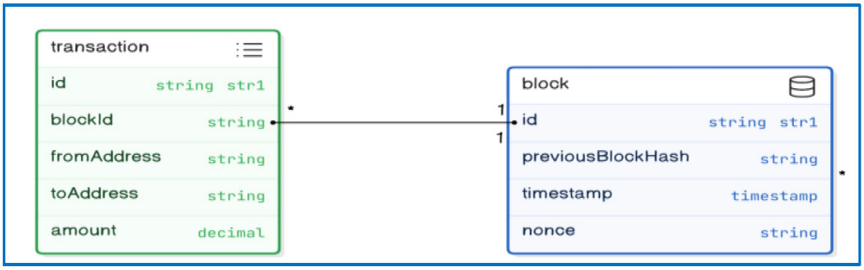

Figure 4

Blockchain Block Structure [7]

2.2 *Calculation and Generation of Hash*

When input data, like transaction details or block contents, are subjected to a cryptographic hash function [14] SHA-256 (Secure Hash Algorithm 256-bit), the result is a fixed-length string of characters that is specific to the input data. This process is known as hash generation. Integrity and security are provided to the data stored on the blockchain by this hash, which acts as a digital fingerprint. Mathematically, it can be represented as:

$$H = \text{HashFunction}(D)$$

where:

- H is the resulting hash value.
- *HashFunction* represents the specific cryptographic hash function used (e.g., SHA-256).
- D is the input data (e.g., transaction details, block contents).

The output H is a fixed-size string of characters representing the unique hash value of the input data D, ensuring integrity and security within the blockchain network. A simple example as a reference is shown in Figure 5. [15]

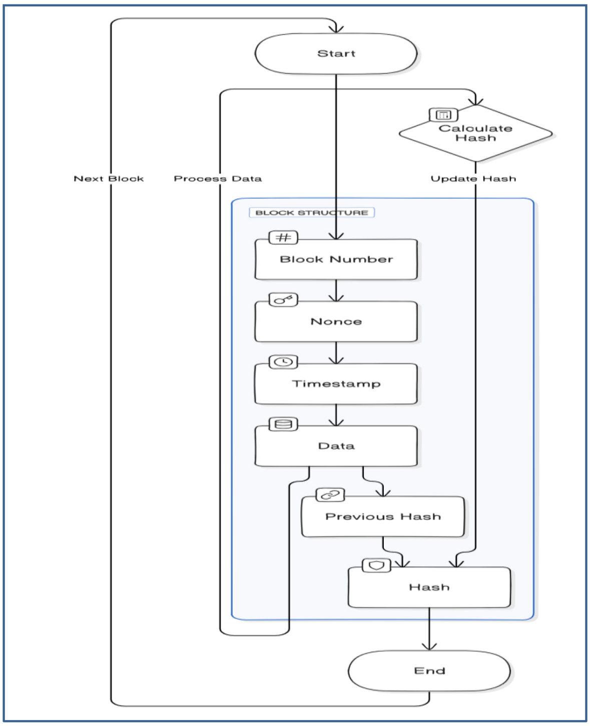

Figure 5

Hash Generation in the Single Block [15]

2.3 *Associated Work*

Shahnaz et al. [22] propose an EHR system based on blockchain, which statements the issue of data security, interoperability and patient privacy in healthcare systems. This system focuses on the creation of a decentralized and tamper-proof ledger of patient records, ensuring data integrity and confidentiality. They demonstrated the feasibility of implementing blockchain-based EHR systems to improve data management and patient care in healthcare settings on the following parameters. Shamshad et al. [23] presented an innovative e-health records storage and sharing scheme based on blockchain technology to modernise healthcare data management, potentially improving both security and accessibility in the healthcare sector. Anik et al. [24] discuss scoping review highlights how blockchain technology might revolutionize patient empowerment and smart health technologies. It also highlights the obstacles that need to be overcome and future directions for study and use in this rapidly developing field. Bertony Bornelus et al. [25] offer a hands-on lab for creating decentralized blockchain applications in public health. The framework, which uses active learning to propose blockchain technology for healthcare, will assist students in determining their present proficiency level. Zheng et al. [26] present a summary of the steps involved in developing smart contracts, the obstacles that developers must overcome, and solutions for those issues. Conti et al. [27] article demonstrates how Algorand, using various criteria and study findings, may resolve the blockchain technology trilemma very effectively and efficiently. It also describes how to maximize smart contract performance by utilizing consensus mechanisms from a different blockchain.

Together, these research articles examine the potential and obstacles [28] related to deploying blockchain technology in healthcare while highlighting the technology's significant uses in this field. Blockchain has the ability to change healthcare data management, improve patient outcomes, and increase confidence and openness in healthcare systems with more study and cooperation.

3. System Design and Architecture

Implementations of blockchain technology in healthcare [4] [29] that have been done till now are listed in the associated work section. As mentioned before, they provided particular remedies for the typical problems with blockchain technology. Most of the research on the topic was concerned with the scalability and data-sharing challenges of blockchain technology. They proposed utilizing IPFS [30] for both on-chain and off-chain data storage, together with Ethereum for the overall establishment of the blockchain framework. However, we will employ a novel strategy for efficient data storage called Algorand for improved scalability, security and interoperability. Python and Teal will be used for the overall implementation.

3.1 *System Design*

The architectural planning and execution of blockchain-based systems is referred to as system design. It entails creating a blockchain network's architecture, protocols, and constituent parts with the intention of achieving particular objectives, including efficiency, scalability, security, and decentralization [31][32]. To build a reliable and efficient blockchain system, trade-offs between decentralization, security, scalability, and usability must be balanced.

Figure 6 below illustrates the six elements that make up our proposed framework or system. Integration of these modules would not affect our system's functionality. The following layer will see the complete development of three new modules, while some ideas pertaining to these entities or modules must be understood: Blockchain consensus on Pure Proof of Stake (P-POS) [27] and the application layer using smart contracts, Python and Teal tools and programming modules, as previously mentioned in Figure 6. Users such as doctors, nurses, administrators, and patients may find value in the proposed framework. They were given a great deal of access because their power levels within the system ought to differ. The different modules or layers are Application layer which will facilitates DApps [12] via Algorand smart contracts. Smart contracts here can be used as Stateful [27] or Standard Assests. [33]. The main advantage of Algorand is its security [33] and achievement of ensuring blockchain [34] trilemma.

Blockchain layer will ensures that all transactions are executed permanently and transparently by integrating cryptographic verifiability and Byzantine fault tolerance. [35] [36] By fusing speed, security, and decentralization. The consensus used will be P-POS. [17] [18].

Network layer provide us with strong P2P networking in order to ensure that transactions and consensus messages [37] securely takes place between nodes and it will be permission less blockchain network . CIA security triads can be achieved using cryptography algorithms [38][39].

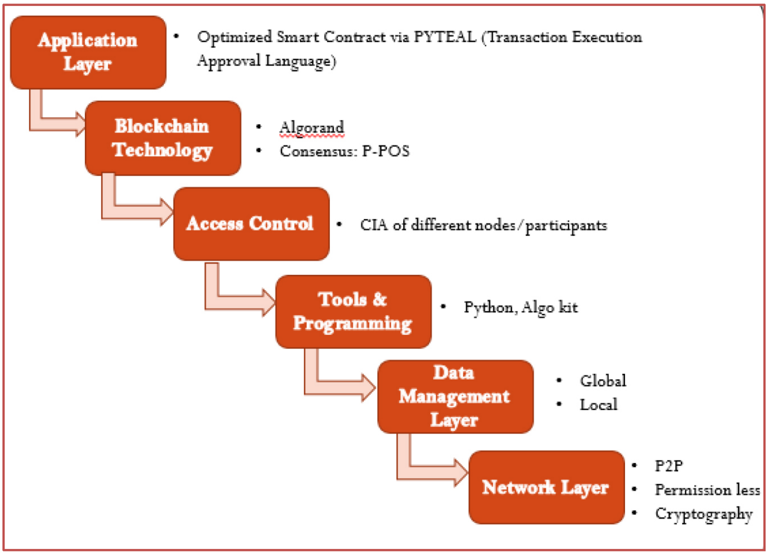

Figure 6

Proposed System Design

3.2 *Data Storage in Blockchain*

We can store data with the help of transactions and blocks in the form of chains. [38] We will validate the block using ALGORAND [27] Blockchain (P-POS) in our proposed algorithm. To participate in block creation and validation, validators in Pure Proof of Stake (P-PoS) may or may not "stake" their own cryptocurrency holdings as collateral, unlike Proof of Work (PoW) [14] and Proof of Stake (PoS), where miners compete to solve intricate puzzles. In this, the variable random function is used, which will validate the block.

3.3 *Benefits of P-POS*

- **Energy Efficiency:** Significantly lower energy consumption compared to PoW, making it more environmentally friendly.
- **Security:** The high cost of staking disincentivizes malicious behaviour, enhancing network security.
- **Scalability:** PoS can be more scalable than PoW, enabling faster transaction processing.
- **Decentralization:** More individuals can participate in the consensus mechanism, promoting decentralization.

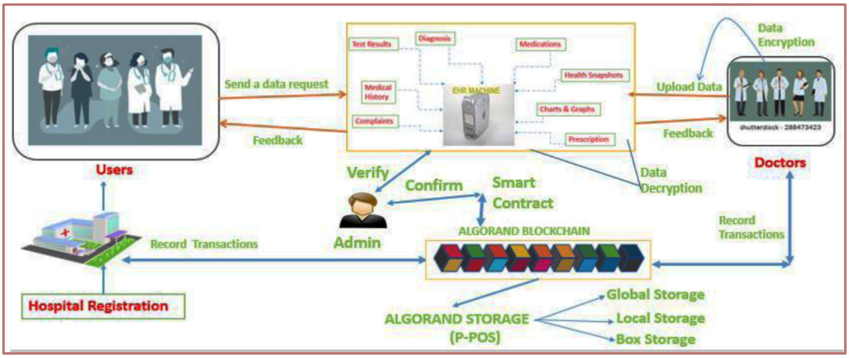

Figure 7

Proposed Framework based on P-POS Consensus

4.0 Blockchain-Based Healthcare Framework

The proposed framework discusses how efficiently and securely we can store and access patient data using the ALGORAND blockchain. Figure 7 uses the P-POS consensus mechanism in which we require a variable random function instead of miners.

Algorithm 1: Smart contract for hospital registration

1. Define the Smart Contract Logic by deciding on the rules and conditions for hospital registration.
2. Handle registration fees, permissions as per role-based, and other aspects.
3. A snippet is shown below:

```
def hospital_registration():
# Define contract logic here
# Example: Require a specific account to register a hospital
return and(
# Add more conditions as needed
)
```

Algorithm 2: Smart contract for storage using P-POS

1. On-Chain Smart Contract:

   - The PyTeal smart contract handles the registration and updating of hospital IDs on the Algorand blockchain.
   - When a new hospital is registered, the contract increments a counter and stores the hospital ID.
2. Off-Chain Database:
   - A MySQL database stores detailed hospital information, including name, address, and phone number.
   - The Python script interacts with both the MySQL database and the Algorand blockchain.
   - register_hospital and update_hospital functions handle the registration and updating of hospital details both off-chain (in the MySQL database) and on-chain (via the Algorand smart contract).
3. Interaction:
   - The algosdk library is used to interact with the Algorand blockchain, sending transactions to the smart contract.

5. Conclusion

In summary, an encrypted Blockchain-based approach to acquiring and storing EHRs provides a private, safe, and compatible means of handling patient health records. Healthcare stakeholders can guarantee the privacy, accuracy, and availability of private medical data by utilizing blockchain technology, which will ultimately enhance patient outcomes and healthcare provision. To fully utilize blockchain in healthcare, tackling issues like scalability, regulatory compliance, and user adoption is imperative. The use of blockchain in EHR management has the potential to transform healthcare systems around the globe and, in the end, enhance patient outcomes and treatment quality despite possible obstacles, including scalability and regulatory compliance.

Our suggested framework takes use of the Algorand blockchain, which facilitates easier system operation and comprehension for physicians and patients. Transactions in Algorand store data and the note field allows for the addition of new data. Data management and archiving can also be done with smart contracts as part of their state. Data is redundantly stored throughout the decentralized network and becomes unchangeable once it is registered on the blockchain, offering a safe, dependable, and scalable solution for data management and storage.

We shall talk about this framework's performance in the future based on predetermined characteristics including scalability, average latency, average throughput, and user count. Additionally, any potential improvements will also be examined. With any luck, this will address the blockchain's trilemma as well as other issues and concerns.

References

[1] N. Moosavi, H. Taherdoost, N. Mohamed, et al., "Blockchain Technology, Structure, and Applications: A Survey," *Procedia Comput. Sci.*, vol. 237, pp. 645–658 (2024).

[2] G. Tripathi, M. A. Ahad, and G. Casalino, "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges," *Decis. Anal. J.*, vol. 9, p. 100344, Dec. (2023).

[3] S. G. S. Yadav, L. Gunisetti, S. B. Koduri, T. Scaria, A. Dixit, and S. Lokesh, "Securing electronic health records using blockchain technology for IoT in healthcare domain," *Soft Comput.*, Jun. (2023).

[4] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *Int. J. Intell. Netw.*, vol. 2, pp. 130–139 (2021).

[5] J. A. Jaoude and R. Saade, "Business Applications of Blockchain Technology – A Systematic Review," *IEEE Access* (2019).

[6] "Jaoude and Saade Business Applications of Blockchain Technology – A.pdf (2019).

[7] Han Wang, "The Application of Blockchain to Electronic Health Record Systems:A Review ," *International Conference on Information Technology and Biomedical Engineering (ICITBE)*, Nanchang, China, pp. 397-401 (2021).

[8] Digital Transformation in Healthcare Market Size Report (2032).

[9] L. A. Linn and M. B. Koo, "Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research" (2016).

[10] A. Tandon, "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda," *Comput. Ind.* (2020).

[11] U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," *J. Ambient Intell. Humaniz. Comput.*, vol. 13, no. 1, pp. 693–703, Jan. (2022).

[12] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Comput. Secur.*, vol. 97, p. 101966, Oct. (2020).

[13] A. J, D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions," *J. Netw. Comput. Appl.*, vol. 215, p. 103633, Jun. (2023).

[14] T. L. Tan, I. Salam, and M. Singh, "Blockchain-based healthcare management system with two-side verifiability," *PLOS ONE*, vol. 17, no. 4, p. e0266916, Apr. (2022).

[15] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, "Blockchain technology in the healthcare industry: Trends and opportunities," *J. Ind. Inf. Integr.*, vol. 22, p. 100217, Jun. (2021).

[16] S. S. Kushwaha, S. Joshi, and A. K. Gupta, "An efficient approach to secure smart contract of Ethereum blockchain using hybrid security analysis approach," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 5, pp. 1499–1517 (2023).

[17] A. S. Abdulbaqi, I. F. Muslim, A. A. A. Al-Ameer, and A. J. Obaid, "Healthcare surveillance based on cloud computing utilizing mobile devices," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 4, pp. 1189–1196 (2023).

[18] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and cryptocurrency technologies: a comprehensive introduction" Princeton University Press (2016).

[19] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System".

[20] R. Manoj and S. Joshi, "Ensuring wallet application security by resolving reentrancy attacks in blockchain smart contracts," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 3, pp. 927–937 (2023).

[21] Srivastava et al., "Analyzing the Prospects of Blockchain in Healthcar. pdf," (2022)

[22] A. Shahnaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," *IEEE Access*, vol. 7, pp. 147782–147795 (2019).

[23] S. Shamshad, Minahil, K. Mahmood, S. Kumari, and C.-M. Chen, "A secure blockchain-based e-health records storage and sharing scheme," *J. Inf. Secur. Appl.*, vol. 55, p. 102590, Dec. (2020).

[24] F. I. Anik, N. Sakib, H. Shahriar, Y. Xie, H. A. Nahiyan, and S. I. Ahamed, "Unraveling a blockchain-based framework towards patient empowerment: A scoping review envisioning future smart health technologies," *Smart Health*, vol. 29, p. 100401, Sep (2023).

[25] B. Bornelus, H. Chi, and G. A. Francia, "Integrating Blockchain Technology in Healthcare via Active Learning," in *Proceedings of the 2020 ACM Southeast Conference, Tampa FL USA: ACM*, 2020, pp. 122–126, Apr (2020).

[26] Z. Zheng *et al.*, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. (2020).

[27] M. Conti, A. Gangwal, and M. Todero, "Blockchain Trilemma Solver Algorand has Dilemma over Undecidable Messages," Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury CA United Kingdom: ACM, pp. 1–8, Aug. (2019).

[28] E. A. Abdullah, A. A. Shamiri, and A. A. G. Al-Khulaidi, "Encrypting the Electronic Health Record using the Cloud Computing and Blockchain Technologies," *Int. J. Intell. Syst. Appl. Eng.*

[29] H. Saeed *et al.*, "Blockchain technology in healthcare: A systematic review," *PLOS ONE*, vol. 17, no. 4, p. e0266462, Apr. (2022).

[30] K. Shuaib, J. Abdella, F. Sallabi, and M. A. Serhani, "Secure decentralized electronic health records sharing system based on blockchains," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5045–5058, Sep. (2022).

[31] Y. Y. Zhao, W. Z. Li, T. Gao, X. Y. Deng, Z. Q. Hai, and X. Zhao, "A Multi-Layered Block Chain Network for Individual-Oriented Health-Care Records Storage and Management," Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, Xi'an China: ACM, pp. 64–69, Dec. (2019).

[32] L. J. Ramirez Lopez, P. A. Buitrago Pineda, J. M. Perez Rincon, and W. M. Rojas Reales, "A systematic review on Blockchain in electronic prescriptions and electronic medical records using PRISMA methodology in databases.," *Inform. Med. Unlocked*, p. 101525, May (2024).

[33] S. Xuan, H. Tang, W. Wang, and W. Yang, "Application of Block Chain Technology in Constructing Network Threat Intelligence System," in Proceedings of the 2020 2nd International Conference on Blockchain Technology, Hilo HI USA: ACM, pp. 144–149, Mar. (2020).

[34] N. Poonguzhali, S. Gayathri, A. Deebika, and R. Suriapriya, "A Framework For Electronic Health Record Using Blockchain Technology," *International Conference on System, Computation, Automation and Networking (ICSCAN)*, Pondicherry, India, pp. 1–5, Jul (2020).

[35] K. Riahi, M.-A. Brahmia, A. Abouaissa, and L. Idoumghar, "Multi-Task Learning for PBFT Optimisation in permissioned Blockchains," *Blockchain Res. Appl.*, p. 100206, May (2024).

[36] H. Qin, Y. Cheng, X. Ma, F. Li, and J. Abawajy, "Weighted Byzantine Fault Tolerance consensus algorithm for enhancing consortium blockchain efficiency and security," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8370–8379, Nov. (2022).

[37] M. Marcozzi and L. Mostarda, "Analytical model for performability evaluation of Practical Byzantine Fault-Tolerant systems," *Expert Syst. Appl.*, vol. 238, p. 121838, Mar. (2024).

[38] M. Kuliha and S. Verma, "Secure internet of medical things based electronic health records scheme in trust decentralized loop federated learning consensus blockchain," *Int. J. Intell. Netw.*, vol. 5, pp. 161–174 (2024).

[39] G. D'Alconzo, A. Meneghetti, and P. Piasenti, "Security issues of CFS-like digital signature algorithms," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 1, pp. 175–187 (2024).

Received March, 2024