Available online at www.dergipark.org.tr/en

INTERNATIONAL ADVANCED RESEARCHES
and
ENGINEERING JOURNAL

Journal homepage: www.dergipark.org.tr/en/pub/iarej

e-ISSN: 2618-575X

International Open Access

Volume 05
Issue 02

August, 2021

Review Article

A survey: blockchain utilization for securing healthcare system

Elnaz Dadvar [a,*] ***and Kubra Kalkan*** [a]

[a]*Ozyegin University, Faculty of Engineering, Computer Science Department, Istanbul 34794, Turkey*

ARTICLE INFO

Article history:
Received 13 October 2020
Revised 19 March 2021
Accepted 23 May 2021

Keywords:
Blockchain Technology
Healthcare System
IoMT
Privacy
Security

ABSTRACT

Nowadays healthcare systems have started to be integrated with Internet of Things (IoT) in order to deliver some benefits in diagnosis and treatment process, such as remote patient monitoring and data usage for analytics and fast treatment. With the rise of IoT healthcare devices, number of electronic health records are increased to a rate that it is estimated to exceed billions in the next few years. Although cloud computing is a practical solution for processing this kind of data, healthcare records contain confidential and sensitive patient data which makes this system very vulnerable to the security and privacy threats, so it needs more investigation. For making this critical information more secure, researchers have come up with a solution of applying blockchain technology in healthcare. In this paper, we review the latest literature of blockchain application in healthcare from the security and privacy perspective. Several existing works have been discussed and a comparative study is done among the published works, along with potential future perspectives.

1. Introduction

Healthcare has a vital role in today's society, because it is concerned with improving the quality of life. Traditionally, healthcare information recording was paper based, which was prone to alteration and missing, it was also hard and time taking to access data when required. Researchers came up with the idea of digitizing the medical data and integrating it with IoT, to perform the tasks that may lead to serious breakthrough in healthcare, including (1) automated healthcare record system; (2) sharing reliable information between trusted parties; (3) analysing big data; and (4) collaboration in clinical practice and diagnosis [1]. However, along with these advancements a lot of security and privacy challenges have been risen. For example, there is storage limitation in databases for this huge and ever-growing amount of data which are also exposed to cyberattacks. Patient's sensitive data may be accessed by attackers which then can be altered or utilized to the detriment of the patient. So, it is not reliable to utilize a centralized database system, because chance of cyberattacks is rising in a centralized system. This is where a peer-to-peer (P2P) network comes in handy to enable the decentralization feature [2]. Therefore, blockchain technology has risen as a practical solution and transparent mechanism for storing and distributing the data with the potentiality of dealing with data security, privacy, and integrity issues in medical healthcare, such as tampering and data leakage threats [3]. Blockchain technology provides a distributed, immutable, and secure system for all transactions. it can revolutionize medical database interoperability. Overall blockchain technology has the potential to dramatically improve medical care [4]. This distributed ledger technology can guarantee reliability by itself. And if we utilize this technology together with cloud computing, storage issues can be solved, because cloud is known for being trustworthy for data storage and processing. Rehman et al. [5] has employed a secure mechanism for providing services in IoT devices which preserves the security of edge servers of these devices with the contribution of smart contracts. Based on a study done at [6], blockchain is also proved to be a practical tool for improving the security issues of cloud computing environment.

Some literature review articles are proposed in recent

* Corresponding author. Tel.: +90-216-564-9150.
E-mail addresses: : elnaz.dadvar@ozu.edu.tr (E. Dadvar) , kubra.kalkan@ozyegin.edu.tr (K. Kalkan)
ORCID: 0000-0003-0092-8901 (E. Dadvar), 0000-0003-1918-8587 (K. Kalkan)
DOI: 10.35860/iarej.809797

years. They covered blockchain technology application in healthcare domain comprehensively [7-9]. As compared to these studies and other available state-of-the-art comprehensive surveys in this area, this survey focuses precisely on the security and privacy aspects of healthcare systems along with blockchain-based proposed solutions in the most recent years. This paper offers a baseline for researchers by giving a general overview of blockchain technology use case for securing different aspects of sensitive medical data management such as storing, accessing, sharing, and monitoring, while considering the privacy of users. It also offers a concise comparison between recent schemes proposed for securing healthcare systems using blockchain and identifying the gaps and limitations in the existing solutions. We have also proposed a new prototype for a potential future research direction.

The study initially starts by giving a brief background of blockchain technology and its characteristics, then we will discuss how blockchain can contribute to the medical system for solving potential security and privacy issues in healthcare systems. Afterwards, we will propose a new prototype and discuss around it. And finally, we conclude this review by comparing and discussing the related studies of blockchain application in healthcare and provide a perspective for future study directions.

2. Blockchain Background

Blockchain technology originally has been introduced as an infrastructure for cryptocurrencies in 2008 [10]. This technology's infrastructure is a peer-to-peer network [11]. Blockchain is a decentralized and distributed ledger which is shared among different parties in a system that records transactions. The main features of this technology are decentralization, reliability, and immutability, which are required for managing medical records [12]. The framework of blockchain technology is distributed in which we have a real-time sharing of captured data among trusted parties. In all transactions, each block holds a timestamp, transaction data, and a hash value as a pointer to the previous block [13]. Another characteristic of blockchain is transparency which makes the system autonomous and eliminates the need for any intermediary or third-party [14]. In blockchain, when a node receives the message it checks for accuracy of the message, if it is confirmed it will be stored in a separate block, then the consensus algorithm is applied for confirming the stored data in blocks; this action is called "Proof-of-work (PoW)". When the algorithm is finalized a new block joins into the chain. This process continues until it gets all network node's admission on the chain. Blockchain is a decentralized framework that applies strong and different encryption algorithms to store digital data in a transparent, secure, and anonymous way [15].

Blockchain has been introduced initially for the financial sector, however, researchers have embedded it with other technologies, so that it can be utilized in different fields. One of the useful and emerging integrations is the utilization of blockchain along with IoT and cloud computing which makes the best fit for solving healthcare security problems.

2.1. Compatible Characteristics of Blockchain For Healthcare System

In this section we provided important characteristics of blockchain that makes it suitable for healthcare system [1]:

- Decentralized: This is the main feature of blockchain that gives the system the opportunity to give open access control to anybody associated with the network. Due to this feature there is no single point of failure in blockchain, this means if a node fails then other nodes are able to continue accessing their data
- Immutable: When records are stored in blockchain they cannot be modified or deleted subsequently without having the admission of more than 51% of the system users.
- Secure: In blockchain encryption algorithms are utilized to encrypt data in order to give data access only to the authorized participants. Also, data integrity is satisfied from the very beginning process until the end.
- Autonomous: Every block can act independently; means they can alter their own data securely and safely. The execution of distributed transactions are done automatically under user-defined conditions.
- Anonymous: When data transferring takes place between nodes the identity of nodes remains anonymous which makes system more reliable.
- Synchronized: All nodes in blockchain have the same chance of accessing exactly the same data at the same time.

2.2. Blockchain Types

Basically, blockchain is divided into two types: private and public. However, we have some other variations too, such as consortium and hybrid blockchains. Based on every system's requirement each one of these can be selected, but they all have some features in common, and that is each blockchain operates on a P2P network and has a cluster of nodes in which each node keeps a copy of the shared ledger and updates it promptly. Nodes has the capability to verify transactions, initiate or receive any process in the system independently [16]. Some detailed explanation of blockchain types are discussed as follows [11].

1. Public Blockchain: This is a permission-less distributed ledger system. That means anyone can join the network and be an authorized node in the system. Public blockchains are secure only if the clients follow the

security conventions. Examples of this type of blockchain are: Bitcoin (BTC) and Ethereum (ETH).

2. Private Blockchain: This type of blockchain is also called permissioned blockchain which operates only in a closed network. Private blockchain's usage is very similar to public blockchain, but its network is much smaller and restrictive. Examples of this type of blockchain are: Ripple (XRP), Multichain and Hyperledger (Fabric, Sawtooth), Corda, etc.

3. Consortium Blockchain: Consortium blockchain has semi-decentralized framework. In contrast to private blockchain, here there is more than one organization managing the network. And each one can act as an independent node. Examples of consortium blockchain can be: Quorum, Energy Web Foundation, R3, etc.

4. Hybrid Blockchain: This blockchain is created by merging private and public blockchain. It also integrates the features of both types of blockchains in a way that user can have both a private permission-based system along with a public permission-less system. Employing this network helps users to have control over who gets access to which data in the blockchain. Only partial data is allowed to be publicly available, but the rest of records are kept confidential using the private network. So, this type of blockchain can communicate with outer world easily while preserving network's privacy. Hybrid blockchain has gained a vast usage domain, Dragonchain can be a good example of a hybrid blockchain.

Each of these blockchain technologies can be utilized based on the system requirements. Most of the research studies on applying blockchain in the healthcare domain have primarily focused on utilizing permissionless Ethereum blockchain technology, but this type of blockchain has some downsides such that it consumes heavy energy, it is very restricted in scalability, and the network throughput is very low. For fulfilling these gaps there is a crucial need for a much scalable, fault-tolerant, timely managed, secure, and private blockchain to meet the demands of the healthcare systems. Based on the researches done so far, a permissioned blockchain has proved to be more compatible for healthcare data management with the results of reducing the computational overhead and so lowering energy consumption, by meeting the security and privacy factors much efficiently in compared with Ethereum blockchain.

3. How Blockchain Meets Healthcare Requirements

Blockchain provides a 'secure by design' approach in which security is considered the primary factor of the architecture. Blockchain satisfies required security, and by integrating with other supporting solutions it opens up other complexities of the system. The reference architecture applied to healthcare system is as follows: The user of blockchain syncs up with other nodes in the network. Then a particular server manages the transaction records. Data integrity and provenance is fulfilled by applying cryptographical algorithms. The massive scale of operation of blockchain software makes it almost impossible to break into the framework or other applications which are running on it. Hence, there is no need for a central third party to issue, authenticate and validate ownership of the data. When there is two or more nodes possessing same blocks in their own databases, we can consider them to be in consensus. So, according to the blockchain features and applications it can feasibly meet the healthcare requirements such as security, interoperability, data access and data sharing. For better understanding, we designed a general flowchart for a potential blockchain-based healthcare system, Figure 1. It shows all technical and functional platforms of the architecture for applying blockchain in healthcare. This platform consists of four main layers, the very first layer is public network, which includes user interface applications that are utilized to collect user data. In the second layer cloud network, the gathered data from patients or doctors are first encrypted and then pushed to the cloud for secure storing. All data are hashed before transferring in order to avoid data leakage during transferring process to the blockchain service. In blockchain service layer there is a consensus algorithm which helps at reaching to a common agreement between all participated nodes of the network by approving the transactions. There are multiple methods of reaching consensus; the frequently used ones are proof of work, proof of stake and multisignature schemes. A shared ledger in this layer holds approved and authenticated transactions and distributes data among other confirmed members, thus user's privacy is guaranteed. In this layer smart contract holds and executes the coded agreements of blockchain network. During these processes data security are assured by applying cryptographic algorithms. Ultimately, communication between blockchain and enterprise network layer is accomplished using an appropriate API.

4. Comparison of Related Studies

As we mentioned before, healthcare data is very sensitive, and it is crucial to protect them in means of privacy and security. So, for processing, sharing, storing and handling medical information a secure platform should be designed [17]. Blockchain technology has been proposed and explained by several research studies in recent years for dealing with security and privacy risks, due to its potential to promote better data sharing and management and its assistance in treatment process.

Azaria et al. [18] have proposed MedRec as a novel system which utilizes blockchain for managing large medical data.

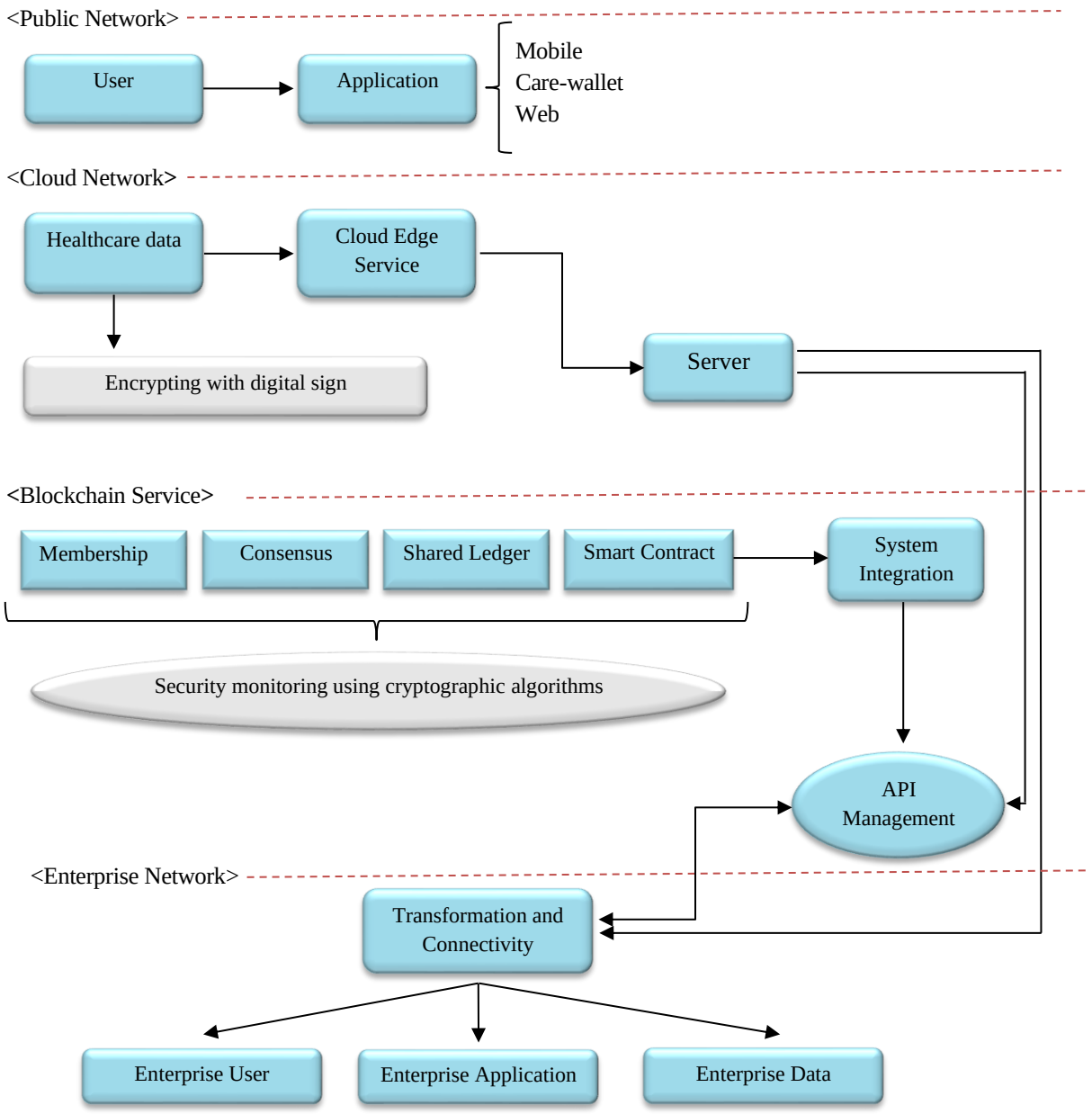

Figure 1. Blockchain-based healthcare system flowchart

It provides easy access to data and feasible patient data sharing. Theodouli et al. [19] has facilitated a Healthcare system that enables sharing data in a private and auditable manner by considering patient pseudonymity and hiding the identity of the user whose data is shared. A 3-layered architecture is also proposed for respectively storing patient's data in a web or cloud platform. In this architecture there is a cloud middleware layer which its task is data fetching from the cloud layer to the next layer, which is blockchain network, by utilizing an API and interacting with smart contracts. A smart contract is a self-executing protocol which is coded and executed inside of a blockchain and it contains terms and conditions of an agreement between peers. It also consists of rules that helps to keep medical data secure in a way that the data is accessible only to the authorized person by digital signature [20]. The Ethereum platform is utilized for executing smart contracts. Liu et al. [21] has improved security and privacy related issues in biomedical systems by designing a blockchain and distributed ledger based secure scheme. Authors have proved that this system is capable of maximizing the data sharing ratio while minimizing the computation and response time by ensuring the privacy of users.

Zhang et al. [22] has proved that smart contract can be a potential solution to tackle the challenges of interoperability in healthcare, so that medical data are shared and communicated in a secure way. Ethereum smart contracts is also being used in [23], to design a MedRec prototype which is a proof-of-concept system, and to manage the access to healthcare records. Researchers in [24], have applied smart contract in their unique architecture, which is independent of

any previously designed blockchain platforms, in this system they could guarantee the integrity in the records of EHR systems, and they enhanced the interoperability of the system. Smart contracts are considered to be dynamic in nature, so they are best fit to be employed in designing access control policies for example, authors in [25], proposed an Enhanced Bell–LaPadula model to classify the healthcare data and access control policies and so implement a scalable and secure healthcare network. Some hybrid methods are recently proposed by researchers in which they combine the power of blockchain technology with other existing technologies to fulfil the security and privacy gaps of healthcare system. Chakraborty et al. [26] has utilized Blockchain technology along with machine learning to provide a secure framework in order to store and maintain patient's data such as providing accurate and authentic health records. In this system machine learning is applied to detect any anomality in the newly generated data of patients. De Oliverira et al. [27] provides an approach for a private and scalable EMR storage by the incorporation of Public Key Infrastructure (PKI) with blockchain technology. Zhao et al. [28] developed a key management scheme for healthcare blockchain to enhance security and privacy in healthcare system. They integrated Body Sensor Network (BSN) with health blockchain and created an efficient recovery strategy for managing the keys. Another study related to key management by blockchain is done recently in [29], researchers designed a new sharing scheme based on blockchain for privacy protection and enhancing access control management process through symmetric and attribute-based encryption. Healthcare data are dynamic, and they are changing constantly and there should be a system that can adopt to the metadata alteration efficiently. Shen et al. [30] proposed a scheme called MedChain that integrates blockchain, digest chain and P2P network aspects to provide an efficient system for data sharing in healthcare. Xia et al. [31] has also utilized blockchain to propose a framework for sensitive medical data sharing which is stored in cloud. The blockchain type used in this system is permissioned blockchain that gives access only to the verified users. Putting encrypted medical data into blockchain is first proposed by [32], an App was also designed to this purpose. Researchers in [33], have proposed the requirements along with their potential solution for having an efficient healthcare system with combining blockchain and cryptographic algorithms. And the details for applied cryptographic techniques are discussed at [34]. For example, ARX Symmetric Encryption Algorithm has been applied in order to have an efficient encryption of the sensitive data of blockchain. Digital Signature is used in authentication process and for keeping the users anonymous and protecting the privacy of users Digital Ring Signature is applied. A three-layered architecture is proposed in [35], for ensuring a private and secure data management in healthcare IoT devices. The layers include Sensing, NEAR processing, and FAR processing layer. Sensing layer is for patient data acquisition and transmitting to IoT devices. NEAR processing layer is used for sensing the IoT devices, and FAR processing layer includes servers for cloud and high computations. Digital Ring Signature and SSS is applied in this system to fulfil security requirements in healthcare agent's communication process. Authors of [36], set up a shared key for providing a private access to medical data to be used in the process of diagnosis and treatment. This shared key is created using sibling intractable function families (SIFF). The key is utilized for encrypting and storing data in a blockchain for protecting data. The evaluation of proposed system proves to have a good efficiency in aspects of integrity, availability, and privacy of medical data. In a most recent study [37], a Multi-Modal Secure Data Dissemination Framework is proposed for data access control management in IoMT devices. In this scheme data is encrypted in blockchain and decrypted only by private key of patient. By employing blockchain in this framework security and privacy is enhanced significantly compared to previously proposed methods. Due to the ever-growing amount of medical data in the world, security and privacy issues of health data have become a major research topic for academicians and security engineers. Figure 2. depicts the global picture of security related research areas. Proposals in the literature can be classified mostly in the concept of data sharing and access management in a secure manner. In Table A.1 (in Appendix). we carried out a detailed summary of the current blockchain-based healthcare systems proposed by researchers so far along with their contribution and gaps to form a point of comparison between methods.

5. A New Prototype For Enhancing The Security of Healthcare In Emergency Condition

In the conventional healthcare systems for any medical process patient authorizes access to the healthcare records, in other words most of the proposed systems have implemented to be patient-centric in data sharing and accessing in order to keep data private and secure. But these systems may act poorly in emergency cases. When the patient loses his/her consciousness, its hard and almost impossible to be able to issue any access authorization or share health related data with a medical service provider which may lead to a delay in diagnosis and treatment process and put a patient's life in danger. We have proposed a prototype for handling this issue. In this prototype we classified system users into three categories based on their access level permissions to patient's sensitive health data. The main focus lies on generating a group of trusted parties and transferring the personal medical data's partial- ownership to these parties in emergency cases, these parties may be a healthcare provider, family member or another trusted party which is pre-specified by the real data owner.

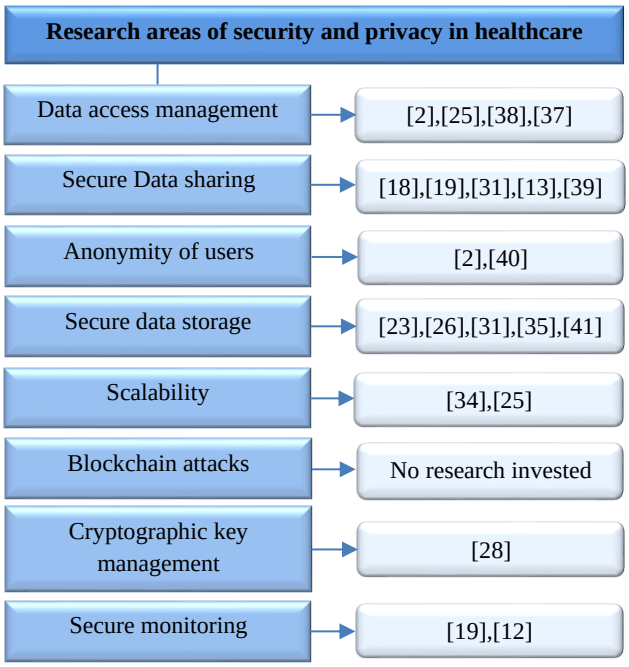

Figure 2. Classification of Security in healthcare studies

If the trusted party is a related medical service provider, diagnosis and treatment process takes place, if not the case they will authorize the access and share only required data with a third-level party which may be EMT staff or agencies. A potential architecture for our proposed prototype is provided in Figure 3. As it is observed in this figure, the user who can be the patient, doctors, nurses, health organizations or emergency staff makes data request in emergency condition, this request then would be validated through edge service and be sent to the transaction manager. The pre-defined policies in smart contract along with identity access management will be processed in order to make the authorization and accept or reject the request, then the status of the request (accept/reject) would be sent to the requester user and the partial access to the data would be issued. For our future research direction, we are planning to apply this system on a private blockchain, Hyperledger platform to form a feasible protocol for emergency access authorization while considering patient's privacy and data security.

6. Discussion and Future Perspectives

- A fundamental concern in modern healthcare systems, such as Electronic Medical Record (EMR) systems is patient's data security and privacy. In health systems data storing process should be done securely and keep the system safe from unauthorized users. These issues are addressed using different cryptographic algorithms along with adopting blockchain technology to the system. For example [18], have utilized blockchain for managing the medical data access, but they have not investigated enough on the database security.
- Scalability can be a critical issue in EMR systems. Because of the growing number of patients, the data is increasing exponentially, so we need a scalable system that can be adopted to this increasing rate which existing works have not investigated enough in this area.
- One research challenge that needs more investigation can be cryptographic key management and replacement in case of any loss or change.
- Research study on the specific blockchain attacks that can affect whole functionality of the system, have not been investigated.
- Research is needed to focus on authorization issue. The proposed systems so far have given the data access permission confirmation only to patients, in other words the access process is patient centric. But they have not considered the likelihood of emergency cases. So, there should be some protocols for emergency cases that allows authorized doctors to have access to the data.
- The studies done so far in this area are mostly a proof-of-concept research. So, one of the main research gaps that can be seen in the published papers used in this review study is the lack of implementation and experiment on real-world healthcare data so that the proposed solutions and systems can be evaluated for real.

Overall, implementing blockchain technology needs a decent framework along with experts. These might be considered as technical barriers to achieving success in the healthcare industry.

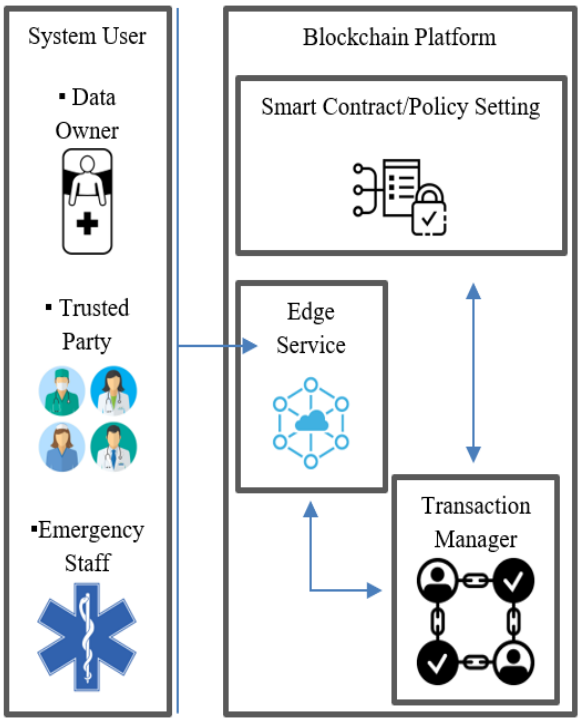

Figure 3. Architecture of proposed prototype for PHR access in emergency condition using blockchain

6. Conclusion

Healthcare has been a crucial part of human life and so the medical data. These data include the personal details of the patient's health condition, so it should not be shared with third parties to protect from being misused. This is where blockchain technology is proposed to deal with security and privacy issues. Blockchain has made a huge contribution to the healthcare handling many difficulties such as providing secure and efficient data storing, sharing, and accessing and also data integrity is fully satisfied. Blockchain technology is now setting new standards for patient care.

In this study, a general and clear classification is provided about the global research studies related to securing healthcare systems. We also reviewed current researches done on maintaining health data and how blockchain can affect and empower patients in controlling the sharing process of their personal health data. A consensus has been observed among most papers that blockchain will help in authentication process and the data will be exclusively managed by patient. In this paper we carried out a literature study and reviewed all possible works on the medical healthcare using blockchain technology with a comparative study. We proposed a new prototype for improving the privacy and security of patients in emergency conditions of healthcare, we also covered major research initiatives and future research opportunities. Some major issues are still open, like mining incentives and specific blockchain attacks, which form the core mechanism of a blockchain have not been fully investigated in these studies, whereas these problems can break the entire system.

Blockchain technology is an emerging technology, and its utilization in healthcare system is started to be investigated from 2016 up to now. However, initial studies in this area only defined general terms and then moved to the proof-of-concept phase. Most recently initial experiments have been started in a testable system for applying blockchain for patient data sharing and patient monitoring system to provide some real work security guarantee. Nevertheless, there are still many open challenges in this area that demand further and precise investigation.

Declaration

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article. The authors also declared that this article is original, was prepared in accordance with international publication and research ethics, and ethical committee permission or any special permission is not required. The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author Contributions

E. Dadvar: conceptualization, methodology, writing the original draft, visualization, investigation, writing - review and editing. K. Kalkan: conceptualization, methodology, visualization, supervision, investigation, writing - review and editing.

References

1. Roman-Belmonte, J. M., H. De la Corte-Rodriguez, and E. C. Rodriguez-Merchan, *How blockchain technology can change medicine.* Postgraduate medicine, 2018. **130**(4), p. 420-427.
2. Al Omar, A., M. S. Rahman, A. Basu, and S. Kiyomoto, *Medibchain: A blockchain based privacy preserving platform for healthcare data.* International conference on security, privacy and anonymity in computation, communication, and storage. Springer, Cham, 2017. Volume 10658, pp. 534–543.
3. Yaeger, K., M. Martini, J. Rasouli, and A. Costa, *Emerging blockchain technology solutions for modern healthcare infrastructure.* Journal of Scientific Innovation in Medicine, 2019. **2**(1):1.
4. Heston, T.F., *Why Blockchain Technology Is Important for Healthcare Professionals.* SSRN Electronic Journal, 2017. SSRN 3006389. pp. 1-4.
5. Rehman, M., N. Javai, M. Awais, M. Imran, and N. Naseer, *Cloud based Secure Service Providing for IoTs using Blockchain.* IEEE Global Communications Conference (GLOBECOM), 2019. pp. 1-7.
6. Gupta, A., S.T. Siddiqui, S. Alam, and M. Shuaib, *Cloud Computing Security using Blockchain.* J. Emerging Technol. Innovative Res., 2019. **6**(6): p. 791-794
7. Soltanisehat, L., R. Alizadeh, H. Hao, and K. K. R. Choo, *Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review.* IEEE Transactions on Engineering Management, 2020. p. 0018-9391
8. Khezr, S., M. Moniruzzaman, A. Yassine, and R. Benlamri, *Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research.* Applied sciences, 2019. **9**(9): p. 1736.
9. Zubaydi, H. D., Y.W. Chong, K. Ko, S. M. Hanshi, and S. Karuppayah, *A review on the role of blockchain technology in the healthcare domain.* Electronics, 2019. **8**(6): p. 679.
10. Nakamoto S., *Bitcoin: A peer-to-peer electronic cash system.* Available from: http://bitcoin.org/bitcoin.pdf, 2009.
11. Hölbl, M., M. Kompara, A. Kamišalić, and L. N. Zlatolas, *A systematic review of the use of blockchain in healthcare*. Symmetry, 2018. **10**(10): p. 470.
12. Griggs, K. N., O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, *Healthcare blockchain system using smart contracts for secure automated remote patient monitoring.* Journal of medical systems, 2018. **42**(7): p.130.
13. Zhang, A., and X. Lin, *Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain.* Journal of medical systems, 2018. **42**(8): p.140.
14. Rennock, M., A. Cohn, and J. R. Butcher, *Blockchain technology and regulatory investigations.* Practical Law Litigation, 2018. pp. 35-44.
15. Lin, I. C., and T. C. Liao, *A survey of blockchain security issues and challenges.* IJ Network Security, 2017. **19**(5): p. 653-659.
16. Zheng, Z., S, Xie, H. N. Dai, X. Chen, and H. Wang, *Blockchain challenges and opportunities: A survey.* International Journal of Web and Grid Services, 2018. **14**(4): p. 352-375.

17. Puppala, M., T. He, X. Yu, S. Chen, R. Ogunti, and S. T. Wong, *Data security and privacy management in healthcare applications and clinical data warehouse environment.* IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI), 2016. pp. 5-8.
18. Azaria, A., A. Ekblaw, T. Vieira, and A. Lippman, *Medrec: Using blockchain for medical data access and permission management.* 2nd International Conference on Open and Big Data (OBD), 2016. pp. 25-30.
19. Theodouli, A., S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, *On the design of a Blockchain-based system to facilitate Healthcare Data Sharing.* IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom/BigDataSE), 2018. pp. 1374-1379.
20. Wohrer, M., and U. Zdun, S*mart contracts: security patterns in the ethereum ecosystem and solidity.* International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2018. pp. 2-8.
21. Liu, H., R. G. Crespo, and O. S. Martínez, *Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts.* Multidisciplinary Digital Publishing Institute, 2021. **8**(3): p. 243.
22. Zhang, P., J. White, D. C. Schmidt, and G. Lenz, *Applying Software Patterns to Address Interoperability in Blockchain-Based Healthcare Apps.* arXiv preprint arXiv:1706.03700, 2017.
23. Ekblaw, A., A. Azaria, J. D. Halamka, and A. Lippman, *A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data*. In Proceedings of IEEE open & big data conference, 2016. **(13)**: p. 13.
24. Yang, G., C. Li, and K. E. Marstein, *A blockchain-based architecture for securing electronic health record systems.* Concurrency and Computation: Practice and Experience, Wiley, 2019. e5479, **31**.
25. Kumar, R., and R. Tripathi, *Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model.* Journal of Ambient Intelligence and Humanized Computing, 2020. pp. 1-18.
26. Chakraborty, S., S. Aich, and H. C. Kim, *A secure healthcare system design framework using blockchain technology.* IEEE International Conference on Advanced Communication Technology (ICACT), 2019. pp. 260-264.
27. de Oliveira, M. T., L. H. Reis, R. C. Carrano, F. L. Seixas, D. C. Saade, C. V. Albuquerque, N. C. Femandes, S. D. Olabarriaga, D. S.V. Medeiros, and D. M. F. Mattos, *Towards a blockchain-based secure electronic medical record for healthcare applications.* IEEE International Conference on Communications (ICC), 2019. pp. 1-6.
28. Zhao, H., P. Bai, Y. Peng, and R. Xu, *Efficient key management scheme for health blockchain.* CAAI Transactions on Intelligence Technology, 2018. **3**(2): p. 114-118.
29. Wang, S., D. Zhang, and Y. Zhang, *Blockchain-based personal health records sharing scheme with data integrity verifiable.* IEEE Access, 2018. **7**: p. 102887-102901.
30. Shen, B., J. Guo, and Y. Yang, *MedChain: Efficient healthcare data sharing via blockchain.* Applied sciences, 2019. **9**(6): p. 1207.
31. Xia, Q., E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, *BBDS: Blockchain-based data sharing for electronic medical records in cloud environments.* Information, 2017. **8**(2): p. 44.
32. Yue, X., H. Wang, D. Jin, M. Li, and W. Jiang, *Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control.* Journal of medical systems, 2016. **40**(10): p. 1-8.
33. Srivastava, G., J. Crichigno, and S. Dhar, *A light and secure healthcare blockchain for iot medical devices.* IEEE Canadian conference of electrical and computer engineering (CCECE), 2019. pp. 1-5.
34. Dwivedi, A. D., G. Srivastava, S. Dhar, and R. Singh, *A decentralized privacy-preserving healthcare blockchain for IoT.* Sensors, 2019. **19**(2): p. 326.
35. Uddin, M. A., A. Stranieri, I. Gondal, and V. Balasubramanian, *Blockchain leveraged decentralized iot ehealth framework.* Internet of Things, 2020. **9**: p. 100159.
36. Tian, H., J. He, and Y. Ding, Medical data management on blockchain with privacy. Journal of medical systems, 2019. **43**(2): p. 26.
37. Arul, R., Y. D. Al-Otaibi, W. S. Alnumay, U. Tariq, U. Shoaib, and M. J. Piran, *Multi-modal secure healthcare data dissemination framework using blockchain in IoMT.* Personal and Ubiquitous Computing, 2021. pp. 1-13.
38. Chakraborty, S., S. Aich, and H. C. Kim, *A secure healthcare system design framework using blockchain technology.* International Conference on Advanced Communication Technology (ICACT), 2019. pp. 260-264.
39. Fan, K., S. Wang, Y. Ren, H. Li, and Y. Yang, *Medblock: Efficient and secure medical data sharing via blockchain.* Journal of medical systems, 2018. **42**(8): p. 136.
40. Li, H., L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, *Blockchain-based data preservation system for medical data.* Journal of medical systems, 2018. **42(**8): p. 141.
41. Kaur, H., M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, *A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment.* Journal of medical systems, 2018. **42**(8): p. 156.
42. Ismail, L., H. Materwala, and S. Zeadally, *Lightweight blockchain for healthcare.* IEEE Access 7, 2019. P. 149935-149951.

Appendix

Table A.1. Comparison of the current studies on blockchain-based healthcare system security and privacy

Reference Article	Concept	Secured Information data type	Use Case In Healthcare	Blockchain Type	Contribution	Gaps
[12]	Smart contracts for secure remote patient monitoring	PHI	Managing medical sensors	▪Permissioned blockchain ▪ Public Ethereum blockchain	Patient's data validation using PBFT consensus mechanism	▪ Lack of verification step in consensus mechanism ▪ Inefficient data
[41]	Blockchain usage in cloud environment for storing and managing the EMRs	EHR	Medical data stored in cloud	Undefined	Maintaining and storing the heterogeneous medical data in distributed form	Key generation is not addressed
[31]	Blockchain framework for sharing data of EMRs system in cloud environment	EMR	Shares medical data into cloud for secure access	Permissioned blockchain	Guaranteeing user anonymity using identity-based authentication along with key agreement protocol	Communication and authentication protocols are not fully investigated
[2]	Blockchain-based mechanism fort he privacy of health data	Healthcare data	Securing the interaction between patient and system	Permissioned blockchain	Patient-centric system for healthcare data management by ensuring pseudonymity and anonymity using cryptographic primitives	Key generation in the protocols are not fully addressed
[13]	Providing e-health system based on blockchain for secure data sharing	PHI	Diagnosis process improvements in e-health system	▪ Consortium blockchain ▪ Private blockchain	Secure sharing of PHR using cryptographic primitives for improving the diagnosis	Scalability inprivate blockchains is not addressed
[38]	Timely remote data fetching by considering the data privacy and security of patients	EMR	Real-time data delivery to medical practitioner	Consortium blockchain	Protecting the system from stakeholder's data manipulation and leakage while providing a timely mannered and secured access to data	Security and cryptographic details are not discussed
[18]	Sharing and managing medical data using blockchain	EMR	Gives patients easy access to treatment sites	Ethereum blockchain	Patient data sharing and mining Incentives is addressed	No key replacement capability, and legal issues are not addressed
[19]	Blockchain-based system for sharing the medical data	Healthcare Data	Used for data sharing between patients and medical research centers	Consortium blockchain	▪ Enables private data sharing ▪ Enhances security by access permission management	Cryptographic techniques are not discussed
[39]	Blockchain-based framework for protecting the electronic medical record while data sharing	EMR	Patients can access to different hospital EMRs through this framework	Public blockchain	Guaranteeing privacy by combining access control protocol with encryption algorithms	PBFT consensus is not fully investigated
[40]	Data preservation system for Medical Data	Medical Data Records	Storing medical data in a reliable system	Ethereum blockchain	Ensuring verifiability of stored data while protecting users' privacy	Authentication protocol is not fully investigated
[22]	Software patterns for addressing interoperability issues in healthcare apps	Medical Records	Enhancing communication between users and medical applications	Ethereum blockchain	Maximizing sharing of resources and application scalability by applying foundational software patterns	Privacy and security concerns are not investigated enough
[23]	Blockchain-based record management system for handling EHR	EHR	Provides easy data access to patients	Ethereum blockchain	Secure and interoperable medical record access system	Cryptographic techniques are not discussed
[33]	Blockchain-based security approaches for remote patient monitoring	Healthcare Data	Remote patient monitoring for diagnosis and treatment process	Undefined	Security and privacy is provided for IoT-based patient monitoring utilizing cryptographic algorithms	Cryptographic algorithms are not implemented in a testable system

[42]	Scalable and efficient blockchain architecture to meet healthcare data management issues	EHR	Managing healthcare data	Permissioned blockchain	The architecture reduces the computational and communication delay in a more scalable environment	Security and privacy performance in this architecture is not fully investigated
[21]	Enhanced blockchain and distributed ledger based secure scheme for secure data sharing	EHR	Used for maximizing the secure sharing rate along with minimizing the complexity in EHRs	Undefined	Classification-based authentication reduced the computation time and provides a secure and private data sharing	Scalablity is not addressed
[24]	A new scalable and adoptable architecture for dealing with interoperability	EHR	Recording the healthcare data while considering the integrity	Private blockchain	Guarantees the integrity of healthcare records with a multiple access system for block creation	Consensus mechanism detail is not fully investigated
[25]	Enhanced Bell–LaPadula model to classify the healthcare data and access control policies	Healthcare Data	Accessing healthcare data in a secure and private manner	Permissioned blockchain	Secure and scalable healthcare network by dynamic access control policies	No gap identified
[26]	Secure framework for storing and maintaining patient's data	PHR	Remote data fetching from patient's wearable devices and insurance companies	Consortium blockchain	Accurate and authentic health records	There may be delays in treatment process because system is patient-centric
[27]	Integrating blockchain with public key Infrastructure for maximizing privacy and security	EMR	Securing EMR's for healthcare applications	Permissioned blockchain	private and scalable EMR storage	There may be latency problem in treatment and diagnosis process
[28]	Key management scheme for healthcare blockchain	Undefined	Not specified	Undefined	Efficient encryption key backup and recovery scheme enhances security	System may not be timely mannered
[29]	Health data sharing while considering the integrity	PHR	Encrypting personal health records for secure data sharing	Ethereum blockchain	Privacy protection and sharing, enhanced access control management process through symmetric encryption and attribute-based encryption.	Interoprability is not ivestigated
[30]	Efficient and secure data sharing scheme	EHR	Secure data sharing between medical laboratories and institutions	Consortium blockchain	Integrating blockchain, digest chain and P2P network to provide an efficient system for data sharing in healthcare	Proposed system is not fully automated
[32]	Healthcare Data Gateway App for private data control by patient	Personal Electronic Medical Data	A mobile app to maintain he control and sharing process of personal electronic medical dta	Private blockchain	Access control model which enables patients to possess, and share their own data while preserving privacy	No consideration for emergency situations
[35]	Architecture for private and secure data management in IoMT devices	EHR, EMR, PHR	Storing medical data generated from IoMT devices	Ethereum blockchain	Contributing to a secure and private communication by proposing a layered architecture	High storage overhead
[36]	A shared key is proposed for protecting medical data privacy	PHR	Private medical data sharing for diagnosis and treatment process	Private blockchain	Protecting data by storing encrypted data into blockckchain	Scalablity is not addressed
[37]	Framework for access control management in IoMT devices	Healthcare Data	Managing health related data collected by IoMT devices	Private blockchain	A key-based framework for a private and secure data access	Interoprability is not investigated in details