Multimedia Tools and Applications (2023) 82:28493–28519
https://doi.org/10.1007/s11042-023-14488-w

Blockchain-based privacy and security preserving in electronic health: a systematic review

Kianoush Kiania[1] · Seyed Mahdi Jameii[2] · Amir Masoud Rahmani[3]

Received: 3 January 2022 / Revised: 9 January 2023 / Accepted: 31 January 2023 /
Published online: 17 February 2023

Abstract
In today's world, health and medicine play an undeniable role in human life. Traditional and current Electronic Health Records (EHR) systems that are used to exchange information between medical stakeholders (patients, physicians, insurance companies, pharmaceuticals, medical researchers, etc.) suffer weaknesses in terms of security and privacy due to having centralized architecture. Blockchain technology ensures the privacy and security of EHR systems thanks to the use of encryption. Moreover, due to its decentralized nature, this technology prevents central failure and central attack points. In this paper, a systematic literature review (SLR) is proposed to analyze the existing Blockchain-based approaches for improving privacy and security in electronic health systems. The research methodology, paper selection process, and the search query are explained. 51 papers returned from our search criteria published between 2018 and Dec 2022 are reviewed. The main ideas, type of Blockchain, evaluation metrics, and used tools of each selected paper are discussed in detail. Finally, future research directions, open challenges, and some issues are discussed.

Keywords Electronic Health Records (HER) · Blockchain · Security · Privacy · Smart contract · SLR

1 Introduction

Nowadays, healthcare is considered to be one of the most important human concerns. A lot of data related to healthcare are generated, stored, and reused frequently. One of the most important subsets of healthcare systems is Electronic Health Records (EHR). Electronic patient records

✉ Seyed Mahdi Jameii
sm.jameii@iau.ac.ir

[1] Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran

[2] Department of Computer Engineering, Shahr-e-Qods Branch, Islamic Azad University, Tehran, Iran

[3] Future Technology Research Center, National Yunlin University of Science and Technology, 123 University Road, Section 3, Douliou, Yunlin 64002, Taiwan

provide many opportunities for healthcare stakeholders. For example, it allows medical records to be accessed by patients and avoids expensive tests, radiology, and repetitive imaging. Moreover, even if the patient is treated in different medical centers or in hospitals located in different cities, provinces, or other countries, physicians based in all those medical centers can access the patient's records across far distances from each other using EHR. Another advantage of using EHR is having access to a history of medications used by the patient, which will help physicians in prescribing a new drug for the patient. Another advantage of using EHR is the use of patients' medical records for research purposes and finding new treatment methods.

One of the basic challenges of using EHR in healthcare is how to preserve the patient's privacy. With the wide access to patient records, the patients' privacy is an important challenge. Another challenge for EHR is that the patient does not own his/her data and instead, it is the medical centers who own the patient's data. Physicians and researchers can access a patient's EHR without his or her consent to use these data for treatment and research purposes, and this is one aspect of the patient's privacy. From a security perspective, using EHR brings up several challenges: First, the abundant use of IoT (Internet of Things) and wearable sensors to diagnose the disease and record data in the medical record of that patient can increase the risk of attacks. This could affect the physician's prescription for the disease and endanger the patient's life. The second security issue is fraud detection. There have been many cases where doctors have prescribed a drug for a patient that is not necessary for him/her just because that certain drug is available at the hospital's pharmacy or medical center where the doctor works. As a result, the patient's health may be compromised and/or the patient may be forced to bear unnecessary costs. Another security challenge is counterfeit drugs. Many people die of the use of counterfeit drugs or suffer from serious side effects from the use of these drugs. To address this challenge, a drug supply chain must be put in place in which critical information is accessible. This information must include the name of the pharmaceutical plant that has manufactured the drug, then where and how it has been stored; by what distributor it has been transported to the pharmacy, the distribution date, etc. To overcome the above-mentioned problems, Blockchain technology can be used. The distributed ledger of Blockchain has a distributable feature so it reduces the risk of an attack on an integrated center. Moreover, this distributed ledger cannot be changed and the transactions registered in it cannot be modified. In addition, only the patient can permit a third party to read or change their data by having their private key and public key. To do this systematic review, the guidelines proposed in [30, 64] were adopted and the existing Blockchain-based approaches that tried to preserve privacy and security in healthcare are reviewed. The remaining of the paper is organized as follows. In Section 2, previous review papers are discussed. Section 3 describes the methodology and criteria for selecting the papers. In Section 4, the advantages and disadvantages of using Blockchain in the field of healthcare are discussed. The existing Blockchain-based approaches that tried to improve the privacy issue in healthcare are mentioned in Section 5. The existing Blockchain-based approaches that tried to improve security issues in healthcare are described in Section 6. In Section 7, the reviewed papers are discussed and analyzed. Section 8 describes the open Issues and future research directions. Section 9 is dedicated to the conclusions and limitations of this SLR study.

2 Related work and motivation

In this section, we discuss the related survey and SLR papers that examined the Blockchain-based privacy and security approaches in healthcare.

The authors of [23] reviewed 143 papers on the role of Blockchain in healthcare and discussed the existing challenges in the EHR domain (including power consumption, failure, and attack points). Blockchain was used to solve these challenges of trustless environments and secure data exchange. In this paper two platforms were introduced: permissionless Blockchain (Ethereum) and permissioned Blockchain (Hyperledger) to solve EHR challenges. The authors reviewed the issues of privacy and security, and compared traditional EHR methods with those implemented by Blockchain. Finally, the limitations of the methods were mentioned.

In another study [55], 52 papers were reviewed. These papers discussed how Blockchain technology, along with smart contract systems, can support healthcare applications for physicians, patients, insurance companies, and assets such as patient's data, medical information, equipment, and pharmaceutical chains.

The authors of [7] reviewed 31 papers. This paper described how this technology improves healthcare and prevents diseases and suggested a new protocol to ensure patient privacy and guarantee confidential data. Secure encryption methods and digital signatures were introduced to ensure authorized access to shared information using Blockchain. Then, a strong review of the accuracy of the EHR data was presented.

The authors of [31] reviewed 69 papers. This paper discusses the role of Blockchain in healthcare. This paper addressed the challenges of system security, interoperability, data sharing, and mobility in the field of EHR and explained how Blockchain can handle these challenges. Then, the following platforms were introduced to implement Blockchain in healthcare: Gem Health Network, OmniPHR, Medrec, Inclusive Social Networking System (PSN), and Virtual Resources.

Another study [54] was a systematic literature review that reviewed 42 papers published between 2016 and 2019 related to applying Blockchain in healthcare. In this paper, some challenges such as using Blockchain in healthcare, sharing and processing medical data and patient records were analyzed. The authors examined the implementation model, limitations, and costs of using Blockchain in healthcare.

The authors of [52] conducted a systematic review of 62 papers related to Blockchain-based approaches in healthcare systems published between 2016 and 2020. In this paper, the authors reviewed the use cases, challenges, and structures of Blockchain-based approaches in healthcare. Then, the implementation methods, technical cases, and the use of Blockchain in the field of medicine were evaluated. Finally, future directions and future works in this field were discussed.

The authors of [4] studied 37 papers related to Blockchain-based approaches in healthcare published between 2017 and 2020. This paper examined how to access medical records, security, data tracking, and medical information and how to exchange information in the Blockchain healthcare network. Also in this paper, challenges such as how to register and accept transactions, how to implement interoperability, regulations, and restrictions related to medical data in the community, and issues related to scalability and management of access permissions were mentioned.

The authors of [18] reviewed 39 papers that used Blockchain in healthcare approaches published between 2018 and 2020. This paper mentioned that using Blockchain can be effective for data integration, access control, and interoperability. The authors of this paper believed that using Blockchain in healthcare systems is expanding rapidly and therefore research in this field can be absolutely vital and useful.

Another study [19] reviewed a total number of 940 papers, and books published between 2016 and 2020 that used Blockchain technology in healthcare. This paper discussed telecare and the role of security and privacy. In this paper, some issues of using Blockchain in healthcare such as interoperability, scalability, and storage were discussed.

In another study [24], 50 papers published on reputable scientific sites between 2015 and 2020 that used Blockchain in healthcare were analyzed. This paper highlighted the role of quality criteria. First, new trends of using Blockchain in healthcare were introduced, then these new trends were analyzed, and finally, the challenges of using these new trends were discussed. This paper also discussed issues such as integrating cloud computing technology and Blockchain in healthcare.

The authors of [46] reviewed a total of 626 papers published between 2016 and 2020 that used Blockchain technology in healthcare. In this paper, systematic methods for reviewing papers were presented. These systematic methods include: relying on scientific methods, the number of authors of the paper per year, the introduction of the institutions that created the paper, and the separation of papers based on the country of the author of the paper.

Akbar et al. [5] reviewed 72 articles between 2017 and 2021 on the role of Blockchain in healthcare. In this research, the fuzzy technique has been used to prioritize and sort the existing solutions in the field of Blockchain-based healthcare. Also, in this research, new methods have been used to optimize and create a road map in the field of Blockchain-based healthcare.

Sharma et al. [51] reviewed 47 articles between 2017 and 2021 on the use of Blockchain in healthcare. In this research, challenges such as optimal use of resources, data integrity, and rapid development of the healthcare Blockchain have been addressed.

Rahmani et al. [42] reviewed 34 articles between 2016 and 2021 in the field of using Blockchain in the Internet Medical of Thing (IoMT). In this research, the challenges of trust in the context of cloud computing for storing Internet of Things data have been discussed. Blockchain is mentioned as a solution for decentralization and security of data generated by sensors and wearable devices.

The authors of [48] reviewed 51 articles between 2017 and 2021 on the use of Blockchain in the field of healthcare. In this research, the major challenges such as lack of integrity, manipulation, and fraud in medical care data have been identified, and Blockchain has been mentioned as a solution to overcome these challenges. Also, in this research, the benefits of using the Blockchain in the field of healthcare are mentioned, such as more efficiency, less delay in information transmission, more data security, and improved management of resource consumption.

Abbas et al. [1] reviewed 53 articles between 2016 and 2021 on the use of Blockchain technology in healthcare. In this article, advantages such as non-alteration and manipulation of healthcare data, anonymity of participating parties, protection of patients' privacy, improvement of drug supply chain management, and safe and fast access to patient's records in the healthcare Blockchain are mentioned.

Examining the mentioned papers, several defects are found. For example, some of these papers are not SLR or the selection process is not clear or the tools used for evaluation and the framework are not specified in these papers. In this systematic review, we attempted to address these shortcomings.

Table 1 lists survey and SLR papers on healthcare security and privacy using Blockchain in recent years. In this table, each paper is examined considering the publication year, main topic, review types, paper selection processes, tools or framework, and covered years.

3 Research methodology

In this section, a methodology for doing this systematic review is mentioned. A systematic literature review has several advantages over traditional reviews, including: greater

Table 1 Summary of the related works

Reference	Publication year	Main topic	Review type	Paper selection process	Blockchain type	Evaluation metrics	Tools or Framework	Covered years
Mohamad Kassab et al. [23]	2019	Analysis of the challenges of using Blockchain in healthcare for stakeholders (patients, physicians, healthcare providers, insurance companies)	Survey	Clear	Not mentioned	Not mentioned	Clear	2015–2018
TOQEER ALI SYED et al. [55]	2019	Analysis of several applications that use Blockchain in the field of healthcare	Survey	Not clear	Mentioned	Not mentioned	Not clear	2015–2018
Susel Góngora Alonso et al. [7]	2019	An overview of the role of the Blockchain in healthcare and new ways to share data in this area	Survey	Not clear	Not mentioned	Not mentioned	Not clear	2015–2018
Thomas McGhin et al. [31]	2019	Analysis of challenges such as: security, interoperability, data sharing in the field of healthcare using Blockchain	Survey	Not clear	Not mentioned	Mentioned	Not clear	2016–2017
Anushree Tandona et al. [54]	2020	Analysis of processing and sharing and the patient records and medical data	SLR	Clear	Mentioned	Mentioned	Clear	2016–2019
Leili Soltanisehat et al. [52]	2020	Review of the use cases, challenges and structures of using Blockchain in healthcare	SLR	Clear	Mentioned	Not mentioned	Not clear	2016–2020
Israa Abuelez et al. [4]	2020	Analysis of the challenges of accessing medical records, security, data tracking and medical information and how to exchange information in the Blockchain healthcare network	Survey	Clear	Not mentioned	Not mentioned	Not clear	2017–2020
Anton Hasselgren et al. [18]	2020	Analysis of the challenges of access control, interoperability, and integrity of medical data using Blockchain	Survey	Not clear	Mentioned	Not mentioned	Not clear	2018–2020
Hassan Mansur Hussien et al. [19]	2021	Analysis of the challenges of Telcare medical information system and improving security and privacy in this area	Survey	Clear	Mentioned	Mentioned	Not clear	2016–2020
SABITA KHATRI et al. [24]	2021	Systematic analysis of Blockchain aggregation with healthcare	Survey	Clear	Not mentioned	Not mentioned	Not clear	2016–2020
	2021		Survey	Clear	Not mentioned	Not mentioned	Not clear	2016–2020

Table 1 (continued)

Reference	Publication year	Main topic	Review type	Paper selection process	Blockchain type	Evaluation metrics	Tools or Framework	Covered years
Abderahman Rejeb et al. [46]		Opportunities and use cases of Blockchain in healthcare						
Akbar et al. [5]	2022	Presenting fuzzy techniques for sorting and prioritizing existing solutions in the field of using Blockchain in healthcare.	SLR	Clear	Mentioned	Mentioned	Not clear	2017–2021
Sharma et al. [51]		Reviewing the challenges such as resource optimization, data integrity, and rapid Blockchain-based healthcare development.	SLR	Not clear	Mentioned	Not mentioned	Clear	2017–2021
Rahmani et al. [42]	2022	Systematic analysis of the Blockchain-based Internet Medical of Things in cloud computing	SLR	Clear	Not mentioned	Not mentioned	Not Clear	2016–2021
Saeed et al. [48]	2022	Analysis of the Challenges such as lack of integrity of data, manipulation and fraud in medical data, and delay in transmission of healthcare data	Survey	Clear	Mentioned	Mentioned	Not Clear	2016–2021
Abbas et al. [1]	2022	Systematic analysis of the Blockchain-based solutions for data sharing and supporting the anonymity of participating parties in the healthcare network.	SLR	Clear	Mentioned	Not mentioned	Not clear	2016–2021
This work	-	Analysis of the approaches for Improving healthcare security and privacy using Blockchain	SLR	Clear	Mentioned	Mentioned	Clear	2018–2022

transparency, more accurate reviews, step-by-step analyses, and more regular reviews. The article selection process and the research questions are also explained in this section.

3.1 Question formalization

The research questions that are answered in this study are as follows:

RQ1: What are the advantages and disadvantages of using Blockchain in Healthcare?

RQ2: How the patient's privacy in EHR is guaranteed by Blockchain?

RQ3: How the patient's security in EHR is guaranteed by Blockchain?

RQ4: What evaluation metrics are applied for evaluating the Blockchain-based approaches for improving security and privacy in healthcare?

RQ5: What are the tools or frameworks used in the Blockchain-based approaches for improving security and privacy in healthcare?

RQ6: What kind of Blockchain was used in the existing research studies?

RQ7: What are the open issues and future research directions of using Blockchain for improving the privacy and security of healthcare?

3.2 Paper selection process

Figure 1 summarizes the papers selection process in three steps:

Step 1: At this step, the papers are selected based on the title, abstract and keywords. 487 papers were selected at the end of this step.

Step 2: At this step, the continuation of the selection process of papers has been carried out based on the inclusion and exclusion criteria given in Table 3. At the end of this step, 331 papers were remained.

Step 3: Finally, by studying the full text of the papers and removing inappropriate ones, 51 papers were remained as final selected papers to be reviewed in this systematic review.

This study reviews papers published between 2018 and August 2022 that focused on Blockchain-based approaches for improving security and privacy in healthcare. Various databases have been used to conduct this study. The URLs of the used database are listed in Table 2.

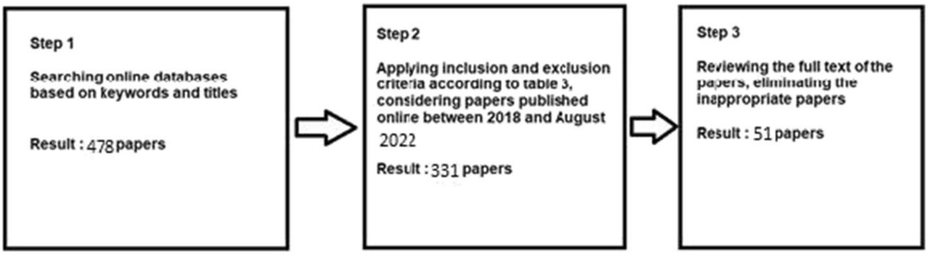
Step 1
Searching online databases based on keywords and titles
Result : 478 papers
Step 2
Applying inclusion and exclusion criteria according to table 3, considering papers published online between 2018 and August 2022
Result : 331 papers
Step 3
Reviewing the full text of the papers, eliminating the inappropriate papers
Result : 51 papers

Fig. 1 Paper selection process

Table 2 The searched online databases

Online database	URL address
Google Scholar	www.Scholar.google.com
IEEE	www.ieeexplore.ieee.org
ACM	www.dl.acm.org
Science Direct	www.sciencedirect.com
Springer	www.link.springer.com
Taylor & Francis	www.tandfonline.com
Wiley	www.onlinelibrary.wiley.com
Inderscience	www.inderscienceonline.com
ACM	www.dl.acm.org
Sage	www.online.sagepub.com
Emerald	www.emeraldinsight.com
Wiley	https://onlinelibrary.wiley.com
MDPI	www.mdpi.com
Hindawi	www.hindawi.com

The search keywords for the papers were as follows:

> "Blockchain" AND ("Healthcare" OR "EHR" OR "Medicine" OR "Electronic Health Record")

Table 3 lists the criteria for including and excluding the papers.

After applying the above keywords, 331 journal papers and 156 conference papers were found at the end of step 1. The number and percentage of journal and conference papers are shown in Fig. 2.

Figure 3 illustrates the number and percentage of final papers selected from each database.

Figure 4 shows the number of final papers selected at the end of step 3 categorized by years.

4 Advantages and disadvantages of using Blockchain in healthcare

In this section, we try to answer RQ1: What are the advantages and disadvantages of using Blockchain in Healthcare?

Using Blockchain technology can improve the integrity, privacy, and security and it provides better access to the necessary services. With Blockchain technology, both specialists and health organizations can act faster and more efficiently based on the available information

Table 3 Inclusion/exclusion criteria

Criteria	Description
Inclusion	These papers are exactly fit for this study
Studies that focused on Blockchain-based approaches for improving security and privacy in healthcare	These papers have a high scientific value
Journal papers published online from 2018 to August 2022	
Exclusion	This group of resources does not fit into our selection criteria.
Thesis, books, or book chapters	
Review papers or papers that only interpret the role of the Blockchain in healthcare	The intended solution in these papers is not clear
Not English papers or unjudged papers	Because these papers have not been fully judged and evaluated, they are not selected

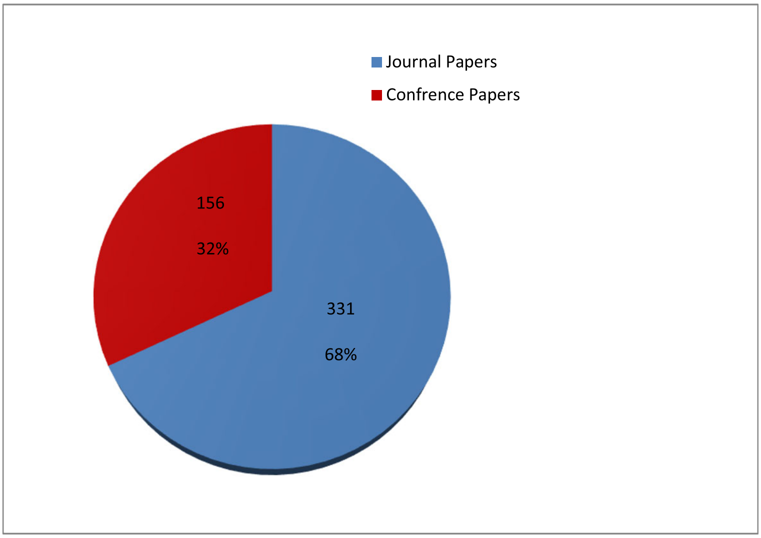

Fig. 2 Total selected papers at the end of step 1

which is safe and reliable. A safe and effective infrastructure can be created using smart contracts to increase the quality of healthcare and improve the well-being of individuals.

The authors of [47] presented the creation of the prototype and evaluation of the OmniPHR architectural model. A Personal Health Record (PHR) is a file that allows patients to access and manage their data. The OmniPHR integrates the Blockchain distributed records and OpenEHR. The performance of the OmniPHR was evaluated by dividing it into workloads and simultaneous sessions to transfer the database to a network of ten clouds. The results of the experimental evaluations in this paper showed that the Blockchain architecture of OmniPHR provides high-quality performance at the network level.

In another study [66], some applications of Blockchain in healthcare domains were presented as follows: (1) Track prescriptions to detect drug overdoses. (2) Sharing data for

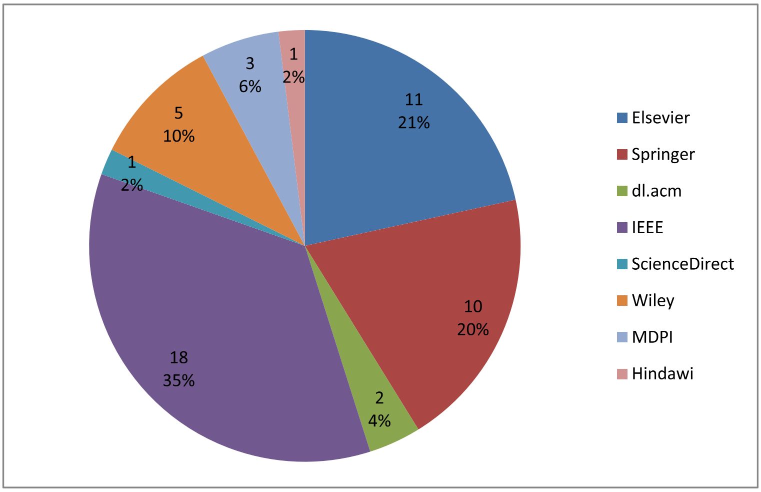

Fig. 3 The number and percentage of final papers selected from each database

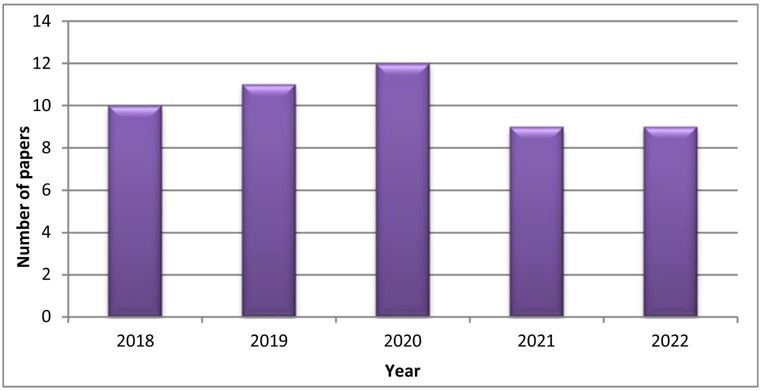

Fig. 4 The number of selected papers at the end of step 3 categorized by years

integrating traditional care into telemedicine. (3) Sharing data with the provider so that the patient can specify what data is being authorized. (4) Sharing the registered cases of cancer; collecting all of the observed cases of cancer. (5) Managing the patient's digital identity to better match the patient's history. (6) Creating a personal health record that can be fully accessed and controlled. (7) Automation of health insurance claims for error detection and fraud. This paper also discusses the challenges of using the Blockchain in healthcare, such as system evolution, privacy protection, etc.

Another study [29] mentioned some healthcare projects that benefit from Blockchain technology. One of the projects worth mentioning here is PokitDok. With PokitDok, organizations related to healthcare can implement modern business in Blockchain and a secure network of electronic health records and pharmaceutical equipment is provided.

In another study [60], a Blockchain-based security model was presented for electronic health records called EMRSB. In this model, medical data can be shared safely and effectively. By using Blockchain technology in EMRSB, Data loss and manipulation problems can be easily solved. Large files are stored in the IPFS file system[1] and the hash file is added to the Blockchain, which saves important resources in the Blockchain. This can increase the security level of the patient's privacy information.

The authors of paper [27] believed that the decentralization of the Blockchain would safeguard healthcare data and preserve the privacy of stakeholders in the field. Another important point mentioned in this paper is the lower cost of transferring data in the Blockchain compared to traditional methods. Data transfer in the Blockchain is done without the use of a central entity, which makes it less costly. It also uses Blockchain data tracking to ensure that healthcare data comes from a reliable source.

In another study [34] the characteristics of data integration and the immutability of data in the Blockchain were mentioned, which makes the Blockchain a suitable platform for maintaining healthcare data. In the healthcare network implemented by the Blockchain, the data added to the ledger cannot be changed and manipulated. The decentralization of the Blockchain means that there is no single failure point for the healthcare network. The paper also referred to smart contracts that allow transactions and agreements to be drawn up between parties involved in the healthcare Blockchain network without third-party intervention.

[1] The InterPlanetary File System.

Another study [62] listed several advantages of using Blockchain in healthcare, including: 1- Data accuracy in healthcare applications: Storing all healthcare data in the Blockchain makes this accompanying information up-to-date, traceable, and non-manipulative. These capabilities help medical professionals improve the treatment process of patients. 2- Interoperability of healthcare data: By using interoperability in the Blockchain network, the exchange of information between stakeholders in this field becomes better because all data in the Blockchain follow a certain standard, so the exchange of information is more efficient. 3- Data security in the field of healthcare: Capabilities such as hashing and data immutability in the Blockchain network make data healthcare more secure. 4- Lower cost of healthcare data management: The cost of data management in traditional healthcare data systems is much higher than storing these data seamlessly in a Blockchain network because the information is stored in different centers and databases. 5- Global sharing of healthcare data: A patient may be treated in one country and then travel to another to continue treatment. In this case, if traditional medical care systems are used, sharing patient's data among several different countries will be very difficult and perhaps impossible. Using a Blockchain network, patient's data can be easily shared globally. 6- Improving the audit of healthcare data using Blockchain: Using data audits in healthcare ensures that laws and regulations are fully complied with by institutions and stakeholders in this field. As data in the Blockchain is verifiable and information in the Blockchain is non-manipulative, it improves the audit of healthcare data.

The authors of [33] believed that wearable devices and patient-connected sensors play an important role in modern healthcare systems. In this paper, the data generated from these devices are integrated with Blockchain technology. This integration plays an important role in maintaining the security of this data.

The authors of [59] dealt with parallel healthcare systems (PHSs) and the role of Blockchain in maintaining data security of these systems. This paper proposed a method in which Blockchain is combined with PHS and using a consortium, healthcare data is shared more effectively.

Another study [20] pointed out some of the challenges in using Blockchain in healthcare, including high energy consumption, inefficient scalability, and relatively low throughput. To address these challenges, this paper introduced an architecture called lightweight Blockchain. In a lightweight Blockchain network, nodes were distributed in several clusters and a ledger was maintained in each cluster. This reduced the computational and communication costs of the healthcare network.

In [53], the attribute-based signature scheme was introduced to further protect the privacy of medical stakeholders. In this design, keys called master key to authenticate users and update key to specify attributes related to certain nodes were introduced. In this scheme, a number of parties participating in the Blockchain network (such as physicians) were identified with certain characteristics (such as < Hospital A. Department of Oncology. senior Physician>. After analyzing the patient information, these attributes are taken away from them by an algorithm called KUNodes.

Jeet et al. [21] developed a Blockchain-based framework for IoT data. In this framework, patient's data were collected by sensors and wearable devices, and were updated every moment. Therefore, new symptoms of illness and sensitivity in response to drugs can be recorded in the Blockchain immediately. Sha-256 encryption was used in this framework and the techniques used in this research reduce the encryption time.

Rajasekaran and Azees [43] presented a scheme for authentication of participating parties in the healthcare Blockchain. This scheme is a lightweight authentication scheme that supports the anonymity of participating parties in the healthcare Blockchain. In this scheme, doctors given the opportunity to share information about patients with other doctors without compromising the privacy and security of patient's data. Using the authentication method of this scheme, only authorized users can view the data of the healthcare field.

The authors of [69] presented a scheme for secure storage and sharing of medical data based on Blockchain. In this research, the authentication of all parties involved in the healthcare system has been carefully examined and a solution to the problem of information dispersion in the healthcare field has been provided.

5 Privacy in healthcare using the Blockchain

In this section, we try to answer RQ2: How the patient's privacy in EHR is guaranteed by Blockchain?

Blockchain technology can create a balance between the privacy of health data and access to those data. The purpose of the privacy policy is to protect patients' privacy while disclosing PHI[2]. Four goals must be achieved here: 1- Giving t full control of EHRs to patients. 2- Determining who can access and track the documents. 3- Making possible the secure transfer of the records. 4- Minimizing the chance of unauthorized people obtaining PHI. Blockchain technology can help achieve these four goals.

In [12], the authors recommended an efficient and secure Blockchain-based framework for accessing medical records called Ancile. Smart contracts in this framework were used for controlling and preventing data misuse. In addition, for improving security, advanced encryption techniques were applied. The purpose of this paper is to address privacy and security issues in healthcare. This framework focused on the rights of patient's data ownership. Data ownership is held by the patient, while parental or caregiver control is provided.

Paper [63] mentioned that in modern healthcare systems, patient participation is an important matter. This paper discussed Blockchain-based location sharing for E-health systems. The first step defines the basic needs for Blockchain-based location sharing, including decentralization, privacy, and reliability. Then, using Merkel's cryptography and root, a Blockchain-based privacy-preserving scheme called BMPLS was proposed for Location Sharing[3]. The results showed that this plan meets the necessary requirements. Finally, the outputs of this project and the results of the analysis confirm that this project is useful and feasible for the field of medical care. In short, the scheme could be used to share telecare Blockchain-based privacy for medical information systems.

In another study [66], Healthchain, a large-scale Blockchain-based health data privacy project was presented, in which health data were encrypted to control micro-access. With the introduction of the Healthchain, IoT data and physician diagnoses cannot be deleted or manipulated. Security analysis and experimental results suggest that Healthchain's proposal applies to the smart healthcare system. The important points mentioned in this paper are as follows: 1- A Blockchain-based healthcare system is recommended to protect the privacy of large-scale health data, called a Healthchain. The Healthchain allows users to download IoT data and receive feedback from physicians. Physicians are then able to read data and upload feedbacks. 2- In the Healthchain, for reducing the computational overhead and ensuring

[2] Personal Health Information.

[3] Blockchain-Based Multi-level Privacy-Preserving Location Sharing.

privacy, data is encrypted and stored in the IPFS[4]. 3- In addition, by transferring updated transactions, Healthchain allows users to revoke physicians' access at any time.

In another study [39], a Blockchain-based data storage scheme in healthcare was proposed. The proposed scheme can help improve privacy. Encryption techniques were used to protect patient's data and alias. In this approach, data processing methods as well as the cost-effectiveness of smart contracts used in the system were analyzed. Patients and health organizations participate as data transmitters and data receivers. With the assistance of these EHR systems and storing data in cloud network, patients share their personal data with physicians and health organizations.

The authors of [50] proposed a plan for implementation of EHR, which would protect EHR data more securely and privately. In this design, a framework was introduced that used the Hyperledger Fabric Blockchain.

In the proposed platform in [40], many problems are solved by storing encrypted health information in the cloud system. This platform ensures that patient's data in the cloud environment is controlled only by the patient himself. The goal is to maintain important healthcare data for network integrity and security. Current health systems do not have a pseudonym because they only store data in the cloud environment. But the proposed platform guarantees patients' aliases. Acquired aliases are obtained using cryptographic functions.

The proposed approach in [15] used four technologies that could be used in Blockchain for improving privacy. These four technologies are: zero-knowledge proofs, trusted execution environments, homomorphic encryption, and federal learning. In zero-knowledge proofs, one party involved (the prover) is allowed to validate a transaction or validation for the other party (the verifier) without disclosing any critical information. In healthcare contexts, for example, how a patient is treated can be expressed without disclosing the patient's true identity. In federal learning, an algorithm is sent to a node, then that node analyzes the algorithm and finally shares the updated algorithm among all the nodes in the Blockchain. In this way, by separating how to update the algorithm from other nodes, the risks of privacy and security breaches are minimized. Homomorphic encryption allows calculations to be performed on encrypted data. For example, a patient can encrypt their data and send it to an unreliable third party. This third party performs an analysis on the encrypted data and then sends the result of its analysis to the patient in an encrypted form. In this way, the patient can utilize another person's review of their data without exposing his/her data. In trusted execution environment technology, privacy is met through hardware. Most cell phones today use this technology in their structure.

In [44], Blockchain-based knapsack algorithms were used for privacy. The greedy algorithm of knapsack can lead to Blockchain-based privacy and security in healthcare. In this method, first the healthcare data is encrypted by the knapsack algorithm and then this encrypted data is transferred to the Blockchain. In the Blockchain, healthcare data is validated and then decrypted by the knapsack algorithm and finally sent to the desired nodes. Knapsack algorithms are symmetric cryptographic systems. This method uses public keys to encrypt and private keys to decrypt.

Paper [32] suggested a framework that uses off-chain computing and storage technology. Off-chain Blockchain hybrid design architecture (OCBS) processes and manages information through distributed software that interacts with off-chain sources. This system tries to improve privacy and scalability. In the framework proposed in this paper, the ownership rights of

[4] Inter-Planetary File System.

patient's data are observed. Moreover, in this framework, patients can manage their own data and digital identity.

Paper [67] proposed a Blockchain-based telephone privacy tracking plan in the field of healthcare. In this plan, healthcare stakeholders can connect to the Blockchain network with their mobile phones. In this plan, first, the location of the caller is determined and then it is determined whether a particular patient has called this system. In the design proposed in this paper, the integration of emerging 5G technology with Blockchain-based healthcare systems leads to higher reliability, less communication delay and improved privacy of medical stakeholders.

Another study [58] pointed to the role of Blockchain technology in better management of healthcare data and maintaining the security of this data. In this paper, a prototype using the Hyperledger platform was proposed. This prototype was an authorized private Blockchain that ensures better control of access to healthcare data.

The paper [3] proposed a reliable framework for wearable devices and patient-connected sensors that utilized Blockchain technology. With data management, this framework protected the privacy of information related to the field of healthcare and ensured the confidentiality and integrity of data.

The authors of [25] introduced a framework that uses Blockchain technology. Using smart contracts, this framework provided effective management to conserve human resources. In this framework, the human resource data were created and then these data were distributed on a global platform based on Blockchain.

In another study [65], fuzzy analytic on the blockchain platform was introduced. Using fuzzy analytic network, a Blockchain implementation model to improve the security of healthcare data was introduced. In this study, a permissioned private Blockchain network was used to manage access to medical data.

A decentralized architecture based on Blockchain was proposed by Nishi et al. [38]. In this architecture, the patient is the real owner of his/her data, in such a way that any permission to view the data related to the patient must be done with his/her permission. In this architecture, attribute authorities can issue or revoke the attribute only with the patient's permission.

Alsayegh et al. [8] investigated how the privacy and security of EHR sharing can be maintained in two types of Blockchain networks. Private Blockchain was used to store encrypted EHRs and consortium Blockchain along with smart contracts to verify the identity of patients.

The authors of [2] introduced a framework for greater security and privacy of individuals who received the Covid-19 vaccine using Blockchain. In this framework, the W3C standard certificate is used to prove the certificate of receiving the vaccine. In this framework, IPFS has also been used to protect the privacy of vaccine recipients. In this framework, users have been given the opportunity to share their data with other people without compromising their security and privacy.

6 Securing healthcare data by using the Blockchain

In this section, we try to answer RQ3: How the patient's security in EHR is guaranteed by Blockchain?

In the smart health scenario, one of the most important issues is the security of the health system. The main challenges for a smart health system are security and the reduction of accurate data with the rule. Blockchain technology suggests that a consortium shall consist of several stakeholders such as hospitals, physicians, pharmacists, pathologists, researchers, and insurance companies. The security debate here means the secure exchange of data among all the parties involved. Moreover, all the stakeholders must be authenticated and authorized to enter each level of the Blockchain.

The authors of [26] stated that Blockchain may provide a solution to address current EHR performance limitations. In Blockchain, the patient's entire record is stored in the ledger and encrypted by the patient's private key. Although the Blockchain system is not completely impenetrable, it is more secure than most current systems.

The authors of [11] suggested that data theft in the EHR can endanger patient privacy. In general, most data in the EHR remains unchanged after being uploaded to the system. Therefore, Blockchain can be used to share this data more effectively. Participating organizations and medical parties can more confidently access EHRs stored in Blockchain. In this paper, a cryptographic scheme for healthcare was proposed based on Blockchain technology. The index for the EHR is stored in the Blockchain. Because only this index is transferred to Blockchain for ease of publication, patients have complete control over who can view their EHR data. In this system, only search indices are added to the Blockchain and facilitate EHR distribution, while real EHRs are stored encrypted on another server. To access EHRs, users must grant their permission to the information owner with a decryption key.

Paper [36] presented a new EHR sharing scheme based on cloud computing and Blockchain. Initially, the authors identified the main challenges of current health systems, and effective solutions to these problems are proposed through the implementation of a real prototype. To test the proposed method, an Amazon-based Ethereum Blockchain is proposed. Moreover, to achieve data storage and data sharing, the IPFS storage system integrates with Blockchain. The results of this program showed that the proposed framework can share medical information more safely and quickly compared to conventional methods. By using access control, unauthorized access to health data can be detected and prevented. The advantages of the proposed model showed that the Blockchain solution is a more effective way to manage medical records compared to traditional methods.

Paper [28] addressed the problems of data collaboration and the use of healthcare programs in a heterogeneous cloud environment. A framework called ChainSDI suggests that the Blockchain technique, along with many computational resources, may be used to manage secure data. The prototype shows how this framework works.

The proposed method in [10] had the following architecture contributions: First, a healthcare framework called ChainSDI is presented which is based on a combined "home-edge-core" SDI to provide real-time performance and accountability for home-based healthcare services. Second, they are looking to build a secure Blockchain network to ensure that any transaction in ChainSDI is in accordance with the regulations, while still being able to interact with the data.

Paper [17] provided telemedicine services on demand (MoD). This technology is used to overcome challenges and improve telemedicine services. This paper proposed an approach to achieve authentication and licensing with greater flexibility and efficiency for the department of defense's services in the medical trap system. A key program has been distributed for independent updates in the telemedicine system, which aims to update the patient's keys separately. Using Blockchain and distributed ledger also protects the integrity of private healthcare data. This prevents malicious users from trying to change the physicians' diagnosis. Using the Blockchain technique in EHR, patient's data is stored in a chain to prevent a user or unauthorized users from manipulating it. Finally, it is concluded that the proposed approach resists collusion attacks in (N-1) destructive attacks.

In [22], containers in the Blockchain substrate were used for greater security of healthcare data. These containers are connected to multiple ports to improve the data transfer process. In this research, a framework called Medichain on a Blockchain platform is proposed. In each block of the proposed framework, a list of patient records is maintained, which is secured using the security features of Blockchain technology. This framework was implemented by the Python programming language and used object-oriented concepts.

The authors of [61] used Blockchain technology to further secure healthcare data. The scheme proposed in this paper places great emphasis on protecting patients' medical records from information theft and unauthorized intrusion. This paper first identified how to manage and control access to medical care data. Then, using Blockchain technology, a platform for data storage and transmission was introduced. In this platform, data transfer and storage were done through cryptographic algorithms. The results of the implementation and simulation of the proposed platform showed better performance in data storage as well as more efficient data transfer than similar schemes.

The authors of [68] emphasized the privacy and security issues of healthcare stakeholders. In this paper, several features of Blockchain technology such as: anonymous signatures, zero-knowledge proofs, attribute-based encryption, and approval of smart contracts were used for more security of healthcare data. This paper also used various security techniques to ensure the data sharing process.

In another study [45], the characteristics of the Blockchain network were investigated. Then, consensus algorithms were analyzed, and finally, a framework for maintaining the security and privacy of data related to patients in the field of healthcare was introduced.

The authors of [57] discussed remote patient monitoring (RPM). In this paper, an architecture was presented that effectively transfers healthcare data and stores them in a Blockchain.

In another study [14], Blockchain's smart contracts were used for the proper analysis and management of data generated in the field of medical care. Using the method presented in this paper, the generated data by sensors connected to the patient's body are analyzed by smart contracts. If the patient-generated data were in critical condition, a warning was sent to the medical center so that the patient could receive immediate intensive care.

In [13], a Blockchain-based healthcare data management system was proposed. Using this information management system, patients can easily access their medical records located in various medical centers. Asymmetric encryption was used to further secure the system data.

The authors of [56] integrated smart health care systems (SHSs) with Blockchain technology. This paper examined the challenges of SHS systems and used Blockchain technology to maintain greater security and data integrity in the field of smart healthcare.

Another study [16] presented an attribute-based signature scheme with different authorities. In this paper, the patient disclosed part of his data without exposing the rest of his information. This part of the information disclosed by the patient is provided to physicians and researchers by healthcare providers. The physician or researcher performs the desired analysis on this data. At the end, these authorities were taken away from them.

The authors of [41] proposed solutions to prevent the production and distribution of counterfeit drugs in the healthcare network using Blockchain technology. This plan covers the drug distribution cycle from production to consumption by the patient. The distribution and production of counterfeit drugs in the healthcare system is prevented by using Blockchain.

Paper [35] dealt with the safe storing of healthcare data. It provided a Blockchain-based framework using a keyless signature protocol for the security of patient's medical records and ensured the integrity and security of data in this area.

Another study [49] introduced a framework based on Blockchain. In this framework, the management and control of access to medical data were effectively proposed. The use of this framework improved data privacy, confidentiality, and decentralization in the medical care system.

Qadar Butt et al. [9] presented a Blockchain technology for use in medical communication and developed a location-independent global health record exchange system for transferring medical data. Using Blockchain technology and a federal identity management system, the proposed system authenticates users and the person requiring user information under the guidance.

The authors of [37] presented a scheme for sharing data in the field of healthcare using Blockchain and edge computing. This scheme guarantees the security and privacy of shared data. In this scheme, the hash and filtering functions were used to maintain the security of the shared data. Also, in this research, a process has been designed to determine the amount of reward for miners to mine healthcare blocks.

In [6], Blockchain was used to access keywords for searching in distributed healthcare databases and a new mechanisms are used to revoke the public and private keys of users. Therefore, any user will not be able to access the healthcare blockchain after a certain period of time. This makes the healthcare Blockchain more secure. In the proposed approach, public and private keys are given to the participating parties only for a certain period of time to prevent unauthorized people from entering the healthcare Blockchain.

7 Discussion

This section analyzes the reviewed papers to answer the remaining research questions:

> **RQ4:** What evaluation metrics are applied for evaluating the Blockchain-based approaches for improving security and privacy in healthcare?

Table 4 lists the evaluation metrics for assessing the Blockchain-based approaches for improving security and privacy in healthcare. Evaluation metrics such as integrity (in 10% of papers), access control (in 8% of papers), security (in 25% of papers), privacy (in 17% of papers), availability (in 6% of papers), latency (in 4% of papers), scalability (in 10% of papers), performance (in 17% of papers) and cost (in 4% of papers) were reviewed and analyzed. Figure 5 represents the percentage of using each evaluation metrics considered in the selected papers.

> **RQ5:** What are the tools or frameworks used in the Blockchain-based approaches for improving security and privacy in healthcare?

Table 4 lists the tools and frameworks used in the existing Blockchain-based approaches for improving security and privacy in healthcare. Various frameworks, platforms and tools have been used in the papers reviewed in this review paper. These frameworks, platforms and tools have various features, the most important of which are: Use of smart contracts to control access

Table 4 A summary of the reviewed papers

Reference	Main idea	Kind of Blockchain	Tool(s) or framework(s)	Evaluation metrics
Roehrs et al. [47]	Creation of the prototype and evaluation of the OmniPHR architectural model	Private	A method called OmniPHR	MTBF, MTTR
Peng Zhang et al. [66]	Several practical applications of Blockchain in healthcare	Both(public and private)	Not mentioned	Not mentioned
Jorge Lopes et al. [29]	A safe way to improve the security and privacy of healthcare	Not clear	Not mentioned	Not mentioned
Sihua Wu, Jiang Du [60]	A secure model for Blockchain-based healthcare data sharing	Not clear	Not mentioned	Not mentioned
Tian-Fu Lee et al. [27]	A plan for telecare of healthcare information using Blockchain	Private	Not mentioned	Security, Performance, efficient computation and communication.
AHMAD MUSAMIH et al. [34]	Tracking of medical data in Blockchain-based healthcare network	Public	Not mentioned	Cost, Security, Scalability
Ibrar Yaqoob et al. [62]	Projects and case studies to demonstrate Blockchain performance in various healthcare applications	Both(public and private)	Not mentioned	Not mentioned
Mulalo Muofhe et al. [33]	Manage and control patient's data in healthcare systems using Blockchain	Not clear	Not mentioned	Not mentioned
Wang et al. [59]	Create an artificial model of electronic health records to simulate and display real data Blockchain-based healthcare systems	Consortium	A framework called PHS	integrity, interoperability and facilitating medical research
Leila Ismail et al. [20]	Secure transfer of transactions and confidential data between nodes participating in a Blockchain-based healthcare network	Public	Not mentioned	Security, Privacy, Performance
QIANQIAN SU et al. [53]	A revocable signature-based scheme for healthcare data using Blockchain	Private	Proposed a revocable signature framework	Security, Privacy, Performance
Rubal Jeet et al. [21]	Using the Blockchain to prove the receipt of the Covid-19 vaccine	Public	A framework for the security and privacy of people receiving the Covid-19 vaccine	Scalability, Data integrity
Arun Sekar Rajasekaran And M. Azees [43]	Providing a lightweight scheme to support the anonymity of participating parties in the healthcare Blockchain	Public	Not mentioned	Communication Cost

Table 4 (continued)

Reference	Main idea	Kind of Blockchain	Tool(s) or framework(s)	Evaluation metrics
Duo Zhang et al. [69]	A scheme for secure storage and sharing of medical data based on Blockchain	Consortium Blockchain	A framework for authentication, uploading and updating data	Access Control, Integrity, Auditability
Dagher et al. [12]	Control the level of access to healthcare data using Blockchain	Private	A framework called Ancile	Recognize the difficulty of accessing healthcare data
Ji et al. [63]	Blockchain-based privacy for Telecare medical information systems	Hybrid	A Blockchain-based multi-level location sharing scheme (BMPLS)	initialization, location record, and location sharing
Al Omar et al. [39]	Propose a platform for Blockchain-based healthcare stakeholder data privacy	Hybrid	A platform called MediBchain	Pseudonymity, privacy, integrity, accountability and security
Yogesh Sharma, Balamurugan [50]	Propose a Blockchain-based system for improving the privacy and security of healthcare data	Private	Framework based on Hyper Ledger Fabric	Not mentioned
Prateek Pandey, Ratnesh Litoriya [40]	Propose a plan for the global implementation of Blockchain-based health services	Public	Not mentioned	Not mentioned
Marielle Gross, Robert C. Miller [15]	Use four Blockchain-based technologies to protect healthcare data	Not clear	Not mentioned	Not mentioned
Ranjith J, Mahantesh K [44]	Blockchain-based Knapsack algorithms for privacy	Not clear	Knapsack crypto-system	Execution time, Block generation time
Ken Miyachi, Tim K. Mackey [32]	suggest a framework that uses off-chain computing and storage technology	Consortium	A framework that uses off-chain computing and storage technology	Performance,
Can Zhang et al. [67]	proposes a Blockchain-based telephone privacy tracking plan in the field of healthcare	Both(public and private)	Not mentioned	Computational costs, communication costs
Muhammad Usmana, Usman Qamar [58]	Improved access control and medical data sharing	Not clear	Mentioned	Not mentioned
ABOU-NASSAR et al. [3]	Models to make healthcare data more secure using Blockchain	Private	A framework called DITrust Chain	Scalability, mutual authentication, trustworthiness, privacy, data integrity and availability

Table 4 (continued)

Reference	Main idea	Kind of Blockchain	Tool(s) or framework(s)	Evaluation metrics
KIM et al. [25]	Propose a framework for maintaining the privacy of health record management	Hybrid	Not mentioned	latency and failure point
Zarour et al. [65]	Evaluate the Blockchain-based approach to improve the security of healthcare records	Private	Not mentioned	Patient's identity, data security, data monitoring and immutability
Farjana Khanam Nishi [38]	A decentralized architecture based on Blockchain	Public	An Ethereum framework for decentralized data sharing	Not mentioned
Muneera Alsayegh et al. [8]	A decentralized Blockchain-based architecture for encrypted data storage and patient identification	Consortium- Private	An Ethereum framework	efficiency
Amal Abid et al. [2]	A framework for more security and privacy of persons who receiving the Covid-19 vaccine	Private	A framework for secure data sharing of people who receiving the Covid-19 vaccine	Scalability, Cost
Nir Kshetri [26]	Cyberattacks against healthcare data	Not clear	Not mentioned	Not mentioned
Chen et al. [11]	Searchable encryption for encrypting healthcare data using Blockchain	Hybrid	EHRs sharing scheme	system security and privacy
NGUYEN et al. [36]	Mobile and cloud-based healthcare data sharing using Blockchain	Hybrid	A Blockchain-based searchable encryption framework	Access control, network latency, flexibility, availability, single point of failure and integrity
Li et al. [28]	Propose a plan to implement healthcare data software infrastructure in accordance with the rules using Blockchain	Private	A framework called ChainSDI	Threat model and security analysis, Blockchain performance analysis and service performance analysis
Sabyasachi Chakraborty et al. [10]	Create a framework for managing, controlling and storing patient's data	Consortium	A framework for managing, controlling and storing patient's data	Not mentioned
GUO et al. [17]	An effective and flexible model for implementing a telemedicine system using Blockchain	Hybrid	Not mentioned	authority, traceability and integrity

Table 4 (continued)

Reference	Main idea	Kind of Blockchain	Tool(s) or framework(s)	Evaluation metrics
Rahul Johari et al. [22]	Improve the security of healthcare data using Blockchain	Not clear	A framework called Medichain to secure patient’s data	Not mentioned
HONGJIAO WU et al. [61]	The scheme proposed in this paper places great emphasis on protecting patients’ medical records from theft of information and unauthorized intrusion.	Not Clear	Not mentioned	Security, Performance
Rui Zhang et al. [68]	Several features of Blockchain technology such as: anonymous signatures, zero-knowledge proofs, attribute-based encryption and approval of smart contracts were used for more security of healthcare data.	Private	Not mentioned	Not mentioned
Partha Pratim Ray et al. [45]	Use Blockchain to improve the security of data generated by sensors and wearable devices	Not Clear	Not mentioned	Not mentioned
ASHRAF UDDIN et al. [57]	Improve data sharing among healthcare stakeholders	Private	Not mentioned	Privacy, Security, Performance
Kristen N. Griggs et al. [14]	Use smart contracts to monitor patient’s data	Private	Not mentioned	Security, Privacy
Kai Fan et al. [13]	Improve the management and sharing of healthcare data	Both(public and private)	Not mentioned	Privacy, Security, Performance
Gautami Tripathi et al. [56]	Intelligent healthcare systems using Blockchain	Not mentioned	A framework based on intelligent healthcare systems	Not mentioned
RUI GUO et al. [16]	Attribute-based signature model	Not mentioned	Not mentioned	Privacy, Security
Prateek Pandey, Ratnesh Litoriya [41]	Prevent the distribution of counterfeit drugs using Blockchain-based networks	Private	Hyperledger framework	Transparency, Privacy, Security
Gayathri Nagasubramanian et al. [35]	Improve the integrity of healthcare data	Not mentioned	Keyless signature infrastructure framework	Integrity
AYESHA SHAHNAZ et al. [49]	Secure storage of healthcare data in compliance with the rules and regulations of medical organizations	Public	A framework for secure storage of healthcare data	Latency, Integrity, Access control

Table 4 (continued)

Reference	Main idea	Kind of Blockchain	Tool(s) or framework(s)	Evaluation metrics
Ghulam Qadar Butt et al. [9]	A Blockchain technology for use in medical communication and developed a location-independent global health record exchange system for transferring medical data	Private	Hyperledger Fabric framework	Latency
Xueli Nie et al. [37]	A blueprint for healthcare data sharing using Blockchain and edge computing	Public	A framework for IoMT edge computing and more security and privacy of IoMT data	Latency, Cost
Aitizaz Ali et al. [6]	Using Blockchain for faster keyword searching in healthcare distributed databases	Public	A framework for the privacy-preserving in IoT	Not mentioned

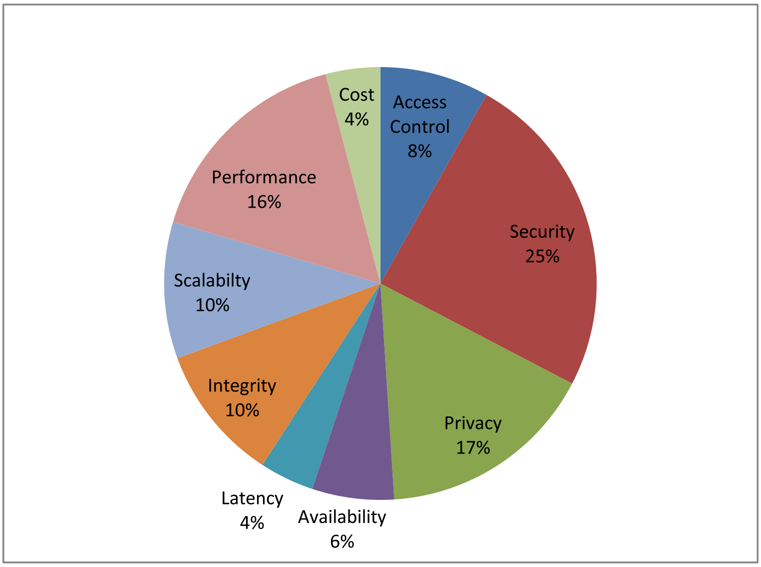

Fig. 5 The percentage of using each evaluation metric considered in the selected papers

and protection of data, guaranteeing access to data and ensuring that the patient owns the information about himself/herself, protection of data generated by sensors and wearable devices, distribution of data globally and Internationally, artificial intelligence decision making for better disease diagnosis, searchable encryption for sharing medical records, secure management of healthcare data, telemedicine services, etc.

RQ6: What kind of Blockchain was used in the existing research studies?

Table 4 lists the types of Blockchains used in each paper. Figure 6 represents the percentage of the Blockchain's type, used in each reviewed paper. 35% of the reviewed papers used private Blockchain, 10% used hybrid Blockchain, 43% used public Blockchain, and 12% used consortium Blockchain.

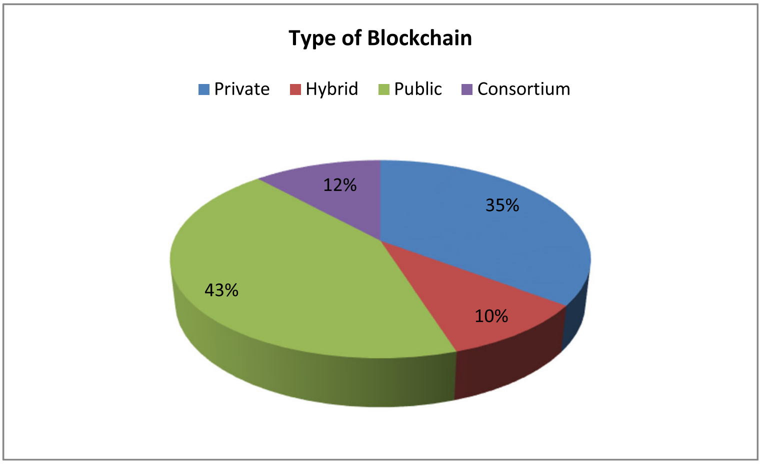

Fig. 6 The percentage of Blockchain's type used in the reviewed papers

8 Open issues and future research directions

In this section, we aim to answer RQ7: What are the open issues and future research directions of using Blockchain for improving the privacy and security of healthcare?

Some issues of using Blockchain in Healthcare such as cost, profitability, and scalability require further research. Using a distributed system for eliminating intermediaries can effectively overcome many of the current challenges in the medical and healthcare systems. Moreover, despite the existence of a pandemic such as Corona (Covid-19), the creation of a Blockchain network, which is a consortium of all the parties involved in the disease, could be the subject of future research. Using this Blockchain consortium network, various medical centers, governments, patients, insurance companies, information centers, etc. can exchange all information about epidemics. Therefore, by using this safe platform, all treatment methods as well as accurate statistics of epidemic diseases, can be obtained. Some other important open issues and future works are:

- Pharmacy: The use of Blockchain in the pharmaceutical industry improves the tracking of products in this area and prevents the distribution of counterfeit drugs.
- Globalization of healthcare networks: Blockchain-based healthcare networks can be implemented globally. Using global healthcare networks, patients' medical records can be accessed from anywhere in the world.
- Improving the scalability of Blockchain-based healthcare: Due to the increasing use of Blockchain technology in healthcare networks, more research is needed to improve the scalability of these networks.
- Use more efficient cryptographic techniques: Healthcare transactions contain critical information that is considered by many hackers and attackers. Therefore, the development of new and more effective encryption methods requires more researches.
- Use of artificial intelligence in Blockchain-based healthcare networks: As Blockchain-based healthcare systems are growing exponentially; analyzing data in this area will become increasingly difficult. Using artificial intelligence and machine learning can make it easier to parse and analyze data in this area.

9 Conclusion and limitation

This review provided a systematic review of the existing Blockchain-based approaches that tried to preserve privacy and security in healthcare. At first, Blockchain and its characteristics were defined, and then the electronic health records and the role that Blockchain can play in maintaining security and privacy in this area were examined. We selected and reviewed recent papers from valid scientific databases. The advantages and disadvantages of using Blockchain in healthcare compared to traditional methods were mentioned. After applying the mentioned query, 331 journal papers and 156 conference papers were found in all of the above-mentioned databases. Finally, we selected 51 papers published between 2018 and December 2022 according to the mentioned paper selection process. We discussed the main idea, evaluation metrics, and tools or framework, and type of Blockchain used in each selected paper. Evaluation metrics such as integrity (in 10% of papers), access control (in 8% of papers), security (in 25% of papers), privacy (in 17% of papers), availability (in 6% of papers), latency (in 4% of papers), scalability (in 10% of papers), performance (in 16% of papers) and cost (in 4% of papers) were used in the reviewed papers. Regarding the type of Blockchain used in the papers, it was observed that 35% of the reviewed papers used private Blockchain, 10% used hybrid Blockchain, 43% used public Blockchain and 12% used consortium Blockchain.

Regarding the limitations of this paper, we can mention the non-use of conference papers. Conference papers can sometimes contain interesting and innovative materials. In this paper, seven research questions were mentioned and answered, while other researchers may consider additional questions. Also in this review paper, six valid scientific databases were used to search for papers, while other valid scientific databases were also available for search. In this paper, only international journals have been used and national and domestic journals have been omitted. Moreover, non-English papers and book chapters were not used. Finally, this paper reviewed papers that were published between 2018 and August 2022, and papers that were published before 2018 were not reviewed.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare that there is no conflict of interest.

References

1. Abbas AF, Qureshi NA, Khan N, Chandio R, Ali J (2022) The blockchain technologies in healthcare: prospects, obstacles, and future recommendations; lessons learned from digitalization. Int J Online Biomedical Eng 18(9):2–12
2. Abid A, Cheikhrouhou S, Kallel S, Jmaiel M (2022) NovidChain: blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. Softw Pract Exp 52(4):1–24
3. Abou-Nassar E, Iliyasu AM, El-Kafrawy PM, Song O-Y, Bashir AK, Abd El-Latif AA (2020) DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access 8:1–13
4. Abu-Elezz I, Hassan A, Nazeemudeen A, Househ M, Abd-Alrazaq A (2020) The benefits and threats of blockchain technology in healthcare: a scoping review. Int J Med Informatics 142:2–8
5. Akbar MA, Leiva V, Rafi S, Qadri SF, Mahmood S, Alsanad A (2022) Towards roadmap to implement blockchain in healthcare systems based on a maturity model. Journal of Software: Evolution and Process e2500. https://doi.org/10.1002/smr.2500
6. Ali A, Almaiah MA, Hajjej F, Pasha MF, Fang OH, Khan R, Zakarya M (2022) An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors 22(2):2–18
7. Alonso SG, Arambarri J, López-Coronado M, de la Torre Díez I (2019) Proposing new blockchain challenges in ehealth. J Med Syst 43(3):1–5
8. Alsayegh M, Moulahi T, Alabdulatif A, Lorenz P (2022) Towards secure searchable electronic health records using consortium blockchain. Network 2(2):2–18
9. Butt GQ, Sayed TA, Riaz R, Rizvi SS, Paul A (2022) Secure healthcare record sharing mechanism with blockchain. Appl Sci 12(5):1–19
10. Chakraborty S, Aich S, Kim H-C (2019) A secure healthcare system design framework using blockchain technology. Advanced communication technology. IEEE, pp 1–4
11. Chen L, Lee W-K, Chang C-C, Choo K-KR, Zhang N (2019) Blockchain based searchable encryption for electronic health record sharing. Future Gener Comput Syst 95:2–5
12. Dagher GG, Mohler J, Milojkovic M, Marella PB (2018) Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain Cities Soc 39:1–11
13. Fan K, Wang S, Ren Y, Li H, Yang Y (2018) Medblock: efficient and secure medical data sharing via blockchain. J Med Syst 42(8):1–8
14. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Howson, Thaier Hayajneh (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst 42(7):1–6

15. Gross M, Miller RC (2021) Protecting privacy and promoting learning: blockchain and privacy preserving technology should inform new ethical guidelines for health data. Health Technol 11(5):1–4
16. Guo R, Shi H, Zhao Q, Zheng D (2018) Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access 6:3–9
17. Guo R, Shi H, Zheng D, Jing C, Zhuang C, Wang Z (2019) Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system. IEEE Access 7:1–12
18. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A (2020) Blockchain in healthcare and health sciences—a scoping review. Int J Med Informatics 134:3–9
19. Hussien HM, Yasin S Md, Udzir NI, Ninggal MIH, Salman S (2021) Blockchain technology in the healthcare industry: trends and opportunities. J Ind Inf Integr 22:2–20
20. Ismail L, Materwala H, Zeadally S (2019) Lightweight blockchain for healthcare. IEEE Access 7:2–6
21. Jeet R, Kang SS, Hoque S, S. M., Dugbakie BN (2022) Secure model for IoT healthcare system under encrypted blockchain framework. Secur Commun Netw. https://doi.org/10.1155/2022/3940849
22. Johari R, Kumar V, Gupta K, Deo Prakash Vidyarthi (2021) BLOSOM: BLOckchain technology for security of Medical records. ICT Express 8(1):56–60
23. Kassab MH, DeFranco J, Malas T, Laplante P, Neto VVG (2019) Exploring research in blockchain for healthcare and a roadmap for the future. IEEE Trans Emerg Top Comput 9(4):8–13
24. Khatri S, Alzahrani FA, Ansari Md TJ, Agrawal A, Kumar R, Khan RA (2021) A systematic analysis on blockchain integration with healthcare domain: scope and challenges. IEEE Access 9:3–19
25. Kim T-H, Kumar G, Saha R, Rai MK, Buchanan WJ, Thomas R, Mamoun Alazab (2020) A privacy preserving distributed ledger framework for global human resource record management: the blockchain aspect. IEEE Access 8:1–10
26. Kshetri N (2018) Blockchain and electronic healthcare records [cybertrust]. Computer 51(12):1–4
27. Lee T-F, Li H-Z, Hsieh YP (2021) A blockchain-based medical data preservation scheme for telecare medical information systems. Int J Inf Secur 20(4):6–12
28. Li P, Xu C, Jin H, Hu C, Luo Y, Cao Y, Mathew J, Ma Y (2019) ChainSDI: a software-defined infrastructure for regulation-compliant home-based healthcare services secured by blockchains. IEEE Syst J 14(2):1–9
29. Lopes J, Pereira JL (2018) Blockchain technologies: opportunities in healthcare, Digital Science. Springer International Publishing, pp 435–442
30. Marzieh Fathi MH, Kashani SM, Jameii E Mahdipour (2021) Big data analytics in weather forecasting: a systematic review. Arch Comput Methods Eng 29(2):1247–1275
31. McGhin T, Choo K-KR, Liu CZ, He D (2019) Blockchain in healthcare applications: research challenges and opportunities. J Netw Comput Appl 135:1–10
32. Miyachi K, Mackey TK (2021) hOCBS: a privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Inf Process Manag 58(3):6–21
33. Muofhe M, Dlodlo N, Terzoli A (2019) An internet of things-based system integrated with blockchain to manage patient data in the healthcare sector. In: 2019 Open Innovations (OI). IEEE, pp 1–6
34. Musamih A, Salah K, Jayaraman R, Arshad J, Debe M, Al-Hammadi Y, Ellahham S (2021) A blockchain-based approach for drug traceability in healthcare supply chain. IEEE Access 9:6–14
35. Nagasubramanian G, Sakthivel RK, Patan R, Gandomi AH, Sankayya M, Balusamy B (2020) Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput Appl 32(3):1–7
36. Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2019) Blockchain for secure EHRs sharing of mobile cloud based e-health systems. IEEE Access 7:1–11
37. Nie X, Zhang A, Chen J, Qu Y, Yu S (2022) Blockchain-empowered secure and privacy-preserving health data sharing in edge-based IoMT. Secur Commun Netw. https://doi.org/10.1155/2022/8293716
38. Nishi FK, Khan MM, Alsufyani A, Bourouis S, Gupta P, Saini DK (2022) Electronic healthcare data record security using blockchain and smart contract. J Sens: 1–18. https://doi.org/10.1155/2022/7299185
39. Omar AA, Bhuiyan Md ZA, Basu A, Kiyomoto S, Rahman MS (2019) Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Future Gen Comput Syst 95:1–10
40. Pandey P, Litoriya R (2020) Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology. Health Policy Technol 9(1):1–8
41. Pandey P, Litoriya R (2021) Securing e-health networks from counterfeit medicine penetration using blockchain. Wirel Pers Commun 117(1):3–14
42. Rahmani MKI, Shuaib M, Alam S, Siddiqui ST, Ahmad S, Bhatia S, Mashat A (2022) Blockchain-based trust management framework for cloud computing-based internet of medical things (IoMT): a systematic review. Comput Intell Neurosci: 2–10. https://doi.org/10.1155/2022/9766844
43. Rajasekaran AS, Azees M (2022) An anonymous blockchain-based authentication scheme for secure healthcare applications. Sec Commun Netw: 1–10. https://doi.org/10.1155/2022/2793116
44. Ranjith J, Mahantesh K (2021) Blockchain-based knapsack system for security and privacy preserving to medical data. SN Comput Sci 2(4):1–6

45. Ray PP, Dash D, Salah K, Kumar N (2020) Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. IEEE Syst J 15(1):1–7
46. Rejeb A, Treiblmaier H, Rejeb K, Zailani S (2021) Blockchain research in healthcare: a bibliometric review and current research trends. J Data Inform Manag 3:3–13
47. Roehrs A, da Costa CA, da Rosa-Righi R, da Silva VF, Goldim JR, Schmidt DC (2019) Analyzing the performance of a blockchain-based personal health record implementation. J Biomed Inform 92:1–8
48. Saeed H, Malik H, Bashir U, Ahmad A, Riaz S, Ilyas M, Khan MIA (2022) Blockchain technology in healthcare: a systematic review. PLoS ONE 17(4):3–28
49. Shahnaz A, Qamar U, Khalid A (2019) Using blockchain for electronic health records. IEEE Access 7:1–12
50. Sharma Y, Balamurugan B (2020) Preserving the privacy of electronic health records using blockchain. Procedia Comput Sci 173:2–8
51. Sharma V, Gupta A, Hasan NU, Shabaz M, Ofori I (2022) Blockchain in secure healthcare systems: state of the art, limitations, and future directions. Secur Commun Netw: 3–13. https://doi.org/10.1155/2022/9697545
52. Soltanisehat L, Alizadeh R, Hao H, Choo KKR (2020) Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: a systematic literature review. IEEE Trans Eng Manag: 2–12. https://doi.org/10.1109/TEM.2020.3013507
53. Su Q, Zhang R, Xue R, Li P (2020) Revocable attribute-based signature for blockchain-based healthcare system. IEEE Access 8:2–10
54. Tandon A, Dhir A, Islam N, Mäntymäki M (2020) Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda. Comput Ind 122:3–21
55. Toqeer AS, Alzahrani A, Jan S, Siddiqui MS, Nadeem A, Alghamdi T (2019) A comparative analysis of blockchain architecture and its applications: problems and recommendations. IEEE Access 7:1–18
56. Tripathi G, Ahad MA, Paiva S (2020) S2HS-A blockchain based approach for smart healthcare system in Healthcare. Elsevier 8(1):100391
57. Uddin Md A, Stranieri A, Gondal I, Balasubramanian V (2018) Continuous patient monitoring with a patient centric agent: a block architecture. IEEE Access 6:3–23
58. Usman M, Qamar U (2020) Secure electronic medical records storage and sharing using blockchain technology. Procedia Comput Sci 174:1–5
59. Wang S, Wang J, Wang X, Qiu T, Yuan Y, Ouyang L, Guo Y, Wang F-Y (2018) Blockchain-powered parallel healthcare systems based on the ACP approach. IEEE Trans Comput Social Syst 5(4):2–7
60. Wu S, Du J (2019) Electronic medical record security sharing model based on blockchain. Security and Privacy: 13–17. https://doi.org/10.1145/3309074.3309079
61. Wu H, Dwivedi AD, Srivastava G (2021) Security and privacy of patient information in medical systems based on blockchain technology. ACM Trans Multimedia Comput Commun Appl (TOMM) 17(2):3–16
62. Yaqoob I, Salah K, Jayaraman R, Al-Hammadi Y (2021) Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput Applic 34:11475–11490
63. Ji Y, Zhang J, Ma J, Yang C, Yao X (2018) BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems. J Med Syst 42(8):1–13
64. Yin T, Li Y, Ying Y, Luo Z (2021) Prevalence of comorbidity in chinese patients with COVID-19: systematic review and meta-analysis of risk factors. BMC Infect Dis 21(1):1–13
65. Zarour M, Ansari Md TJ, Alenezi M, Sarkar AK, Faizan M, Agrawal A, Kumar R, Khan RA (2020) Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records. IEEE Access 8:1–13
66. Zhang P, Schmidt DC, White J, Lenz G (2018) Blockchain technology use cases in healthcare. IEEE Adv Comput 111:3–35
67. Zhang C, Xu C, Sharif K, Zhu L (2021) Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications. Comput Stand Interfaces 77:4–8
68. Zhang R, Xue R, Liu L (2021) Security and privacy for healthcare blockchains. IEEE Trans Serv Comput 15(6):3668–3686
69. Zhang D, Wang S, Zhang Y, Zhang Q, Zhang Y (2022) A secure and privacy-preserving medical data sharing via consortium blockchain. Secur Commun Netw. https://doi.org/10.1155/2022/2759787

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.