frontiers | Frontiers in Public Health

TYPE Review
PUBLISHED 28 November 2023
DOI 10.3389/fpubh.2023.1272787

OPEN ACCESS

EDITED BY
Hongyu Miao,
Florida State University, United States

REVIEWED BY
Tsung-Ting Kuo,
University of California, San Diego,
United States
Mohammed Faisal,
Kuwait College of Science and Technology,
Kuwait

*CORRESPONDENCE
Fahad R. Albogamy
✉ f.alhammdani@tu.edu.sa

RECEIVED 04 August 2023
ACCEPTED 07 November 2023
PUBLISHED 28 November 2023

CITATION
Hasnain M, Albogamy FR, Alamri SS, Ghani I and Mehboob B (2023) The Hyperledger fabric as a Blockchain framework preserves the security of electronic health records.
Front. Public Health 11:1272787.
doi: 10.3389/fpubh.2023.1272787

The Hyperledger fabric as a Blockchain framework preserves the security of electronic health records

Muhammad Hasnain[1], Fahad R. Albogamy[2]*, Saeed S. Alamri[3], Imran Ghani[4] and Bilal Mehboob[5]

[1]Department of Computer Science, Lahore Leads University, Lahore, Pakistan, [2]Turabah University College, Computer Sciences Program, Taif University, Taif, Saudi Arabia, [3]Electrical Engineer Consultant, Jeddah, Saudi Arabia, [4]Department of Computer and Information Sciences, Virginia Military Institute, Lexington, KY, United States, [5]Department of Software Engineering, Superior University, Lahore, Pakistan

The Hyperledger Fabric (HF) framework is widely studied for securing electronic health records (EHRs) in the healthcare sector. Despite the various cross-domain blockchain technology (BCT) applications, little is known about the role of the HF framework in healthcare. The purpose of the systematic literature review (SLR) is to review the existing literature on the HF framework and its applications in healthcare. This SLR includes literature published between January 2015 and March 2023 in the ACM digital library, IEEE Xplore, SCOPUS, Springer, PubMed, and Google Scholar databases. Following the inclusion and exclusion criteria, a total of 57 articles emerged as eligible for this SLR. The HF framework was found to be useful in securing health records coming from the Internet of Medical Things (IoMT) and many other devices. The main causes behind using the HF framework were identified as privacy and security, integrity, traceability, and availability of health records. Additionally, storage issues with transactional data over the blockchain are reduced by the use of the HF framework. This SLR also highlights potential future research trends to ensure the high-level security of health records.

KEYWORDS

anonymity, Ethereum, blockchain, throughput, latency, health records

1 Introduction

Electronic health records (EHRs) have confidential and sensitive medical information that can be exchanged between healthcare providers, patients, and pharmacists. Clinical information such as past check-up reports, magnetic resonance imaging (MRI) reports, blood reports, and allergies are crucial to patients. This information is available only to patients, physicians, and other authorized users (1). To manage patient information, current EHR techniques are either cloud-based or distributed, which have diverse functionalities and also suffer from financial complications (2). Although EHRs have played a significant role in the healthcare industry, security and privacy concerns have not been comprehensively addressed. Literature reveals that many researchers have used the Ethereum blockchain and cloud-based systems to overcome these concerns (3).

Macdonald et al. (4) presented a comparison of five important blockchain platforms. Ethereum is one of these frameworks. IBM Open Blockchain (OBC), Intel Swatooth Lake, Eris, and BlockStream Side Chain Elements suffer from several limitations. Ethereum has been known as the leader in addressing several challenges, including scalability. Yu et al. (5), in a study, compared the applications of Ethereum and HF frameworks with MultiChain. However, these studies do not consider the applications of blockchain platforms in the healthcare industry (5, 6).

Ethereum and HF are two prominent BCT frameworks. They serve different purposes. The Ethereum platform provides certain features, including public (permission less) and private (permissioned) blockchains. For instance, HF as a decentralized framework is more suitable for permissioned blockchains and can execute distributed applications (Dapps). Both the Ethereum and HF frameworks provide impeccable features to users. However, the HF framework is considered more secure than Ethereum platform (7). Identity, confidentiality, performance, and scalability features of the HF framework are better compared to those of the Ethereum framework (8). Therefore, we choose the HF framework in this study and present its penetration in the healthcare industry.

Recent research explores the importance of hybrid clouds for preserving the security of EHRs (9). A biometric-based schema has been introduced to ensure that legitimate remote users can access the patients' EHRs (10). Another study shows contrasting results regarding trust, traceability, and security features in the healthcare industry. The BCT offers these services to its remote and distributed users (11). Tampered-proof EHRs are generated by using the BCT. The patient records are verifiable and protected from illegal modifications (12). Ancile, as a blockchain-based approach, uses smart contracts to provide access to obfuscated data and employs cryptography for data security (13).

There have been several reviews undertaken on the topic of BCT and its application in various sectors. The first review article focused on cloud-based, software-defined networks (SDNs) and blockchain-based proposed solutions for the security and privacy of medical information. Proposed approaches to challenges concerning the confidentiality and integrity of massive amounts of medical records were focused on in another review (14). Consequently, a scoping review concluded that provenance, data integrity, and interoperability were the main challenges that could be overcome to improve the performance of BCT in healthcare (15). Similarly, a recent review study highlighted the data security and leakage issues while using BCT on clouds (16). Most recently, a review article analyzed several applications of BCT in the data sharing of EHRs, IoT, and federated learning (17). A systematic literature review (SLR) was undertaken to present an overview of blockchain-based applications. The SLR has a very limited discussion about the HF framework (18). We argue that state-of-the-art approaches regarding the HF framework have received very limited attention, even in some reviews that assess the literature on data security and privacy of health records.

Eventually, the existing literature lacks a comprehensive review of the current blockchain-based approaches using the HF framework to ensure the data security and privacy of health records. Our contribution can be summarized as follows:

1. We present an overview of the state-of-the-art HF framework and its role in securing EHRs in healthcare.
2. We provide a privacy preservation mechanism on blockchain based on the existing literature.
3. We give an overview of the state-of-the-art privacy and security challenges of health data collected from IoMT.
4. We deduce future research directions and opportunities from the HF framework.

The remainder of the article is organized as follows: Section 2 is focused on the materials and methods used for conducting this SLR. Section 3 presents results and discussion on the literature about privacy and security challenges of IoMT data; the HF framework and its application in healthcare; and an analysis of data security and privacy challenges and performance metrics used in the literature. Section 4 provides a discussion on future research directions, while Section 5 gives a conclusion to the present study.

2 Materials and methods

A systematic review has been designed using "Preferred Reporting Items for Systematic Review and Meta-Analysis" (PRISMA) guidelines (19).

2.1 Search strategy

A search protocol was designed to search articles on topics from popular databases. A search string was proposed by using the appropriate search keywords and terms. A combination of search keywords and terms was used in the ACM digital library, IEEE Xplore, SCOPUS, Springer, PubMed, and Google Scholar databases. The search for literature on the topic was performed between January 2015 and March 2023. The year 2015 was chosen as the HF framework was first introduced as a permissioned blockchain in the year 2015 by the Linux Foundation (Inc., 2023). To promote the research results, search keywords were used that would help in answering the research questions. We used Boolean operators (AND and OR) for search strings as follows:

> (Hyperledger Fabric) OR (blockchain framework) AND (health records) OR (electronic health records) OR (patient records) AND (security) OR (privacy)
>
> (Hyperledger Fabric) OR (blockchain framework) AND (internet of medical things) OR (IoMT) AND (security) OR (privacy).

2.2 Study selection

The next step of the process was to perform the screening of the relevant studies. The screening process began with the examination of all studies collected from databases in the previous step. We developed a reference list with the help of Endnote X8.0 that was employed to eliminate duplicate studies. The rest of the duplicated documents were removed manually. Titles and abstracts of documents were assessed to determine their relevancy for the current systematic review. Two authors (M.H and I.G) performed the screening of studies using the inclusion and exclusion criteria (Figure 1). Thus, studies that were not clearly focused on the HF framework and its applications in healthcare regarding EHRs were excluded.

2.3 Inclusion and exclusion criteria

This systematic review followed the studies' inclusion and exclusion criteria as follows:

2.3.1 Inclusion criteria

a. Studies with sufficient discussion on the HF framework in the healthcare sector
b. Studies on HF framework and IoMT
c. Studies in English language
d. Studies with research findings on the topic

2.3.2 Exclusion criteria

a. Studies without the availability of full-length text
b. Studies with a focus on other than the HF framework
c. Studies with a focus on the HF framework in other than healthcare sectors
d. Duplicate studies
e. Editorials, short papers, prefaces, readers' letters, posters, and correspondence

2.4 Quality assessment

The quality assessment of the studies was performed according to the guidelines from Kitchenham and Charters (20). This allowed us to assess the relevance of studies to the research topics in this systematic review. Six randomly selected studies were subjected to the process of quality assessment and checked for effectiveness.

Table 1 shows the checklist of quality assessment criteria (QAC) used to qualitatively analyze the collected studies. This checklist was applied to all the studies identified in this systematic review. There were some studies that did not meet one or more of the above-given checklist items, and hence those studies were removed.

2.5 Data extraction

All studies that had passed the QAC had their data extracted to examine the completeness and accuracy of the information contained in each study. Data from studies were extracted, categorized, and stored in the Excel sheets. The categories of extracted data were as follows:

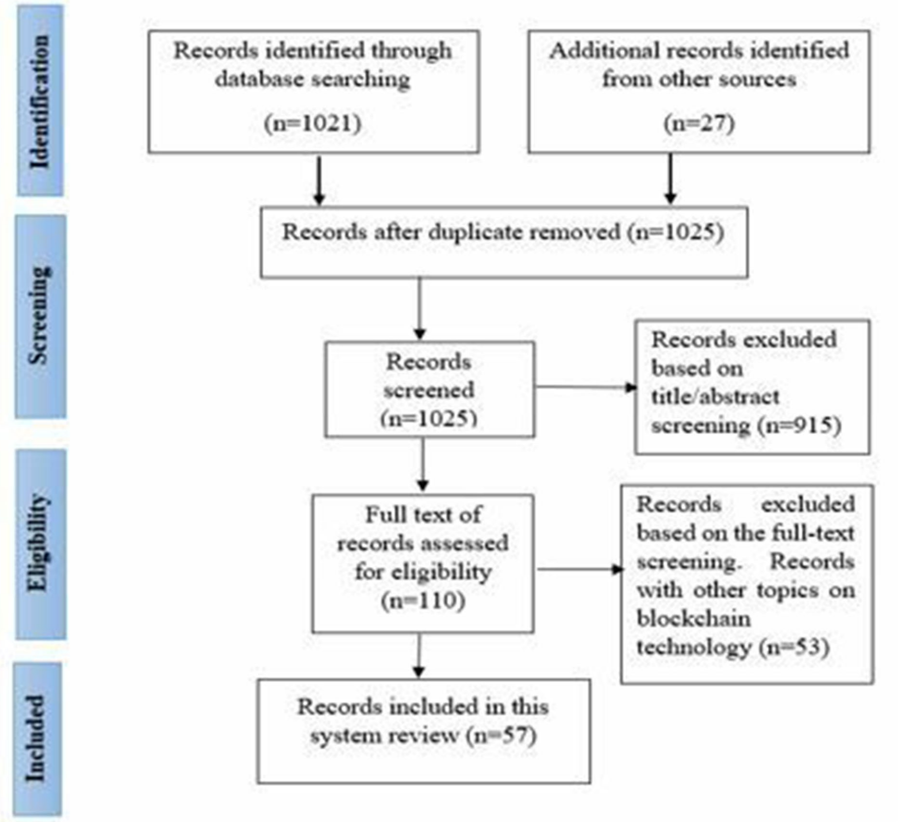
Identification
Screening
Eligibility
Included
Records identified through database searching (n=1021)
Additional records identified from other sources (n=27)
Records after duplicate removed (n=1025)
Records screened (n=1025)
Records excluded based on title/abstract screening (n=915)
Full text of records assessed for eligibility (n=110)
Records excluded based on the full-text screening. Records with other topics on blockchain technology (n=53)
Records included in this system review (n=57)

FIGURE 1
PRISMA flowchart diagram.

TABLE 1 Quality assessment criteria.

Stage#	Topic	Quality assessment criteria
1	HF framework	The study must focus on the use of HF framework or the applications of HF framework to the specific privacy and security problems of health records
2	Context	To elaborate and interpret results accurately, and enough context must be provided by each study.
3	Method	A study must have important details about the use of HF framework to address a specific problem regarding health records
4	Privacy and Security	A study must have enough information about the privacy and security issues of health records
5	Performance	A study must have performance analysis of the HF framework based proposed solutions, and it should be compared with other frameworks
6	Data acquisition	A study must provide the information about the acquired patients' data, its measurement and reporting.

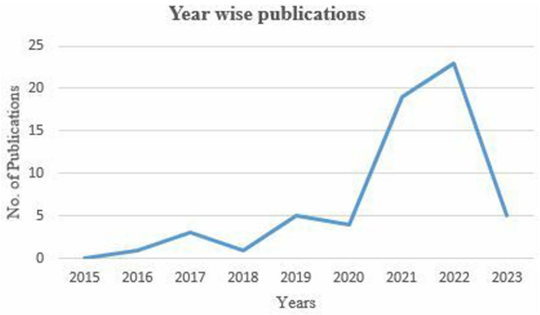

FIGURE 2
Publications over years (January 2015–March 2023).

2.6 Contextual information

Information about the purpose of study, problem addressed, and proposed solution is vital for a comprehensive understanding of the research

- **Pros and cons:** The information about the advantages and disadvantages of proposed solutions.
- **Qualitative data:** Final findings and conclusions from the included studies.
- **Quantitative data:** Data observed from experiments and their results. Data also include performance metrics.

3 Results and discussion

This section presents the results and their discussion.

3.1 Selection results

A total of 1,048 records were identified by using the initial keyword searches on the databases. Of them, 23 duplicate records were removed because they were either conference papers that did not comprehensively explain the research themes, results, and interpretations or short papers that had insufficient information about the topic. Next, 1,021 records were screened based on the title/abstract, following the studies' inclusion and exclusion criteria. After assessing the title/abstract of the remaining documents, they were reduced to 110 papers that were found eligible for the full-length text analysis. After reading the full-length text documents, 57 papers remained, providing the final set of articles included in this SLR.

Figure 2 presents the year-wise distribution of publications for the chosen period. It can be noticed that, as a result of the search process, including the paper's inclusion and exclusion criteria, no publications were found in 2015. From 2016 to 2020, this area of research did not receive much attention from scholars. However, Figure 2 shows an interesting point about the rapid increase in publications from January 2021 to February 2023. The increasing trend in published research indicates a significant surge during these years, suggesting that this area of research may become highly sought-after due to its widespread applications across various domains.

3.2 Privacy preservation mechanism on Blockchain

The privacy preservation mechanism is based on four aspects. The first aspect is the inclusion of symmetric cryptography and the separation of transaction information from on-chain records. The second aspect involved the digital certificate that ensures the legitimization of organizations on the blockchain. The third aspect is the design of separate multichannels for information distribution. The final aspect isolates the information privacy between the various organizations on the same channel. The HF framework performs two primary functions for data processing. Information processing is based on two criteria: the first criteria involve keeping confidential information and ledgers on a channel for people outside the channel; the second criteria set a scenario where information and ledgers are shared among organizations. Some of them will be able to see the transaction, while others can know about the occurrence of transactions and verify the authentication of transactions (28). However, the information security mechanism becomes weak when several medical institutes lack coordination in healthcare and consensus to determine how data should be utilized or shared when needed (29, 30). Hence, fragmentation problems exist that can be tackled by proposing and implementing a consensus mechanism. To some extent, the implementation of the HF framework has addressed the issue of low transaction efficiency when compared to conventional blockchain architectures such as Bitcoin and Ethereum, which rely on high-power or very complex algorithms to reach consensus (31). Furthermore, the sharing of prevalent health data becomes more challenging when it is shared among stakeholders in its various formats and standards (32). Thus, it becomes hard to examine, aggregate, and share health records in emergency situations.

3.3 Data privacy challenges of data collected from the internet of medical things (IoMT)

IoMT is the core application of IoT, which includes remote monitoring and diagnosing health records. Blockchain-enabled IoMT has been deployed to store data at hospital buildings for the provision of real-time monitoring of temperature, air quality, and environmental hygiene (33). Both passive (e.g., tags sensors) and active devices (robots) that can clean hospitals and disinfect can be used. Data collected from these devices can also be used for prescriptive and predictive analysis.

In the context of healthcare, several sensors, such as wearable and off-body sensors, perform sensing of the patient's body and periodically send health records to a personal digital assistant (PDA). This data passes through the cloud and medical servers, where it is assessed and a prescription is suggested using the patients' health records (21). Below, Table 2 shows the features of the studied literature on IoMT in healthcare.

We identified a few benchmark studies that employed IoMT with blockchain frameworks to make health records more secure and confidential. Innovative research on the integration of IoMT with the BCT is in its infancy stage. As listed in Table 2, studies contributed toward the proposal of approaches that employed only HF (21, 24, 25, 27), or in a combination with other frameworks (22–26). Most recent literature shows that the HF framework is mostly used in this emerging area of research. To assess the quality features of medical records, this SLR identified several quality features and relevant issues studied in the literature.

Figure 3 shows the results on the quality features of medical records. This SLR identified 11 quality features and relevant concerns about them. Security as a quality feature has been widely studied in the literature, followed by availability, integrity, privacy, interoperability, and scalability. The rest of the quality features and their issues have been poorly addressed in the literature. Trend analysis, as shown in Figure 3, indicates that security remained among the priority concerns of scholars. Although several issues regarding quality features were mainly focused on the literature, but proposed approaches suffer from certain challenges in their implementation in real-word scenarios. Implementation cost (21), effectiveness (23), performance evaluation (24, 26), and storage cost (25) are open issues in the emerging area of IoMT integrated with the blockchain frameworks.

3.4 Hyperledger fabric platform applications in healthcare

EHRs contain patients' sensitive information, such as name, address, medical history, social security, and insurance numbers. Patients' data have worth for stakeholders, and data exposure to the public has adverse consequences. To reduce the impact of patients' data exposure, the proposed approach used the HF framework to create and test various scenarios for data security (34). The HF framework complies with the General Data Protection Regulation (GDPR) and covers several areas. It has an edge over the other frameworks in preventing cyber-attacks and is best suited for healthcare applications compared to other frameworks. In the following Table 3, we present a summary of the proposed approaches that utilized the HF framework in the healthcare sector.

Most recent approaches using the HF framework have been proposed to secure the exchange of health records and ensure the confidentiality and integrity of records (40–42). The HF framework is focused on monitoring and tracking EHRs on a cloud server, as revealed in a study (43). Health records stored in HF are acquired by the federated server, where they are analyzed and pre-processed. The analyzed and pre-processed data are fed into a module for tailored recommendations, aiding physicians, nurses, and patients in countering health issues. Thus, the survival rate of patients can be increased using the proposed approach. Since the proposed approach integrates blockchain and federated learning, data from emerging COVID-19-like infections require an update to the proposed framework. Before this study, a tamper-resistant mobile health system was developed and evaluated using the HF framework that showed auditability and trusted computing (44). A mobile application using insomnia therapy data was referred to by HF as a blockchain network. This novel implementation led to improved accessibility and data transparency.

3.5 Data security and privacy challenges

This section presents an overview of the existing literature on the BCT-based HF framework and applications to resolve data privacy and security problems. Audio data stored in the cloud can be exposed if a decryption method is not implemented. When audio conversations between physicians and patients are stored on clouds, security concerns remain and data leakage can occur. To overcome this issue, a scheme using the homomorphic encryption library (HElib) was proposed and implemented on the "Contabo" cloud platform. The proposed scheme has the potential to increase the computation speed and performance if other open-source libraries such as PALASIDE, SEAL, and HEAAN are used in future studies (45). When the trust level of a cloud storing sensitive data decreases due to a single node failure, the cloud data provider becomes vulnerable to attacks and data theft (46). Table 4 below shows the summary of the studies relevant to the research topic.

We performed a comprehensive analysis of the pros and cons of the studied literature on the topic. The problems outlined in Table 4 are based on the choices of authors to use blockchain frameworks. Notably, the HF framework was frequently used in research. Out of 14 studies examined, 10 (or 72%) articles employed the HF framework, while 2 (or 14%) articles used the Ethereum framework, and the remaining 2 (or 14%) articles used a combination of two frameworks. Several advantages are brought by the HF framework compared to the Ethereum framework.

The majority of studies reported the performance aspects of their proposed frameworks. Metrics such as latency, throughput, and execution times were commonly used to highlight the better performance of the HF framework. As listed in the table above, there are core issues related to data privacy and security of health records, effectively prevent potential attacks. Critical systems in

TABLE 2 Main features of studied literature on IoMT.

Reference	Main contribution	Blockchain framework	Advantages	Limitations
Chenthara et al. (21)	Proposal and implementation of MedHypChain	HF	Authenticity, scalability, and interoperability of medical data	Proposed approach is complex and requires a higher cost for its implementation in real-world scenarios
Kumar and Chand (22)	Integration of blockchain with MoIT	HF, Quorum, and Corda	Privacy, security, and interoperability of medical data	Contact tracing, location sharing, and supply of medicine during the COVID-19 pandemic are the central issue
Li et al. (23)	Secure sharing of patient records	Not defined	Privacy and security breaches in Internet of Things (IoT). Safe transactions due to asymmetric cryptography technique.	The proposed approach is not efficient in measuring the exact location of patients.
Tiwari et al. (24)	Secure issue of IoT-based health monitoring system	HF	Data integrity, availability, security, and storage issues of transactions	The proposed approach is not evaluated based on performance metrics
Oikonomou et al. (25)	Incorporates machine learning-based anomaly detection in a health monitoring system	HF	A trusted ML-based anomaly detection works better compared to the existing systems	The proposed system is not evaluated based on communication, computational, and storage costs.
Pelekoudas-Oikonomou et al. (26)	Examines the edge learning and IMoT devices	HF and Ethereum	Several features such as fever detection, face mask detection, and in-home cough sound analysis of patients were analyzed	Accuracy of the proposed solution in real subjects is not performed
Rahman Hossain (27)	Efficient and secure transaction of health records	HF	Scalability, traceability, availability, integrity, and confidentiality of patients' records	Interoperability of the proposed system has not been tested with other IoT frameworks

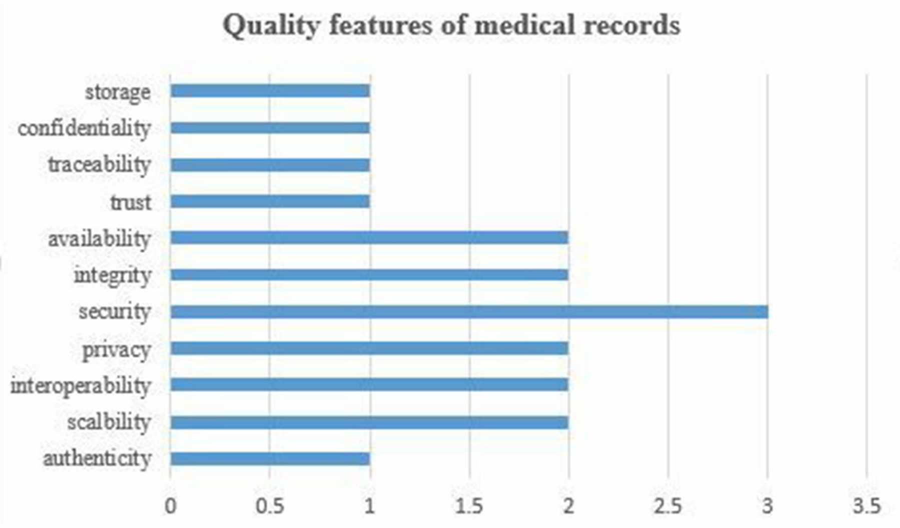

FIGURE 3
Quality features of medical records.

healthcare can be protected from external as well as internal attacks by using the applications of the HF framework in healthcare. Figure 4 below gives compelling evidence of the increasing role of the HF framework in tackling the privacy and security challenges of EMRs in the healthcare sector. Comparatively, the Ethereum framework indicates that only a few studies involved Ethereum either alone or in combination with the HF framework to address data security and privacy issues.

TABLE 3 Summary of the studied literature on the HF framework and their applications in the healthcare sector.

Reference	Study context	Advantages	Disadvantages
Antwi et al.(35)	Secure exchange of health records	Ensures integrity of health records	Not defined
Margheri et al.(36)	Clinical context of patients' data is limited	Reading and writing of patient records is in the order of milliseconds	Although throughput is increased without focusing on security
Bhavin et al.(37)	Security and privacy of stakeholders	Proposed approach prevents EHRs from quantum attacks	Proposed approach is not evaluated and compared with other frameworks
Kaur (38)	Security and storage health records	Efficient in securing and storing of health records	No comparison with the other types of blockchain framework
Hang et al. (39)	Data sharing, security and privacy challenges in clinical trial studies	Decentralized approach can cover data sharing, security, and privacy aspects	Several technical open challenges of BCT are not addressed

Handling EMR operations at hospitals using a decentralized platform is one of the primary requirements. This ensures that patients can receive safe and meaningful assistance from healthcare providers and services. The HF framework ensures low resource utilization and high transaction throughput (59). However, computer specifications and blockchain network size are main concerns that may be addressed by expanding the size of networks and deploying the proposed solutions on cloud architecture. However, migrating patients' data from hospitals to the cloud have its own threat vectors. Sometimes, devices securing medical records become targets of distributed denial-of-service (DDoS) and ransomware attacks (60). To overcome this issue, an interplanetary file system (IPFS) and blockchain can secure and improve data storage (61). Before the emergence of such modern technologies, medical records were either paper-based or stored in conventional databases, which faced issues of security and data duplication. Duplicity of medical records can be prevented by deploying IPFS on networks (Figure 5).

3.6 Performance metrics

The key aspect of the blockchain framework is the performance of the proposed solution based on the BCT. Various scholars employed the Hyperledger Caliper as a benchmark method while working on the implementation of BCT. Hyperledger Caliper can be used to generate reports on different performance metrics, including latency, transaction per second (TPS), and execution time (62). The aim of using these performance metrics was to highlight the importance of the HF framework for health records.

Table 5 demonstrates the key metrics and their values to analyze the proposed approaches. It has been pointed out in several studies that the latency of the proposed systems using the HF framework is always lower than the Proof of Work (PoW) protocol, while they exhibit higher throughput values (54). The HF framework-based privacy and security-preserving techniques show a higher level of confidentiality, traceability, and anonymity as compared to the existing approaches. Even these techniques (22) can handle thousands of concurrent transactions in emergency scenarios during the COVID-19 pandemic.

4 Future research trends

BCT, particularly the HF framework, has brought about several advantages. However, this technology does have a number of limitations regarding its applications for securing EHRs in the healthcare industry. These limitations can be deduced as future research directions and opportunities in the realm of blockchain frameworks and their applications in the healthcare sector. Before discussing the identified future research trends, we present a visual representation of the challenges in the figure below.

Ledger Fabric-based techniques show limitations in validating all transactions with backing nodes (47). The consensus algorithm of the HF framework can be optimized to carry a large amount of transactional data. Additionally, the protection of a backing node is another future direction that may be focused on enhancing the transaction speed of the blockchain.

- Ledger fabric technology has only implemented chain code on the fabric, and no broader applications have been proposed in the literature (48). Any user can verify the patients' records by triggering the chain code. A new user must seek permission to join the chain code. As the chain-code implementation is in its infancy phase, it requires real-world scenarios for testing and implementation.
- Identity Mixer (Idemix) technology, also called zero-knowledge proof (ZKP), provides privacy-preserving features including unsinkability and anonymity (39). However, it has technical limitations, which could be addressed in future releases of the framework.
- The learning rate of the proposed HF framework-based approach is the main limitation (50). This could be overcome by using hyper-parameter optimizers in future studies. Hyper-parameter optimizers are mostly used to solve detection issues using deep learning models (66). By combining the deep learning models with the blockchain, an immutable, secure, and decentralized environment can be enabled for sensitive data. To facilitate the training of deep learning models, hospital premises are a convenient and safe alternative to sharing with the cloud entity (67). This approach helps keep the data under the control of owners and hospital staff, thereby securing health records. Hospitals can be like smart building, and building information modeling (BIM), IoT, and BCTs can be combined to build hospitals such as smart buildings where health data can be stored and managed efficiently and securely (68). This idea could also be applied to other public and private buildings where the safety of humans and other assets, including data, is very significant.
- The punishment mechanism for organizations that submit information is not addressed (51). Therefore, a penalty function

TABLE 4 Key problems and their solution via the HF framework.

Study ID/Reference	Problem	Framework	Advantages	Disadvantages
Kumar and Chand (22)	Privacy preservation of patients' records	HF	Performance analysis using latency, throughput, and execution time is better than the existing approaches	Research shows limitations in showing the implementation of the framework other than HF
Babu et al.(40)	Health records' security	HF	Enhanced the security, access, scalability, and flexibility of healthcare applications	Blockchain-based security solution suffer higher overheads and regulation compliance
Bai et al. (47)	Sensitive data protection	HF and Ethereum	Higher throughput (≥1,000 TPS) using HF framework	Shows limitation in backing nodes to legitimate all transactions
Stamatellis et al. (48)	Identity identification	HF	Achieves higher throughput than 400 TPS	Only implemented chain-code on the fabric and no wider applications
Sammeta and Parthiban (49)	Exposure to medical records	HF	Provides anonymity and unlink-ability	Idemix technology has technical limitations
Zhao (50)	EMRs security	HF	Better approach than the existing approaches	Learning rate of the proposed approach is the main limitation
Pineda Rincón and Moreno-Sandoval (51)	Scheduling plan for emergency in the medical industry	HF	Optimized solution to prevent attacks while processing transactions	Punishment mechanism for organizations that submit information is not addressed
Hashim et al. (52)	EMRs' security	HF	Achieved better throughput and latency rates	No additional architectural designs were proposed to make architectural decisions
Shuaib et al. (53)	Interoperability issue	HF	Minimized the average latency between blockchain transfer	Blockchain still suffers scalability and security and needs to be optimized
Azbeg et al. (54)	Denial of service and security attacks on centralized health applications	HF	Better data integrity and security	Trade-off between latency and throughput is not addressed
Pericàs-Gornals (55)	Healthcare systems' susceptibility to security attacks	Ethereum	Better use of Remix IDE for the protection of patients' data	No comparison between Hyperledger Fabric and Ethereum framework has been provided in this study
Roehrs et al. (56)	High privacy requirements during COVID-19 pandemic	Ethereum	Control and validation of digital COVID-19 certificates	Filtering the requests for data sharing is not focused in the proposed research.
Zhong et al. (57)	Multiple health records are scattered without integration	HF and Ethereum	99% availability of blockchain-based healthcare applications	Limited in evaluating the content of health records. No use of images as image replicate and more space is used for their storage.
Ravi et al. (58)	Prevention of infected cases during COVID-19 pandemic	HF	Ensures the management of rapidly increasing infected cases	Hospital management is in the preliminary phase and rapid development may suffer quality of service issues

can be integrated into future versions of blockchain frameworks to align the proposed techniques with the original requirements.

- Blockchain-based security solutions often face higher overheads and regulatory compliance. A legislative organization may take several years to adopt the technology. The Data Protection Act of 1997 remained the same for this technology proposed in 2018. Cloud computing technology has easier compliance with the GDPR Act 2018, while the implementation of blockchain frameworks struggles with GDPR compliance due to the many resources required to scale up the system.
- Vulnerabilities around the blockchain system can become a major drawback of the system (69). For instance, a blockchain-based system can be attacked during implementation. Poorly written and outdated code leaves vulnerabilities open to exploitation in a decentralized autonomous organization. Vulnerable security attacks on the Hyperledger network can reduce the throughput of the system (70). Additionally, the latency rate increases when these denial-of=service (DoS) attacks are launched.
- A medical cloud platform has been proposed with its several applications in areas of medical institutions, nursing homes, and health monitoring. Compared to conventional big data analysis, it provides users' data privacy. Moreover, it can facilitate the exchange of encrypted messages related to health records, providing safe, low-cost, and high-quality solutions for smart medical records (71). However, problems with the proposed

medical cloud platform can be tackled in future studies. These problems include the efficiency verification of the proposed framework for large-scale applications in cases of real-time requirements. In future studies, the framework's design can be updated or optimized to improve its universality.

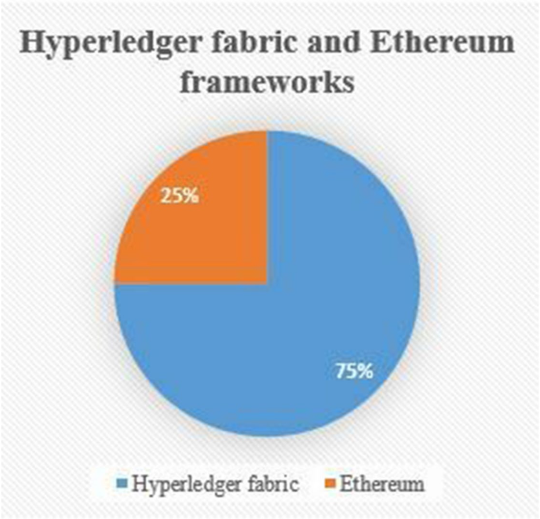

FIGURE 4
Comparison of the HF and Ethereum framework.

- Data storage is a big challenge for HF and similar blockchain frameworks (72). This challenge is more emphasized when massive IoMT data overloads the blockchain system (23). This challenge is more closely related to the scalability feature of a blockchain system (73). It can be overcome by using on-chain and off-chain data storage. An oracle approach must be undertaken to address the validation of data transferred onto the off-chain facility for each medical operation. Furthermore, tackling the redundant information arriving on blockchain storage and synchronizing the information may help reduce the overload on a blockchain system.
- An earlier study on the integration of artificial intelligence techniques with the BCT aimed to secure data coming from IoT devices (74). An emerging area of research involves the combination of IMoT and BTC with deep learning models (75) to optimize the proposed solutions using these technologies. Optimization is a big challenge for the proposed privacy and security-ensuring techniques (76). A blockchain-based deep learning framework has been presented with two levels of security and privacy (77). This framework is more suitable for various sub-domains in the healthcare sector. However, this framework has the potential to be integrated with the particle

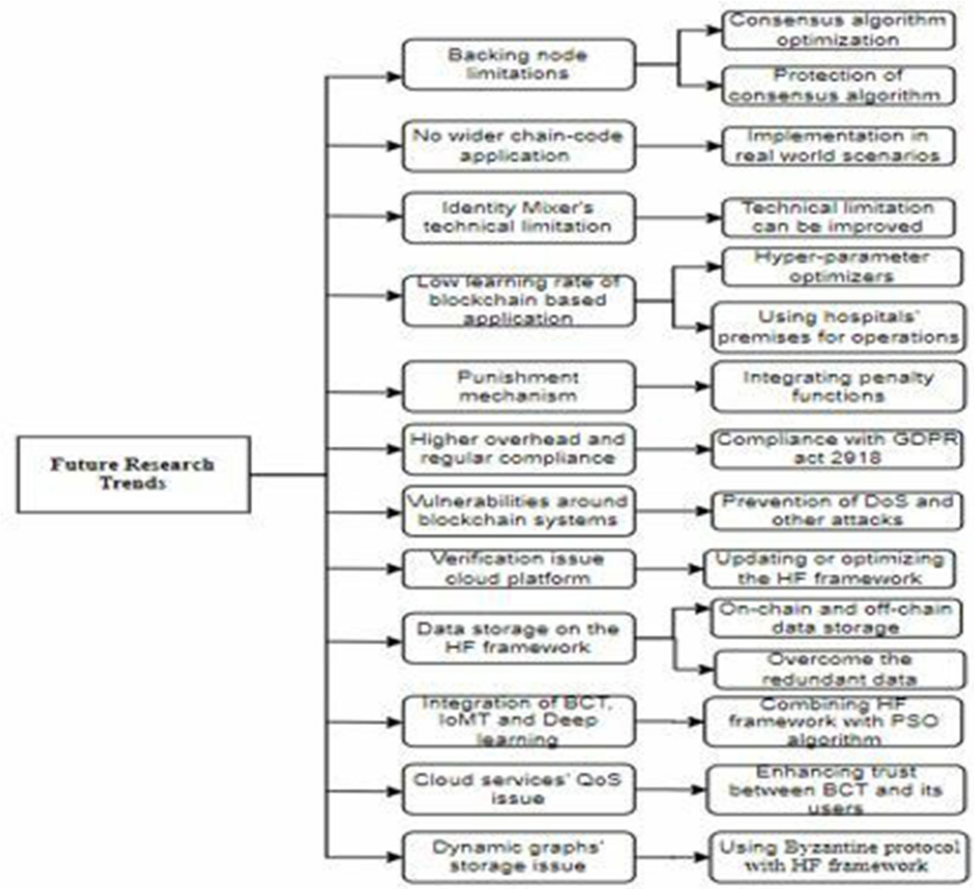
Future Research Trends
Backing node limitations
Consensus algorithm optimization
Protection of consensus algorithm
No wider chain-code application
Implementation in real world scenarios
Identity Mixer's technical limitation
Technical limitation can be improved
Low learning rate of blockchain based application
Hyper-parameter optimizers
Using hospitals' premises for operations
Punishment mechanism
Integrating penalty functions
Higher overhead and regular compliance
Compliance with GDPR act 2918
Vulnerabilities around blockchain systems
Prevention of DoS and other attacks
Verification issue cloud platform
Updating or optimizing the HF framework
Data storage on the HF framework
On-chain and off-chain data storage
Overcome the redundant data
Integration of BCT, IoMT and Deep learning
Combining HF framework with PSO algorithm
Cloud services' QoS issue
Enhancing trust between BCT and its users
Dynamic graphs' storage issue
Using Byzantine protocol with HF framework

FIGURE 5
Future research trends.

TABLE 5 Key performance metrics analysis.

Study Id/Reference	Name of application	No of users/submitted transactions	Latency (second)	Throughput
Kumar and Chand (22)	Query	10,000	12,067	461 TPS
	Invoke	10,000	12,987	152.1 TPS
Bai et al. (47)	Not defined	1,000	3.6	110 TPS
Stamatellis et al. (48)	Single computer	20,000 success rate	1.04	477 TPS
	Multiple virtual machines	20,000 success rate	1.25	345 TPS
Hashim et al. (52)	Not defined	1,000,000	100	Not defined
Azbeg et al. (54)	Add EHR	10,000	350	7 TPS
	Query EHR	10,000	124	19 TPS
Roehrs et al. (57)	Not defined	10,000	0.449	60 MB/s
Xia et al. (62)	Query batch	250	5.28	30.7
	Create batch (25 TPS)	150	16.30	4.4
	Query batch (25TPS)	250	5.6	34.1
Huang et al. (63)	Not defined	100	1286.53	Not defined
Khan et al. (64)	Select query (Ethereum)	500 records/tx (50,000 records)	35	100 TPS
	Ethereum	500	14 ms	800 Kbps
Xu (65)	Medical services	Not defined	87–95 ms	185 bytes

swarm optimization (PSO) algorithm and federated learning to enhance privacy and security in health records.
- Optimizing the quality of service (QoS) metrics is the greatest ambition of a cloud service provider and service users. Recent studies have been undertaken on the impacts of BCT on cloud services (76). The primary objective of the proposed approach is to enhance the scheduling and security of the methods used in delivering cloud services. This could be achieved when users show their trust in cloud services (78). Due to the transparency, anonymity, and autonomy features of BCT, this area can be extended in future studies. Trust in BCT is another research area (79), which can be undertaken to make the blockchain more trustworthy by activating its decentralization and privacy-preserving capabilities. This could be used to ensure the users' trust by protecting them from vulnerable attacks.
- Knowledge graphs can be dynamically created but cannot be stored on chains. It prevents the data from being tampered with (80). However, the use of the PoW algorithm on Ethereum makes the system vulnerable when all nodes simultaneously stop working. This problem can be addressed by shifting toward the HF framework and using the Byzantine protocol as a consensus algorithm (80, 81). Moreover, knowledge graph data, a popular data type, may be used to support authenticated queries, which can be easily manipulated on the blockchain.

5 Conclusion

This SLR presented an overview of the HF framework and its applications in securing health records. A SLR protocol as a research method was used to conduct the study. The findings of the SLR indicate that the use of the HF framework is still in its infancy and is gaining research attention from scholars in various domains, including IoT, AI, and cloud computing. Our SLR identified several challenges related to the privacy and security of health records from different sensors and devices. One of the significant challenges is the evaluation of the HF framework-based approaches in real-world scenarios. Major uses of the HF framework were identified as improving the latency, throughput, and execution time of proposed approaches while securing health records. Additionally, this SLR also presented several future research trends that could be explored in upcoming studies.

Author contributions

MH: Conceptualization, Writing – original draft, Software, Investigation. FA: Investigation, Methodology, Formal analysis, Supervision, Writing – review & editing. SA: Investigation, Methodology, Funding acquisition, Project administration, Validation, Writing – original draft. IG: Formal analysis, Supervision, Writing – review & editing, Resources, Visualization. BM: Project administration, Supervision, Writing – original draft.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Sharma Y, Balamurugan B. Preserving the privacy of electronic health records using blockchain. *Proc. Comp. Sci.* (2020) 173:171–80. doi: 10.1016/j.procs.2020.06.021

2. Dubovitskaya A., Xu Z., Ryu S., Schumacher M., Wang F. Secureand Trustable Electronic Medical Records Sharing Using Blockchain. Amia annual symposium proceedings, (2017). American Medical Informatics Association, 650.

3. Sabu S, Ramalingam H, Vishaka M, Swapna H, Hegde S. Implementation of a secure and privacy-aware E-health record and IoT data sharing using Blockchain. *Glob. Trans. Proc.* (2021) 2:429–33. doi: 10.1016/j.gltp.2021.08.033

4. Macdonald M, Liu-Thorrold L, Julien R. The Blockchain: a comparison of platforms and their uses beyond bitcoin. *Work Pap*. (2017):1–18. doi: 10.13140/RG.2.2.23274.52164

5. Yu H., Sun H., Wu D., Kuo T.T. Comparison of smart contract blockchains for healthcare applications. Amia annual symposium proceedings, (2019). American Medical Informatics Association, 1266.

6. Chowdhury MJM, Ferdous MS, Biswas K, Chowdhury N, Kayes A, Alazab M, et al. A comparative analysis of distributed ledger technology platforms. *IEEE Access*. (2019) 7:167930–43. doi: 10.1109/ACCESS.2019.2953729

7. Polge J, Robert J, Le Traon Y. Permissioned blockchain frameworks in the industry: a comparison. *ICT Express*. (2021) 7:229–33. doi: 10.1016/j.icte.2020.09.002

8. Corradini F., Marcelletti A., Morichetta A., Polini A., Re B., Scala E., et al. Model-driven engineering for multi-party business processes on multiple blockchains. Blockchain: Research and Applications, (2021) 2:100018. doi: 10.1016/j.bcra.2021.100018

9. Kanwal T, Anjum A, Malik SU, Khan A, Khan MA. Privacy preservation of electronic health records with adversarial attacks identification in hybrid cloud. *Comp. Stand. Int.* (2021) 78:103522. doi: 10.1016/j.csi.2021.103522

10. Hathaliya JJ, Tanwar S, Tyagi S, Kumar N. Securing electronics healthcare records in healthcare 4.0: a biometric-based approach. *Comp. Elect. Eng.* (2019) 76:398–410. doi: 10.1016/j.compeleceng.2019.04.017

11. Ahmad RW, Salah K, Jayaraman R, Yaqoob I, Ellahham S, Omar M. The role of blockchain technology in telehealth and telemedicine. *Int J Med Inform*. (2021) 148:104399. doi: 10.1016/j.ijmedinf.2021.104399

12. Zhang G, Yang Z, Liu W. Blockchain-based privacy preserving e-health system for healthcare data in cloud. *Comput Netw*. (2022) 203:108586. doi: 10.1016/j.comnet.2021.108586

13. Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain Cities Soc*. (2018) 39:283–97. doi: 10.1016/j.scs.2018.02.014

14. Jin H, Luo Y, Li P, Mathew J. A review of secure and privacy-preserving medical data sharing. *IEEE Access*. (2019) 7:61656–69. doi: 10.1109/ACCESS.2019.2916503

15. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences—a scoping review. *Int J Med Inform*. (2020) 134:104040. doi: 10.1016/j.ijmedinf.2019.104040

16. Saha A, Amin R, Kunal S, Vollala S, Dwivedi SK. Review on "Blockchain technology based medical healthcare system with privacy issues". *Sec Priv*. (2019) 2:e83. doi: 10.1002/spy2.83

17. Ogundokun RO, Misra S, Maskeliunas R, Damasevicius R. A review on federated learning and machine learning approaches: categorization, application areas, and Blockchain technology. *Information*. (2022) 13:263. doi: 10.3390/info13050263

18. Xi P, Zhang X, Wang L, Liu W, Peng S. A review of Blockchain-based secure sharing of healthcare data. *Appl Sci*. (2022) 12:7912. doi: 10.3390/app12157912

19. Moher D, Shamseer L, Clarke M, Ghersi D, Liberati A, Petticrew M, et al. Preferred reporting items for systematic review and meta-analysis protocols (Prisma-P) 2015 statement. *Syst Rev*. (2015) 4:1–9. doi: 10.1186/2046-4053-4-1

20. Kitchenham B., Charters S. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE 2007-001, Keele University and Durham University Joint Report.

21. Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z. Healthchain: a novel framework on privacy preservation of electronic health records using blockchain technology. *PLoS One*. (2020) 15:e0243043. doi: 10.1371/journal.pone.0243043

22. Kumar M, Chand S. MedHypChain: a patient-centered interoperability hyperledger-based medical healthcare system: regulation in Covid-19 pandemic. *J Netw Comput Appl*. (2021) 179:102975. doi: 10.1016/j.jnca.2021.102975

23. Li X, Tao B, Dai H-N, Imran M, Wan D, Li D. Is blockchain for internet of medical things a panacea for Covid-19 pandemic? *Perv. Mob. Comp.* (2021) 75:101434. doi: 10.1016/j.pmcj.2021.101434

24. Tiwari S, Dhanda N, Dev H. A real time secured medical management system based on blockchain and internet of things. *Measurement*. (2023) 25:100630. doi: 10.1016/j.measen.2022.100630

25. Oikonomou FP, Ribeiro J, Mantas G, Bastos JMC, Rodriguez J. A hyperledger fabric-based blockchain architecture to secure IoT-based health monitoring systems In: *2021 IEEE international Mediterranean conference on communications and networking (MeditCom)*. Athens, Greece: IEEE (2021). 186–90. doi: 10.1109/MeditCom49071.2021.9647521

26. Pelekoudas-Oikonomou F, Zachos G, Papaioannou M, De Ree M, Ribeiro JC, Mantas G, et al. Blockchain-based security mechanisms for IOMT edge networks in Iomt-based healthcare monitoring systems. *Sensors*. (2022) 22:2449. doi: 10.3390/s22072449

27. Rahman MA, Hossain MS. An internet-of-medical-things-enabled edge computing framework for tackling Covid-19. *IEEE Internet Things J*. (2021) 8:15847–54. doi: 10.1109/JIOT.2021.3051080

28. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics Inform*. (2019) 36:55–81. doi: 10.1016/j.tele.2018.11.006

29. Ma C, Kong X, Lan Q, Zhou Z. The privacy protection mechanism of Hyperledger fabric and its application in supply chain finance. *Cybersecurity*. (2019) 2:1–9. doi: 10.1186/s42400-019-0022-2

30. Uddin M. Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *Int J Pharm*. (2021) 597:120235. doi: 10.1016/j.ijpharm.2021.120235

31. Al-Sumaidaee G, Alkhudary R, Zilic Z, Swidan A. Performance analysis of a private blockchain network built on Hyperledger fabric for healthcare. *Inf Process Manag*. (2023) 60:103160. doi: 10.1016/j.ipm.2022.103160

32. Chen Z, Xu W, Wang B, Yu H. A blockchain-based preserving and sharing system for medical data privacy. *Futur Gener Comput Syst*. (2021) 124:338–50. doi: 10.1016/j.future.2021.05.023

33. Dai H-N, Imran M, Haider N. Blockchain-enabled internet of medical things to combat Covid-19. *IEEE Internet Things Magazine*. (2020) 3:52–7. doi: 10.1109/IOTM.0001.2000087

34. Zaabar B., Cheikhrouhou O., Ammi M., Awad A. I., Abid M. Secure and privacy-aware blockchain-based remote patient monitoring system for internet of healthcare things. 2021 17th international conference on wireless and mobile computing, networking and communications (WiMob). (2021) Bologna, Italy: IEEE. 200–205. doi: 10.1109/WiMob52687.2021.9606362

35. Antwi M, Adnane A, Ahmad F, Hussain R, Ur Rehman MH, Kerrache CA. The case of hyperledger fabric as a blockchain solution for healthcare applications. *Blockchain*. (2021) 2:100012

36. Margheri A, Masi M, Miladi A, Sassone V, Rosenzweig J. Decentralised provenance for healthcare data. *Int J Med Inform*. (2020) 141:104197. doi: 10.1016/j.ijmedinf.2020.104197

37. Bhavin M, Tanwar S, Sharma N, Tyagi S, Kumar N. Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications. *J Inf Secur Appl*. (2021) 56:102673. doi: 10.1016/j.jisa.2020.102673

38. Kaur J, Rani R, Kalra N. Blockchain-based framework for secured storage, sharing, and querying of electronic healthcare records. *Concurr Comput*. (2021) 33:e6369. doi: 10.1002/cpe.6369

39. Hang L, Chen C, Zhang L, Yang J. Blockchain for applications of clinical trials: taxonomy, challenges, and future directions. *IET Commun*. (2022) 16:2371–93. doi: 10.1049/cmu2.12488

40. Babu ES, Yadav BRN, Nikhath AK, Nayak SR, Alnumay W. Medi blocks: secure exchanging of electronic health records (Ehrs) using trust-based blockchain network with privacy concerns. *Clust Comput*. (2022) 26:1–28.

41. Elrahman SA, Alluhaidan AS. Blockchain technology and IoT-edge framework for sharing healthcare services. *Soft Comput*. (2021) 25:13753–77. doi: 10.1007/s00500-021-06041-4

42. Lavanya M, Kavitha V. Secure tamper-resistant electronic health record transaction in cloud system via Blockchain. *Wirel Pers Commun*. (2022) 124:607–32. doi: 10.1007/s11277-021-09374-3

43. Hai T, Zhou J, Srividhya S, Jain SK, Young P, Agrawal S. Bvflemr: an integrated federated learning and blockchain technology for cloud-based medical records recommendation system. *J Cloud Comp*. (2022) 11:22. doi: 10.1186/s13677-022-00294-6

44. Ichikawa D, Kashiyama M, Ueno T. Tamper-resistant mobile health using blockchain technology. *JMIR Mhealth Uhealth*. (2017) 5:e7938

45. Iqbal Y, Tahir S, Tahir H, Khan F, Saeed S, Almuhaideb AM, et al. A novel homomorphic approach for preserving privacy of patient data in telemedicine. *Sensors*. (2022) 22:4432. doi: 10.3390/s22124432

46. Chen C-L, Yang J, Tsaur W-J, Weng W, Wu C-M, Wei X. Enterprise data sharing with privacy-preserved based on hyperledger fabric blockchain in Iiot's application. *Sensors*. (2022) 22:1146. doi: 10.3390/s22031146

47. Bai T, Hu Y, He J, Fan H, An Z. Health-zkidm: a healthcare identity system based on fabric Blockchain and zero-knowledge proof. *Sensors*. (2022) 22:7716. doi: 10.3390/s22207716

48. Stamatellis C, Papadopoulos P, Pitropakis N, Katsikas S, Buchanan WJ. A privacy-preserving healthcare framework using hyperledger fabric. *Sensors*. (2020) 20:6587. doi: 10.3390/s20226587

49. Sammeta N, Parthiban L. Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model. *Comp Intellig Syst*. (2022) 8:625–40. doi: 10.1007/s40747-021-00549-w

50. Zhao Y. Design of Optimal Scheduling Model for emergency medical supplies by Blockchain technology. *J Healthcare Eng*. (2022) 2022. doi: 10.1155/2022/4608761

51. Pineda Rincón EA, Moreno-Sandoval LG. Design of an Architecture Contributing to the protection and privacy of the data associated with the electronic health record. *Information*. (2021) 12:313. doi: 10.3390/info12080313

52. Hashim F, Shuaib K, Sallabi F. Connected Blockchain federations for sharing electronic health records. *Cryptography*. (2022) 6:47. doi: 10.3390/cryptography6030047

53. Shuaib K, Abdella J, Sallabi F, Serhani MA. Secure decentralized electronic health records sharing system based on blockchains. *J King Saud Univ-Comp Inf Sci*. (2022) 34:5045–58. doi: 10.1016/j.jksuci.2021.05.002

54. Azbeg K, Ouchetto O, Andaloussi SJ. Block med care: a healthcare system based on IoT, Blockchain and Ipfs for data management security. *Egypt Inform J*. (2022) 23:329–43. doi: 10.1016/j.eij.2022.02.004

55. Pericàs-Gornals R, Mut-Puigserver M, Payeras-Capellà MM. Highly private blockchain-based management system for digital Covid-19 certificates. *Int J Inf Secur*. (2022) 21:1069–90. doi: 10.1007/s10207-022-00598-3

56. Roehrs A, Da Costa CA, Da Rosa Righi R, Da Silva VF, Goldim JR, Schmidt DC. Analyzing the performance of a blockchain-based personal health record implementation. *J Biomed Inform*. (2019) 92:103140. doi: 10.1016/j.jbi.2019.103140

57. Zhong B, Gao H, Ding L, Wang Y. A Blockchain-based life-cycle environmental management framework for hospitals in the Covid-19 context. *Engineering*. (2022). doi: 10.1016/j.eng.2022.06.024

58. Ravi D, Ramachandran S, Vignesh R, Falmari VR, Brindha M. Privacy preserving transparent supply chain management through Hyperledger fabric. *Blockchain*. (2022) 3:100072. doi: 10.1016/j.bcra.2022.100072

59. Hang L, Choi E, Kim D-H. A novel Emr integrity management based on a medical blockchain platform in hospital. *Electronics*. (2019) 8:467. doi: 10.3390/electronics8040467

60. Kumar S, Bharti AK, Amin R. Decentralized secure storage of medical records using Blockchain and Ipfs: a comparative analysis with future directions. *Sec Priv*. (2021) 4:e162. doi: 10.1002/spy2.162

61. Shahnaz A, Qamar U, Khalid A. Using blockchain for electronic health records. *IEEE Access*. (2019) 7:147782–95. doi: 10.1109/ACCESS.2019.2946373

62. Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. Medshare: trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*. (2017) 5:14757–67. doi: 10.1109/ACCESS.2017.2730843

63. Huang J, Qi YW, Asghar MR, Meads A, Tu YC. Sharing medical data using a blockchain-based secure Ehr system for New Zealand. *Iet Blockchain*. (2022) 2:13–28. doi: 10.1049/blc2.12012

64. Khan AA, Shaikh ZA, Baitenova L, Mutaliyeva L, Moiseev N, Mikhaylov A, et al. QoS-ledger: smart contracts and metaheuristic for secure quality-of-service and cost-efficient scheduling of medical-data processing. *Electronics*. (2021) 10:3083. doi: 10.3390/electronics10243083

65. Xu J. Are blockchains immune to all malicious attacks? *Financ Innov*. (2016) 2:5. doi: 10.1186/s40854-016-0046-5

66. Xin R, Liu H, Chen P, Zhao Z. Robust and accurate performance anomaly detection and prediction for cloud applications: a novel ensemble learning-based framework. *J Cloud Comp*. (2023) 12:1–16. doi: 10.1186/s13677-022-00383-6

67. Rahman MA, Hossain MS, Islam MS, Alrajeh NA, Muhammad G. Secure and provenance enhanced internet of health things framework: a blockchain managed federated learning approach. *IEEE Access*. (2020) 8:205071–87. doi: 10.1109/ACCESS.2020.3037474

68. Lokshina IV, Greguš M, Thomas WL. Application of integrated building information modeling, IoT and blockchain technologies in system design of a smart building. *Proc Comp Sci*. (2019) 160:497–502. doi: 10.1016/j.procs.2019.11.058

69. Zhao J, Wang W, Wang D, Wang X, Mu C. Pmhe: a wearable medical sensor assisted framework for health care based on blockchain and privacy computing. *Journal of Cloud Computing*. (2022) 11:1–17.

70. Andola N, Gogoi M, Venkatesan S, Verma S. Vulnerabilities on hyperledger fabric. *Perv Mob Comp*. (2019) 59:101050. doi: 10.1016/j.pmcj.2019.101050

71. Alzubi OA, Alzubi JA, Shankar K, Gupta D. Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in internet of things. *Trans Emerg Telecommun Technol*. (2021) 32:e4360. doi: 10.1002/ett.4360

72. Mohananthini N, Ananth C, Parvees M. Secured different Disciplinaries in electronic medical record based on watermarking and consortium Blockchain technology. *KSII Trans Internet Inform Syst*. (2022) 16:947–71. doi: 10.3837/tiis.2022.03.011

73. Chen L, Zhang X, Sun Z. Scalable Blockchain storage model based on DHT and IPFS. *KSII Transact Internet and Inform Syst*. (2022) 16:2286–2304. doi: 10.3837/tiis.2022.07.009

74. Veeramakali T, Siva R, Sivakumar B, Senthil Mahesh P, Krishnaraj N. An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. *J Supercomput*. (2021) 77:9576–96. doi: 10.1007/s11227-021-03637-3

75. Roshanzamir M, Darbandy MT, Roshanzamir M, Alizadehsani R, Shoeibi A, Ahmadian D. Swarm intelligence in internet of medical things In: *2022 IEEE 10th Jubilee International conference on computational cybernetics and cyber-medical systems (ICCC)*. Reykjavík, Iceland: IEEE (2022). 000371–6.

76. Almaiah MA, Ali A, Hajjej F, Pasha MF, Alohali MA. A lightweight hybrid deep learning privacy preserving model for fc-based industrial internet of medical things. *Sensors*. (2022) 22:2112. doi: 10.3390/s22062112

77. Babu GJS, Baskar M. Application of blockchain methodology in secure task scheduling in cloud environment. *Adv Eng Softw*. (2022) 172:103175. doi: 10.1016/j.advengsoft.2022.103175

78. Kochovski P, Gec S, Stankovski V, Bajec M, Drobintsev PD. Trust management in a blockchain based fog computing platform with trustless smart oracles. *Futur Gener Comput Syst*. (2019) 101:747–59. doi: 10.1016/j.future.2019.07.030

79. Teng Y. What does it mean to trust blockchain technology? *Metaphilosophy*. (2023) 54:145–60. doi: 10.1111/meta.12596

80. Kshirsagar M., Vaidya G., Yao Y., Kasar S., Ryan C. (2023). Sensible: sequestered aNd SynergIstic Blockchain ecosystem. *Engineering Reports*. 5:e12586. doi: 10.1002/eng2.12586

81. Amazon Web Services, Inc. (2023). *What is Hyperlegder fabric?* Available at: https://aws.amazon.com/blockchain/what-is-hyperledger-fabric/#:~:text=Hyperledger%20Fabric%20is%20an%20open,2015%20by%20The%20Linux%20Foundation