Healthcare Analytics 3 (2023) 100192

Contents lists available at ScienceDirect

Healthcare Analytics

journal homepage: www.elsevier.com/locate/health

A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine

Madhuri Hiwale [a], Rahee Walambe [a,b], Vidyasagar Potdar [c], Ketan Kotecha [a,b,*]

[a] Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune 412115, India
[b] Symbiosis Centre for Applied Artificial Intelligence (SCAAI), Symbiosis International (Deemed University), Pune 412115, India
[c] Blockchain R&D Lab, School of Management and Marketing, Curtin University, Perth 6107, Australia

ARTICLE INFO

Keywords:
Blockchain
Federated learning
Privacy-preserving methods
Healthcare
Telemedicine

ABSTRACT

The unexpected and rapid spread of the COVID-19 pandemic has amplified the acceptance of remote healthcare systems such as telemedicine. Telemedicine effectively provides remote communication, better treatment recommendation, and personalized treatment on demand. It has emerged as the possible future of medicine. From a privacy perspective, secure storage, preservation, and controlled access to health data with consent are the main challenges to the effective deployment of telemedicine. It is paramount to fully overcome these challenges to integrate the telemedicine system into healthcare. In this regard, emerging technologies such as blockchain and federated learning have enormous potential to strengthen the telemedicine system. These technologies help enhance the overall healthcare standard when applied in an integrated way. The primary aim of this study is to perform a systematic literature review of previous research on privacy-preserving methods deployed with blockchain and federated learning for telemedicine. This study provides an in-depth qualitative analysis of relevant studies based on the architecture, privacy mechanisms, and machine learning methods used for data storage, access, and analytics. The survey allows the integration of blockchain and federated learning technologies with suitable privacy techniques to design a secure, trustworthy, and accurate telemedicine model with a privacy guarantee.

1. Introduction

The healthcare sector is crucial for the overall development of any nation around the globe. Historically, the primary goal of healthcare was to cure patients using medical aids. As a result, there was no emphasis on data privacy and security [1]. However, in the digital era, data privacy, secure data storage, exchange, and controlled accessibility of sensitive health data have become the primary concerns for the current healthcare system. As a result, of late, traditional healthcare systems have shown radical growth and eagerness to adopt new and advanced technologies in the pursuit of transferring to modern healthcare systems. Even with the acceptance of the latest technologies, healthcare systems still face numerous challenges related to data ownership, privacy, security, and integrity.

Since 2020, the COVID-19 pandemic has started a new virtual healthcare era. One promising technology in this regard is telemedicine or a remote healthcare system. The speedy global outbreak of COVID-19 has accelerated the demand for telemedicine technology-based solutions to a new height that too on an urgent basis [2]. Telemedicine or a remote healthcare system enhances the ability of all stakeholders to treat multiple patients without face-to-face communication. It establishes a healthier environment to boost the overall standard of healthcare [3]. In the case of infectious disease, telemedicine plays a vital role in improving the health outcomes of patient adherence, hospital readmission, and mortality [4]. Telemedicine effectively eliminates the geographical distance barrier to facilitate proper medical treatment and clinical health care at a low cost to remote patients [5].

Despite the many potential advantages, there are still issues with the widespread adoption of the telemedicine system. Currently, all the stakeholders involved in the telemedicine system rely on centralized storage to exchange health data. Centralized data storage causes many problems, such as data breaches, lack of transparency, and trust, high cost, lack of patient-centric approach, and data privacy [6]. Therefore, any cloud-based solution must address data privacy and security concerns effectively.

One of the core concerns telemedicine faces is ensuring data privacy and security of exchanged data. A set of legal, economic, ethical, and technical problems are also related to health data privacy. Due to privacy concerns, stringent laws and regulations such as Health Insurance Portability and Accountability Act (HIPAA) [7] and General

* Corresponding author at: Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune 412115, India.
E-mail addresses: madhuri.hiwale.phd2020@sitpune.edu.in (M. Hiwale), rahee.walambe@sitpune.edu.in (R. Walambe), Vidyasagar.Potdar@cbs.curtin.edu.au (V. Potdar), director@sitpune.edu.in (K. Kotecha).

https://doi.org/10.1016/j.health.2023.100192
Received 25 February 2023; Received in revised form 18 April 2023; Accepted 30 April 2023

Data Protection Regulation (GDPR) [8] restrict hospitals from sharing sensitive data across healthcare institutes from building data analytics models. Due to these data privacy concerns, novel technologies such as the Internet of Things (IoT), Blockchain, Artificial Intelligence (AI), Machine Learning (ML), Big Data, and newer technology such as Federated learning are incorporated into healthcare to provide appropriate solutions [9].

Since 2018, tremendous growth has been observed in adopting blockchain in healthcare [10]. The blockchain is an immutable, append-only distributed data structure. The acceptance of blockchain has increased as it provides a convenient means to overcome the current challenges of remote healthcare applications and enhance health data transparency, security, trustworthiness, integrity, and authenticity [11]. Estonia's public healthcare system is one of the best examples demonstrating the potential of blockchain application in the healthcare industry. Since 2011, Estonia has deployed *Guardtime* blockchain technology for the complete implementation of its public digital health infrastructure [12]. Transactional data privacy is one of the challenging issues associated with blockchain technology [1]. Blockchain technology alone cannot guarantee advanced data privacy protection [13]. Thus, it is necessary to incorporate appropriate privacy-preserving mechanisms with blockchain technology to enhance its adaptability in the healthcare industry [14,15].

There exists a good amount of literature on the blockchain. In [16], the authors have highlighted the need for exhaustive work to understand the effectiveness of the blockchain in healthcare. The authors in [17] have covered the blockchain's privacy challenges and privacy-preserving mechanisms. Similarly, in [18], the authors have discussed the challenges and provided a detailed research plan for using blockchain in healthcare. Finally, in [19], the authors have discussed blockchain-based use cases and their current status and open issues. This study categorized privacy challenges and provided the taxonomy of existing privacy mechanisms employed with blockchain.

Due to stringent privacy regulations, healthcare organizations are often unwilling to share sensitive data with other entities. However, cross-institute health data is necessary to develop a highly generalized global model. Another emerging technology that can play a vital role in healthcare data analytics in such a situation is Federated Learning (FL) [20]. Google introduced the federated learning approach in 2016. In this approach, the client never uploads the raw data to the coordinating or central server. The model updates are uploaded to the coordinating server [21]. Federated learning facilitates entities to create a collaborative global model without transferring raw data to third parties [22,23]. In global health emergencies, collaborative research and cooperation between multiple healthcare organizations and research institutes are vital to improving health outcomes. Federated learning can make this research collaboration and cooperation possible [24]. However, naive federated learning systems are susceptible to accountability and privacy threats, such as model poisoning attacks [25,26].

Few studies have discussed the recent progress and challenges of federated learning technology for healthcare informatics [27]. In [20], the authors have outlined future directions and challenges in federated learning. In [28], the authors provide detailed categorization of federated learning according to different aspects such as data distribution, privacy mechanisms, architectures, and machine learning models. In [29], the authors provide a detailed classification of security and privacy threats in federated learning. They discussed the trade-off between various privacy-preserving approaches and identified ways to enhance privacy in federated learning.

Federated learning and blockchain techniques are promising in health data analytics and management. Fig. 1 highlights the benefits of integrating blockchain and federated learning for different use cases. Concerning the potential of these technologies, many studies have integrated these technologies for various use cases. However, very few research studies have performed a systematic literature review on this research area [30]. In [31], the authors systematically discussed the challenges and benefits of incorporating blockchain and federated learning. They have focused on three challenges, i.e., incentivization, decentralization, and membership selection. In [32], the authors have discussed the challenges and opportunities in designing a blockchain-enabled federated framework for the mobile-edge computing domain. In [33], the authors presented a systematic review that explored the current state and the future research opportunity to integrate Artificial Intelligence (AI) and blockchain. The authors have expressed how integration may create product innovation and economic value in industries. In [34], the authors have presented an overview of combining machine learning and blockchain for healthcare.

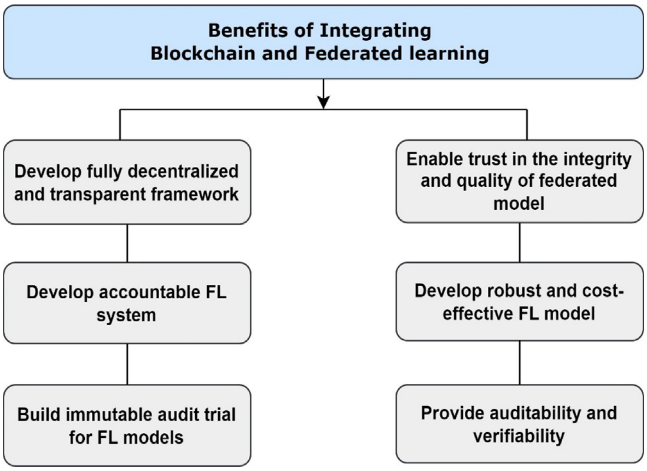

Benefits of Integrating
Blockchain and Federated learning
Develop fully decentralized and transparent framework
Develop accountable FL system
Build immutable audit trial for FL models
Enable trust in the integrity and quality of federated model
Develop robust and cost-effective FL model
Provide auditability and verifiability

Fig. 1. Benefits of integrating blockchain with federated learning for different usecases.

Despite the scholarly contribution in the form of the existing studies, there is still a need to provide an in-depth analysis of the literature that focuses on integrating blockchain and federated learning to develop trustworthy and privacy-oriented remote healthcare applications. In the current remote healthcare era, integrating these emerging technologies into the telemedicine system could facilitate secure storage, exchange, and utilization of patient data, predict patient outcomes in a trustworthy manner and improve overall care quality [34,35]. However, there is a need to understand the current state-of-the-art research to develop reliable and privacy-oriented healthcare applications in alliance with federated learning and blockchain technology. For this reason, this survey discusses the potential benefits of blockchain and federated learning in improving the overall care quality of the telemedicine system. Data privacy is a core concern in remote healthcare applications. In this regard, this survey emphasizes privacy issues/attacks associated with blockchain and federated learning. The main focus is to review various privacy-preserving mechanisms deployed with these technologies to develop privacy-preserving healthcare applications.

In summary, the main contribution of this research study is three-fold.

- To comprehensively review the relevant literature on blockchain and federated learning for developing trustworthy healthcare applications.
- To conduct an investigation and comparative analysis of various privacy-preserving mechanisms deployed on a blockchain and federated learning to develop privacy-oriented data models in the future.
- To discuss and analyze the previous studies about the convergence of blockchain and federated learning techniques for the privacy-preservation of healthcare systems.

The rest of the survey is structured as follows: Section 2 describes the research methodology used to retrieve the relevant literature. Section 3 includes a comprehensive literature analysis that discusses the

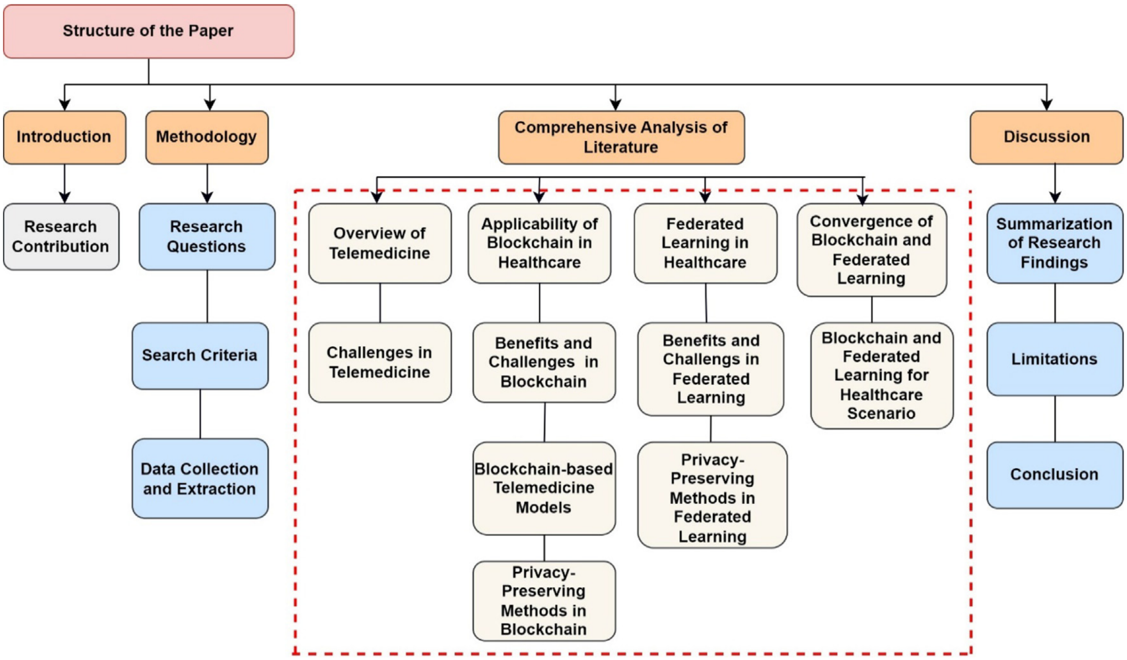

Structure of the Paper
Introduction
Methodology
Comprehensive Analysis of Literature
Discussion
Research Contribution
Research Questions
Search Criteria
Data Collection and Extraction
Overview of Telemedicine
Challenges in Telemedicine
Applicability of Blockchain in Healthcare
Benefits and Challenges in Blockchain
Blockchain-based Telemedicine Models
Privacy-Preserving Methods in Blockchain
Federated Learning in Healthcare
Benefits and Challengs in Federated Learning
Privacy-Preserving Methods in Federated Learning
Convergence of Blockchain and Federated Learning
Blockchain and Federated Learning for Healthcare Scenario
Summarization of Research Findings
Limitations
Conclusion

Fig. 2. Thematic structure of paper.

overview of telemedicine, blockchain, and federated learning. It covers blockchain-based telemedicine models, privacy-preserving methods used with blockchain, and federated learning for healthcare scenarios. Section 4 provides the discussion and main findings of our study. Finally, Section 5 discusses the future opportunity to integrate blockchain and federated learning technologies for developing robust healthcare applications. Fig. 2 depicts the thematic structure of the paper.

2. Research methodology

This section represents the adopted research methodology to identify and analyze relevant literature regarding our research objectives and the topic. We have adopted Kitchenham and Charters method to perform a systematic literature review [36,37]. The Kitchenham and Charters guidelines are composed of three parts. The first part is planning the review; the main aim of this part is to define the research objectives of the Systematic Literature Review (SLR). The second part is to identify well-defined research questions. The main objective of this part is to refine the research questions into specific search queries to facilitate subject analysis and pinpoint the further research direction. The last part is responsible for reporting the results of the review.

This method helps define the research objectives, formulate the topic-specific research questions, and define topic-specific inclusion and exclusion selection criteria. These criteria help to find the documents necessary to develop privacy-preserving healthcare applications integrating blockchain and federated learning. Table 1 highlights the objective-based research questions.

2.1. Search criteria

This study used academic data repositories such as Scopus, Web of Science, ScienceDirect, ArXiv, and IEEE Xplore to retrieve and analyze the relevant literature to include a wide range of publications. These documents helped us understand the state-of-the-art ongoing research in the respective research area. We have used well-defined search queries/keywords to systematically search the relevant research papers to address our formulated research questions. We have used the keywords such as (‘Blockchain AND Healthcare’), (‘Blockchain AND Telemedicine’), (‘Federated learning AND Healthcare’), (‘Federated learning AND Telemedicine’), (‘Blockchain AND Federated learning’), (‘Blockchain AND Federated learning AND Healthcare’), and (‘Blockchain AND Federated learning AND Telemedicine’) to get the basic idea about federated learning and blockchain for developing privacy-preserving healthcare applications such as telemedicine. There was considerable overlap in the research studies found using the initial level search queries. Therefore, this review used several analytical functions and filters provided by databases to extract valuable insight from the data.

2.2. Data collection

In the initial search, we included only journal articles, conference papers, and early access articles written in English. The role of federated machine learning and blockchain in remote healthcare is still emerging, and it is one of the fastest-growing research fields. Due to this, we have included early access articles and ArXiv preprints in our search, as the latest research results may be available as preprints that are valuable to review. The blockchain was launched by Satoshi Nakamoto in 2009, so we have included the documents published after 2009 for blockchain, and for federated learning, we reviewed 2017 onwards documents.

2.3. Inclusion and exclusion criteria

After retrieving the documents from the respective databases based on our search criteria, the next step was screening the relevant documents. For this study, we have screened only journal articles, conference papers, and early-access articles for further in-depth qualitative analysis. The documents were screened based on the title and abstract, and the irrelevant and duplicate copies were removed. Afterward, all the relevant documents were selected, and the references of those documents were also scanned to identify additional significant documents (Forward and Reverse Snowballing). This study excluded the research studies that were found irrelevant and were not peer-reviewed. Several research studies were also excluded from the qualitative analysis process because they were not related to the healthcare domain.

Overall, this review includes the relevant research papers to address our key research questions and excludes those that did not fit our

Table 1
Proposed research questions and main research objectives.

Number	Research questions (RQ)	Research objectives
RQ1	What are the current challenges faced by remote healthcare systems (telemedicine)?	To understand the current workflow of the telemedicine system along with its benefits and challenges.
RQ2	How do Blockchain-based solutions improve the accessibility and security of data in the current healthcare domain?	To know blockchain's applicability, benefits, and challenges for developing healthcare applications.
RQ3	Which privacy-preserving methods are incorporated with blockchain to develop privacy-preserving healthcare applications?	To explore the existing privacy-preserving methods deployed on blockchain for healthcare applications.
RQ4	How does federated machine learning provide better privacy-preservation of patient data over traditional machine learning techniques?	To explore the existing research studies incorporating federated machine learning techniques for the healthcare scenario.
RQ5	Which are different privacy-preserving techniques that develop potential privacy in the federated machine learning domain?	To review the various privacy-preserving methods used in federated machine learning.
RQ6	How are the convergence of blockchain and federated machine learning beneficial to facilitate privacy preservation in the healthcare domain?	The main aim is emphasizing the benefits of integrating blockchain and federated machine learning in healthcare.

Table 2
Search criteria for inclusion and exclusion.

Selection criteria	Databases
Inclusion	Topic-specific peer-reviewed articles, conference papers, and early-access articles
Exclusion	Non-English articles, book chapters, articles addressing general features, and articles irrelevant to addressing research objectives

Table 3
Quality assessment criteria.

Number	Criteria	Score If the criteria are satisfied

1	The research studies must be relevant to address our formulated research questions.	Yes = 1
		No = 0

2	The research studies must focus on the advantages and issues of blockchain in the healthcare domain.	Yes = 1
		No = 0

3	The research studies must discuss privacy-preserving mechanisms used with blockchain in healthcare.	Yes = 1
		No = 0

4	The research studies must design blockchain-based architecture for telemedicine systems.	Yes = 1
		No = 0

5	The research studies must discuss the use of federated learning in healthcare.	Yes = 1
		No = 0

6	The research studies must focus on how blockchain and federated learning work together.	Yes = 1
		No = 0

7	The research studies must focus on the convergence of federated learning and blockchain for the healthcare domain.	Yes = 1
		No = 0

research questions. As a result, 158 research studies were selected for further in-depth analysis. Table 2 depicts the search criteria used for inclusion and exclusion.

2.4. Quality assessment criteria

Quality assessment criteria help evaluate significant research works to answer objective-based research questions. The research works satisfying the desired criteria were selected for further qualitative analysis. Table 3 depicts the quality assessment criteria.

2.5. Data extraction

The data from selected research studies and reports which meet our inclusion criteria were considered for qualitative analysis. Based on the thematic map, the content was categorized and summarized in the following sections and subsections.

3. Comprehensive analysis of the literature

This section provides the analysis of formulated research questions. This section reviews the research papers that show the applicability of blockchain and federated learning for telemedicine systems.

3.1. RQ1: Overview and challenges of telemedicine

Telemedicine is a remote healthcare service. According to the World Health Organization (WHO), telemedicine facilitates the exchange of medical information between geographically separate locations by healthcare providers using information and communication technologies (ICT) for better treatment, prevention, and diagnosis of diseases [3]. This virtual platform establishes remote coordination between patients and healthcare providers and has excellent potential to increase data access and care quality [38]. It creates a safe environment to provide on-demand and personalized treatment quickly. Fig. 3 shows the classic architecture of a telemedicine system.

During the COVID-19 crisis, the adoption of telemedicine systems has shown exponential growth around the globe [39]. According to the global telemedicine market report, a telemedicine system is an efficient solution that facilitates the effective management of COVID-19 [40]. For example- The Italian government launched family-centered telemedicine to control the spread of coronavirus. This developed system provided immediate telemedicine support to children and their families to reduce the risk of psychological burnout and emotional distress during the lockdown phase [41].

Currently, the telemedicine system depends on the Cloud Service Provider (CSP) to gather and transfer healthcare data [42]. Few state-of-art systems rely on the cloud server, such as cyber–physical systems [43] and health monitoring systems designed for stroke management [44]. These system collects health information using medical sensors and stores it on the cloud server [45,46]. This centralized health data storage may result in data breaches, and patients may not trust the telehealth system. Centralized storage allows cybercriminals to launch attacks targeting data integrity, privacy, and confidentiality. Due to this, the patient may feel insecure about storing their personal health information on the cloud server. So, privacy and security are challenging issues in cloud-based service platforms [6]. Another issue in remote healthcare is the secure and authorized control of health data between multiple healthcare providers [47]. Once the data is collected in the cloud, the patient loses control over their data. The patient is unaware of who is accessing and sharing their health records. There is a lack of a data ownership approach and patient-centric access control mechanisms [48]. In such cases, security and easy accessibility of data become critical concerns. Adopting advanced technologies with telemedicine systems is essential to enhance their adaptability in healthcare. Fig. 4 depicts the current challenges faced by the cloud-based telemedicine system.

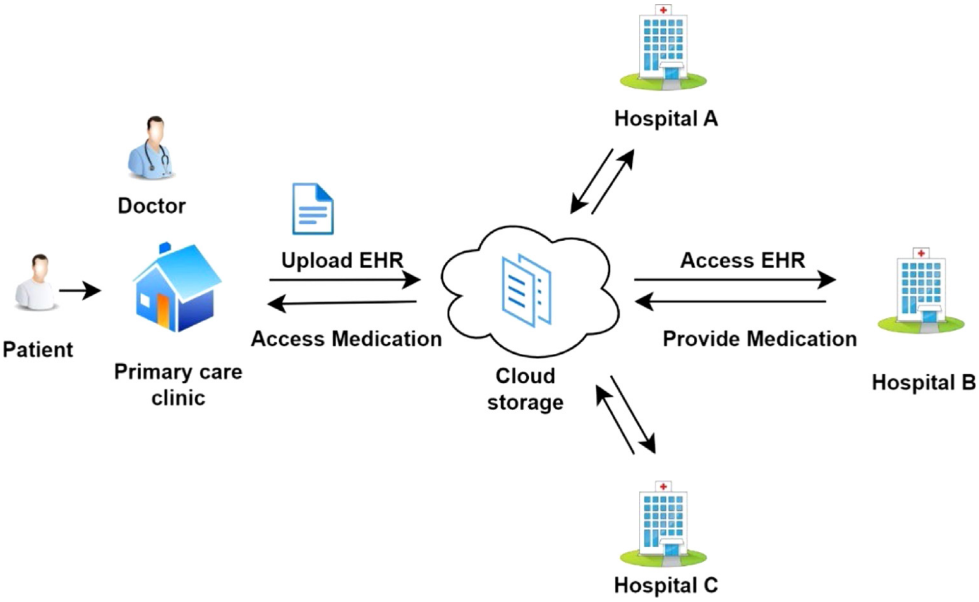


Fig. 3. Architecture of cloud-based telemedicine system.

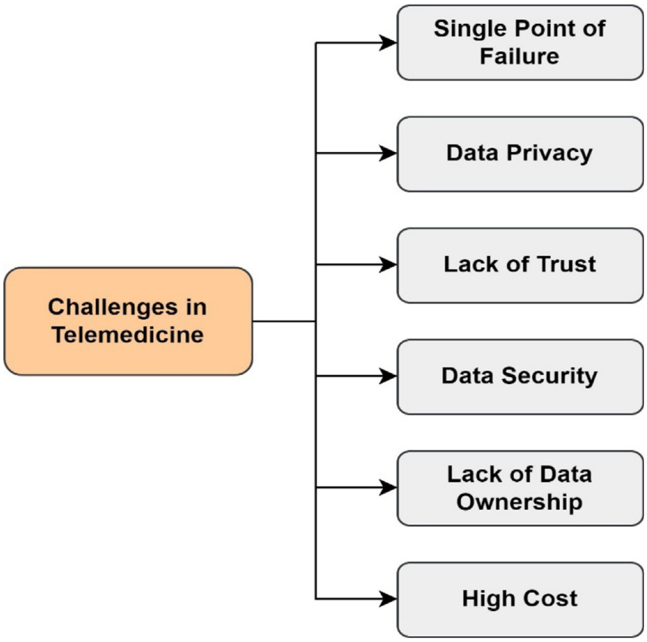


Fig. 4. Challenges in telemedicine system.

Table 4
Advantages and challenges of blockchain.

Sr. no	Advantages	Challenges
1	Decentralized	Scalability
2	Immutable	Low interoperability
3	Transparency and Traceability	Privacy loss
4	Data integrity and confidentiality	High energy consumption
5	Authorized data access	Lack of technical skill
6	Trust	Writing efficient smart contracts

3.2. RQ2: Blockchain-based healthcare solutions

The blockchain is an immutable, append-only distributed data structure. Initially, its applicability was mostly limited to financial sectors in the form of Bitcoin (a cryptocurrency) application [49]. Recently, owing to its inherited potential, it has shown substantial adaptability in various other sectors [12]. In healthcare, blockchain has a huge potential to create a technological revolution [50]. The decentralized and immutable nature of blockchain helps to create a transparent healthcare workflow that allows patients to know how their health data is shared and accessed in the network [16,51]. In addition, blockchain uses a cryptographic algorithm to ensure data security [52]. From the healthcare perspective, blockchain's data provenances, accountability, availability, and robustness are notable benefits to facilitating effective health record management [53]. Blockchain enables efficient, immutable, and scalable data sharing from various sources, for example, EHR, clinical trials, genomic databases, and IoT data from multiple sensors [54].

3.2.1. Advantages and challenges of blockchain in healthcare

Few research studies have explored blockchain's key advantages and challenges to healthcare applications [55]. Table 4 highlights the advantages and problems associated with blockchain technology.

• Advantages of blockchain: Blockchain is a highly effective technology for storing and retrieving health data [56]. One of the fascinating features of blockchain is that it eliminates the dependency on centralized third-party. Blockchain offers a viable data transmission and storage solution owing to its immutability, decentralized, and transparency features. The decentralization quality helps create a transparent healthcare workflow that lets patients know how their health data is shared and accessed in the network. Blockchain technology facilitates secure storage and workflow of health data. It provides authorized data access and ensures data integrity and confidentiality.

The blockchain-based system is resilient against health data corruption and data losses. With the transparency and data availability feature, blockchain creates a trustworthy atmosphere for distributed healthcare applications. The health data saved on the blockchain are time-stamped, cryptographically encrypted, and appended chronologically. It helps ensure health data security [16]. With well-designed smart contracts, blockchain facilitates health data ownership [57].

• Challenges of blockchain: A few specific challenges make healthcare organizations hesitant to adopt blockchain technology. These challenges mainly include scalability, advanced-level privacy, and interoperability issues [58]. Scalability and interoperability are highly discussed technical threats faced by blockchain technology. Scalability is the core problem with the current blockchain implementation [15].

Table 5
Summarization of relevant studies implementing blockchain-based healthcare solutions.

Study references	Telemedicine-related problems addressed in the study	Remarks
[56,65,72,73]	1. Single Point of Failure, 2. Need to rely on third-party.	Blockchain eliminates third-party dependency with its decentralized and distributed nature and provides efficient and trustworthy health data sharing.
[74,75]	2. Lack of trust 3. Lack of transparency in health data exchange.	Blockchain is an immutable, append-only ledger, and the transactions stored within it are a time-stamp that helps to ensure trust and transparency in health data exchange.
[47,67,76–79]	4. Lack of patient-centric data exchange	Smart contracts help to provide patient-centric access to health data, secure data access, and ensure reliable data sharing between health services.
[66,80–84]	5. Insecure data sharing 6. Lack of efficient health data management	Blockchain enables secure and efficient data sharing between patients and health stakeholders. Blockchain improves health data sharing with its distributed, immutable, and transparency features.
[85–89]	7. Lack of authorized access and authentication to exchange health data with health authorities.	The smart contract provides authorized access and secure interaction between healthcare stakeholders and medical applications.
[58,90–92]	8. Interoperability and security issues in EHR management system.	Blockchain with smart contract logic helps to provide personalized and effective EHR data management.
[93,94]	9. Lack of accountability 10. Limited data provenance	With traceability, immutability blockchain guarantees data provenance. With smart contract logic, it provides a robust accountable system.

To solve the scalability problem in [59], the authors have used off-chain storage protocols such as IPFS (InterPlanetary File system). This protocol is the content-addressed, peer-to-peer distributed file structure that helps to access and store health data easily. Integrating IPFS with blockchain helps protect health data and build a robust healthcare system [60].

In the case of the Proof of Work (POW)-based public blockchain, slow transaction speed, high energy consumption, and potential privacy are noticeable threats. Initial installation costs and the lack of essential technical skills by health stakeholders to operate blockchain technology are other issues identified in the previous studies [61]. Writing efficient smart contracts is also a challenging task. Another challenge is the usability of handling complicated healthcare systems. Since health professionals are not technically sound as IT professionals to manage complex healthcare systems. These are the hurdles that blockchain technology needs to overcome before being significantly adopted in healthcare applications.

Recently, several research studies have developed blockchain-based healthcare models to improve the current EHR system [62–64]. Few research studies focus on patient-centric data transfer among multiple healthcare stakeholders [65–67]. Some studies focus on developing a blockchain-based model to overcome privacy and security issues in digital healthcare systems [68–71]. In the following subsection, we have divided the existing studies based on the issues they handled and how blockchain helps deal with them. Table 5 shows the summarization of relevant studies that implemented blockchain-based models.

• Single point of failure: Traditional healthcare systems depend on a centralized authority to store and access health data. The centralized data storage raises issues such as single point of failure and data breaches. To address the existing problems of the traditional healthcare system, many authors have highlighted the benefits of blockchain-based architectures for effective data management [80–82]. In [65], the authors have proposed a novel blockchain-based decentralized framework that eliminates the need to depend on any third party to facilitate secure and patient-centric communication between patients and hospitals. In [80], the authors have described the potential features of blockchain in alliance with personalized mobile-based applications to facilitate trustworthy data exchange.

• Lack of patient-centric approach: Few researchers implemented owner-centric blockchains in healthcare applications. They have developed a blockchain-based patient-centric EHR exchange framework to improvise the current healthcare workflow [66]. For example, In [66], the authors have developed a blockchain-based patient-centric data-sharing model for diabetes patients. They have created multi-signature contracts to control and share access to health data. In [67], the authors have proposed a patient-centric blockchain model. In this architecture, patient-centric smart contracts are designed to grant clinicians consent to use patient data. The EHR data is in the local database, whereas the blockchain contains metadata. Similarly, in [95], the authors have developed dual blockchain platforms: one permissioned blockchain owned by the patient and another consortium blockchain by the health authority.

• Insecure data sharing and management: The framework designed by [47] provides a blockchain-based method to protect medical data exchange. The developed framework guarantees the integrity and trustworthiness of Medical Resonance Imaging (MRI) distributed through various hospital networks. In [84], the authors have proposed BlockHR, a blockchain-based health data management framework to provide better data management and access between patients and healthcare providers. The data retrieval is 20 times faster for BlockHR than the client–server approach. In this regard, the authors in [96] have proposed Hyperledger Fabric and NDN, i.e., Naming Data Networking Protocols, to provide secure health monitoring.

• Lack of access control mechanism: In current healthcare services, EHR is always present in multiple hospitals and accessed by a centralized authority. There is a need to build access control frameworks to protect and secure EHR sharing. In [74], the authors have proposed a public and private blockchain-based framework. Blockchain maintains the interaction between external and internal entities. To solve the issues related to access control, the authors [89] have designed a blockchain-based architecture that uses a Genetic algorithm and Discrete Wavelet Transform to ensure authorized access control and optimize the system performance.

• Interoperability: In [90], the authors have addressed the interoperability and regulatory compliance issues in home-based healthcare applications. They have incorporated a blockchain and edge computing platform called CORD (Central Office Rearchitected as a Data center) to enable authorized communication between patients and home-based applications. In [58], the authors have emphasized the blockchain's significance in overcoming security and interoperability issues of EHR management in eHealth. Similarly, in [92], to improve interoperability and reliability, authors have built a consortium blockchain-based health data sharing architecture called SHAREChain. This architecture incorporates two standards: Cross-Enterprise Document Sharing

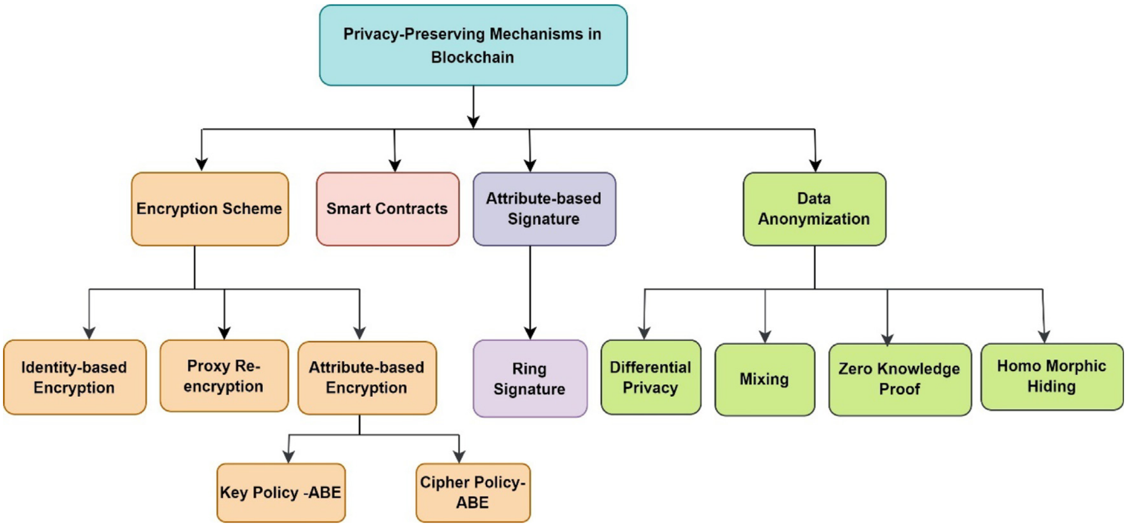


Fig. 5. Privacy-preserving mechanisms deployed on blockchain.

(XDS) and another is Fast Healthcare Interoperable Resource (FHIR). Similarly, in [91], the authors used the FHIR standard to manage health data in an interoperable manner. They have proposed permissioned blockchain-based architecture with Proof of Authority (PoA) technology that facilitates patient-centric data exchange.

• Limited data provenance: Traceability, transparency, and immutability are vital features of blockchain that make it appealing in various applications. Due to these features, In [93], The authors have incorporated blockchain within the public healthcare system to enhance accountability and transparency in public healthcare. In [94], the authors have presented a blockchain-based architecture to improve drug traceability in a decentralized manner. With smart contract logic, blockchain guarantees data provenance and provides a robust end-to-end trace system for the drug supply chain [75].

3.2.2. Blockchain-based telemedicine solutions

Few research studies have developed a blockchain-based telemedicine model to build robust and patient-centric systems for reliable communication between patients and healthcare stakeholders [77,97]. In [98], the authors have designed a blockchain-based patient-centric platform for telemedicine called HapiChain. The framework secures the workflow between patients and doctors for teleconsultation services. In [99], the authors have proposed a blockchain-based telemedical laboratory. They have used the Internet of Medical Things (IoMT) and the cloud to provide better treatment. The article [80] focused on patient location privacy to design a telecare medical information system. The authors have proposed a blockchain-based scheme for protecting patient locations using a Merkle tree and Order-Preserving Encryption (OPE). Merkel tree uses a one-way hash function to construct a binary tree, verifying data integrity.

One of the fascinating applications of telemedicine is telesurgery. In the case of telesurgery or remote surgery, uninterrupted and authorized data access is a crucial part. For this purpose, in [100], the authors have proposed blockchain-based telesurgery. This system uses Interplanetary File System (IPFS) to resolve data storage cost issues and provide higher throughput and lower latency for data distribution.

Similarly, in [101], the authors have proposed a telesurgery framework that uses public blockchain-based smart contracts to develop trust between various entities, such as patients and surgeons. This framework uses IPFS for data storage cost-effectiveness. They have incorporated artificial learning techniques to train the surgical robot. In [102], the authors have developed an interoperable telesurgery framework. This framework uses a permissioned blockchain to design trusted digital agreements to facilitating secure coordination between surgeons, patients, and caregivers. Each surgeon has a copy of complete surgical procedure information executed by all surgeons this transparent and trustworthy.

Teledermatology is considered the well-known application of telemedicine. In [103], the authors have applied a blockchain-based approach to a teledermatology e-health platform. This platform includes smart contracts that manage communication and access between multiple stakeholders. Table 6 summarizes the relevant research studies implementing blockchain-based telemedicine solutions.

3.3. RQ3: Blockchain-based privacy-preserving mechanisms

There are various privacy-preserving mechanisms deployed on the blockchain that helps to ensure data privacy and secure accessibility [110]. This section covers encryption schemes, cryptography, smart contracts, and data anonymization methods.

3.3.1. Privacy issues in blockchain

Privacy is a primary concern for the integration of blockchain in healthcare applications. Even the Bitcoin blockchain has proven illusory in guaranteeing strong privacy as it fails to provide complete anonymity [17,111]. Data privacy and confidentiality are challenging issues for blockchain. In a blockchain, private keys are employed to sign transactions; therefore, these keys are critical for the user's privacy [17]. Several mechanisms, such as encryption-based or anonymization, can improve blockchain privacy and data confidentiality. Most blockchains are publicly accessible databases exposed to various potential privacy challenges, such as on-chain data privacy, transaction likability, malicious smart contracts, and privacy regulation compliance. These potential privacy issues may hinder the wide adaptability of blockchain in the healthcare industry [112]. There are two issues of privacy: identity privacy and transactional privacy [113]. Identity privacy means maintaining the patient's private identity and not mixing it with the transactions. Transactional privacy is a challenging issue faced by blockchain. Some measures, such as pseudonyms, are insufficient to ensure transactional privacy [19]. Therefore, several mechanisms, such as zero-knowledge proof and mixing, were proposed to improve privacy.

3.3.2. Privacy-preserving mechanisms in blockchain

Recently, privacy-preserving data exchange has gained tremendous attention in healthcare scenarios, especially for effective data analytics. For this reason, in previous research studies, several privacy methods have been used with blockchain to strengthen privacy. Fig. 5 shows well-known privacy-preserving mechanisms deployed on

Table 6
Summarization of relevant studies implementing blockchain-based telemedicine solutions.

Study references	Blockchain platforms	Privacy mechanisms	Remarks
Abugabah et al., [97]	Ethereum	–	This study presented a transparent and tamper-proof telemedicine framework to ensure data integrity.
Guo et al., [42]	Consortium	Attribute-based encryption	A privacy-preserving blockchain-based telemedicine system with authorized access policies is proposed.
Gupta et al. [102]	Hyperledger fabric	Cryptographic method	An inter-operable blockchain-based telesurgery framework to provide secure access mechanisms
Kordestani et al., [98]	Ethereum	–	A patient-centric blockchain-based framework to provide reliable and secure teleconsultation service.
Nusrat et al., [5]	Private blockchain	–	A blockchain-based telemedicine model to ensure security and patient-centric accessibility of health data.
Celesti et al., [99]	Ethereum	Data anonymization	A secure telemedical laboratory to form a virtual hospital team incorporating blockchain and the cloud to provide better treatment.
Juyal et al., [104]	Consortium	Asymmetric encryption	A privacy-preserving decentralized skin surveillance system provides secure medical data storage and access.
Mannaro et al., [103]	Ethereum	–	A patient-centric blockchain-based teledermatology consultation platform to improve care quality.
Gupta et al. [100]	Ethereum	–	A blockchain and IPFS-based patient-centric Tele surgical remote service framework to improve the accuracy and quality of the system.
Ji et al. [105]	Hyperledger fabric	Order-preserving encryption	A location-based privacy-preserving medical service among health stakeholders.
Patil et al., [106]	Blockchain platform	–	A blockchain-based secure framework for universal health data storage and analysis.
Son et al. [107]	Consortium	CP-Attribute based encryption	A secure protocol for a cloud-based telecare information system with controlled access using blockchain.
Rahman et al., [108]	Private blockchain	–	The life monitoring blockchain-based model for a cancer patient allows secure data transmission among health stakeholders.
Yazdinejad et al., [65]	Public blockchain	Symmetric key encryption	A distributed network for remote patient monitoring with transparent and secure data transmission using blockchain
Dib et al. [109]	Hyperledger fabric	Trusted execution environment	A user-centric network to privately transfer the data among health stakeholders using blockchain and Intel's SGX.

the blockchain. Encryption schemes such as proxy re-encryption and attribute-based encryption were the well-known cryptographic methods used to develop privacy-preserving data exchange. The permissioned blockchain-based smart contract is an efficient solution for fine-grained access control policies [114]. In the following subsection, we have explored several well-known privacy mechanisms to gain insightful information.

- Encryption Scheme: Encryption is a well-known method used in blockchain. Encryption methods are integrated with blockchain technology to meet data ownership and security requirements [115]. In the symmetric encryption method, the same key is accessible by both sender and the receiver. In the asymmetric scheme, the private key and the public facilitate the decryption and encryption of the data. Several data encryption methods provide access control and security over the network, for example-attribute-based encryption, identity-based encryption [116], and proxy re-encryption [117]. These techniques help securely transfer data from the data owner to the requester. Several past research studies integrated these methods with the blockchain platform. In [118], the authors created Health-chain, a privacy-preserving framework for health data. The hash value of health data stored in IPFS ensures privacy preservation while reducing the computational overhead.
- Identity-based Encryption: Shamir first introduced the novel idea of a public-key cryptography scheme in 1984 [116]. Since then, researchers have proposed several Identity-based Encryption (IBE) proposals [112]. The IBE scheme uses bilinear maps theory. In the article [112], the authors integrated the IBE scheme with permissioned blockchain to provide a privacy protection scheme. This scheme was better than traditional Public Key Infrastructure (PKI), as it avoids complicated certificate management and prevents passive attacks. The IBE scheme uses a unique identity ID to generate the user's public key. With a unique identity ID, any user who wants to join the permissioned blockchain can obtain the encrypted key. In the article [119], the authors used blockchain and identity-based encryption schemes to provide a decentralized and privacy-preserving exchange of Internet of Things (IoT) data. Blockchain provides access control policies, and identity-based encryption facilitates cryptographic access control policies. In the article [120], the authors have developed medical information exchange platform based on blockchain and identity-based encryption to guarantee medical data privacy and confidentiality.
- Proxy Re-encryption: Proxy re-encryption (PRE) is a feasible cryptographic public-key encryption method proposed by Blaze et al. [121] and Mambo and Okamoto [117]. This method permits third parties or proxies to securely transform the ciphertexts or encrypted data from one public key to another. The proxy or cloud service providers cannot acquire any details about the original message [122]. It is a feasible solution to provide secure access delegation. Integrating PRE with blockchain smart contracts provides a fast and efficient platform for sharing and storing data [34,82]. In [123,124], the authors have proposed a blockchain-based model to protect EHR. This model uses the proxy re-encryption method to transfer patient data without revealing the private key. In [125], the authors have designed a proxy re-encryption and blockchain-based distributed secure file storage and sharing system. In [126], the authors have designed a blockchain-based cloud-assisted framework that combines proxy-re encryption and searchable encryption technology to ensure data privacy for EHR sharing.
- Attribute-based Encryption (ABE): This is one of the promising techniques of a public-key-based scheme. It is an efficient technique that guarantees fine-grained access policies [127]. ABE allows only specific users with certain attributes to view or access

the data, depending on the access control policies. In [128], the authors have designed an ABE-based blockchain model for IoT applications. With ABE, only the user with a specific attribute can access the data. This proposed model achieves higher privacy with minimum computational overhead. Few other encryption approaches ensure health data protection, for example- Cipher-Policy Attribute-based Encryption (CP-ABE) [129] and Key-Policy Attribute-based Encryption (CP-ABE) [127]. Only the user with valid attributes (user key) can decrypt the data to achieve authenticity with these methods. With CP-ABE, users can define the access control structure of their health data [107]. The authors of the article [130] have designed blockchain-based privacy-oriented architecture. In this article, the patient specifies the access policies and the time duration to access his data. The architecture used a voting-based Practical Byzantine Fault Tolerance (PBFT) method and encrypted the user's data, ensuring confidentiality.

- Blockchain-based Smart Contracts: Nick Sazabo introduced the Smart Contracts (SC) term in 1997 [131]. Smart contracts are digital contractual conditions of agreements written in various computer programming languages. The smart contract executes automatically once the predefined conditions written in the contracts are satisfied [52]. A smart contract is implemented on the topmost level of the blockchain to guarantee proper access control. Various programming languages such as Golang, Kotlin, Solidity, Java, and JavaScript are used to write down smart contracts depending on the blockchain platform. However, contract correctness, designing careful control flow, improving execution efficiency, proliferation, and redeployment are challenging issues associated with smart contracts [57]. Permissioned blockchain platforms such as *Hyperledger Fabric* (HF) have been used in previous studies to achieve privacy and confidentiality [130,132]. *Hyperledger Fabric* or an enterprise blockchain is feasible to protect private health data. In [124], the authors have utilized HF and public key infrastructure features to provide patient-centric authorized access to health records. In [133], the authors have proposed HF-based modular architecture that adopts fundamental concepts of HF, such as modularity. In [134], the authors have proposed *Ancile*; this blockchain-based model applies smart contracts to maintain the cryptographic hashes of medical records and proxy-re encryption privacy-preservation efficient access control.
- Attribute-based Signature: Attribute-based Signature (ABS) is beneficial in attribute-based messaging and anonymous authentication systems [135]. In an attribute-based signature, an authority issues the set of attributes to a valid user or signer. A signer signs the message or document with a predicate satisfied by the singer's set of attributes. In this scheme, the signature hides any identifying detail about the signer and issued attributes. In [130], the authors have used an attribute-based signature method to propose a privacy-preserving blockchain-based framework. The users, such as doctors and nurses, invoked the Attribute-based signature to upload and access the EHR stored on the blockchain. KUNodes is a node selection algorithm that helps to achieve attribute revocation. Similarly, in [136], the authors have integrated the Attribute-based Multi-Signature (ABMS) method and ABE scheme with *Hyperledger Fabric* and *Hyperledger Ursa library*. This architecture helps authenticate patients anonymously and encrypt EHR to facilitate efficient EHR management.
- Ring Signature: Ring signature is another encryption technique for data privacy protection. This digital signature scheme is developed by Rivest et al. [137]. The ring signature transaction contains only a specific group of members (ring members). Any member can produce a digital signature by randomly selecting multiple member's public keys, a random value, a signer's secret key, and other techniques. It is computationally infeasible to revoke the anonymity of the actual singer. It is an elegant way to solve issues with multiparty computations. In [138], the authors have proposed a ring signature-based blockchain framework to build a privacy-preserving data storage model. This model ensures data privacy.
- Data Anonymization: In the blockchain, differential privacy is a simple anonymization method applied to protect data privacy. For instance, in [139], the authors have employed differential privacy to prevent an adversary who can gather sensitive personal data when implementing federated learning using blockchain to note crowdsourcing activities. In [110,140], the authors have integrated blockchain and differential privacy for the privacy preservation of data. In [141], a differential privacy technique protects personal information while performing federated learning.

Mixing is another anonymization method [142] used in blockchain to conceal the history of transactions. This method makes it difficult to correlate the transaction history [17]. Thus, it helps to make the address non-correctable in the transaction history. In [143], the authors have used a mixing scheme with the Bitcoin blockchain to protect private information. The Zero-Knowledge Proof (ZKP) is a cryptographic method in which the prover attempts to convince the verifier of his knowledge without revealing any other information apart from its gained knowledge [144]. It keeps the sender and receiver transaction detail hidden. Due to this feature, ZKP ensures authentication [82], secure communication, and privacy [145].

3.4. RQ4: Federated learning for privacy-preservation

Machine Learning-based (ML) models have emerged as an efficient approach to achieving robust and accurate health data analytics in the last two decades. However, to take full advantage of the machine learning approach, a large amount of health data is needed to build effective predictive models. For this reason, the collaboration between multiple health organizations must collect and share health data [27]. The recent COVID-19 pandemic has also highlighted the need to effectively share health data, resources, and knowledge globally [146,147]. In practice, the sensitive nature of health data and stringent privacy regulation laws such as HIPAA and GDPR restrict hospitals from sharing their raw health data with other entities. Thus, there is a trade-off between data privacy and better predictive data analytics [148]. The Federated Learning (FL) approach is relevant to remove this trade-off as it eliminates the need to share raw data to train a global machine learning model. FL is an emerging technology that can guarantee data privacy and train a collaborative model from multiple data providers [149]. The main advantage of FL over the traditional centralized machine learning methods is the ability to provide decentralized collaborative learning for implementing ML algorithms. There is no need to collect or process data at data centers; instead, the ML model is trained at the local node. Another advantage of FL is compliance with GDPR, as data never leaves the local node, and only model updates are shared [150].

There are three main steps involved in FL implementation. In the first step, the central or coordinating server initiates the process and shares the global model, i.e., the initial model parameter, with all the federated users/clients. In the second step, all the clients/users train their respective local models using the initial model parameter and their data. Afterward, the client sent trained local model updates to the coordinating server. In the third step, the coordinating server aggregates all the local updates and generates a new global model. Finally, the new global model was shared with all the clients. This iterative process repeats till the model achieves a certain level of accuracy [29].

Generally, categorizing a federated learning system depends on the data distribution characteristics and the client's participation in the FL environment. The three types of FL are horizontal FL, vertical FL, and last one is federated transfer learning. In horizontal FL, datasets

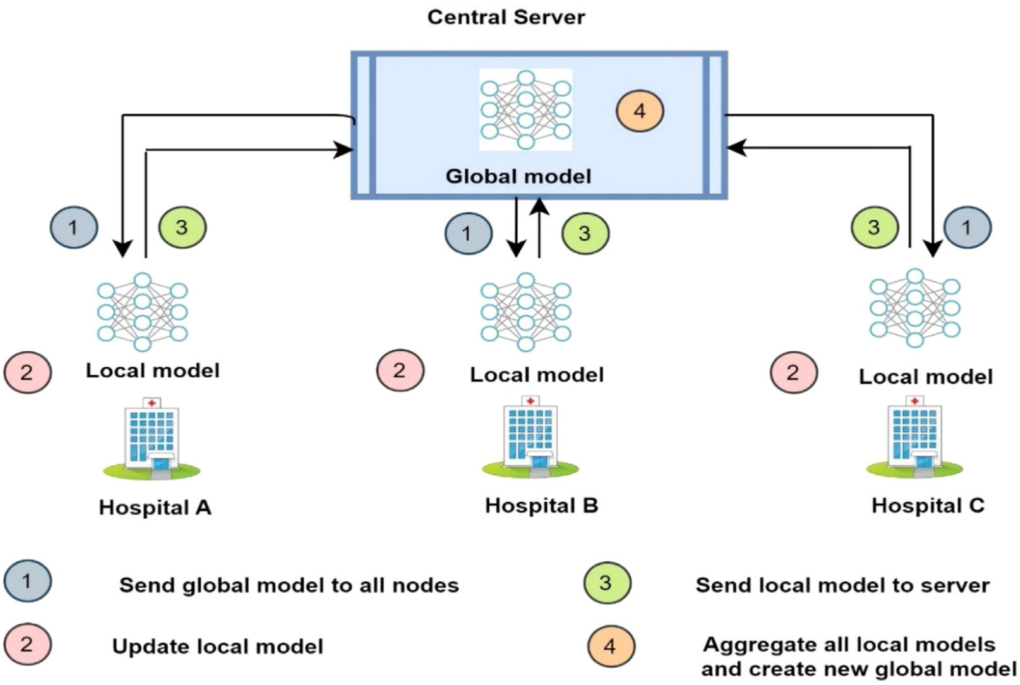


Fig. 6. Architecture of federated learning in healthcare scenario.

own by different clients share similar feature spaces but with different sample spaces. In vertical FL, clients have similar sample spaces with different feature spaces. Federated transfer learning is the hybrid of horizontal FL and vertical FL [151]. FL is a rapidly evolving technology. Google and WeBank have launched open-source FL platforms such as TensorFlow Federated [152] and Federated AI Technology Enabler (FATE) to increase FL implementation [153]. In the recent past, FL has become a promising technique that plays a vital role in various applications to offer low-latency decisions with privacy guarantees. Some well-known applications that highlight the potential of FL are-virtual keyboards, self-driving cars, healthcare, robotics, Unmanned Arial Vehicles (UAV), and supply chain finance [154].

One of the highly influential sectors of FL is the healthcare industry. FL addresses data privacy and governance issues, usually in health data aggregation [27]. In healthcare, FL allows hospitals to collaboratively train a global model without sharing raw data with other entities. In the FL mechanism, multiple healthcare organizations share locally calculated model updates to a coordinating server. These model updates generate a global predictive model without revealing private datasets [155]. Thus, it protects privacy and ensures legal and ethical compliance between hospitals [156]. More recently, in the COVID pandemic, the Standford Institute of Human-Centered AI created a federated learning-based in-home system to monitor persons for coronavirus symptoms. In addition, some research works proposed FL-based solutions to detect coronavirus infections while preserving patient data privacy [146,157]. Similarly, NVIDIA Clara is a healthcare service platform that uses federated learning to protect patient data privacy in healthcare and medical institutions. Fig. 6 shows a typical model of federated learning.

3.4.1. *Advantages and privacy issues in federated learning*

Compared to the traditional ML approach, FL naturally provides a privacy guarantee. Multiple hospitals train models collaboratively in federated learning scenarios without a centralized dataset. Hospitals only shared updated models with the coordinating servers. Thus, FL avoids collecting massive health data at any centralized repository. FL reduced the training time and cost and improved data security. Table 7 shows the advantages and challenges of federated learning.

Table 7
Advantages and challenges in federated learning.

Sr. no.	Advantages	Challenges
1	Enable Scalability	Lack of trust
2	Improve security and Accuracy	Traceability
3	Ensure privacy	Accountability
4	Low cost of training	Potential privacy
5	Reduce training time	Communication

3.4.2. *Privacy attacks/threats in federated learning*

FL offers initial privacy protection but is still susceptible to potential privacy attacks. Despite the significant research on FL schemes, existing FL schemes are still vulnerable to potential privacy attacks. FL schemes cannot meet the advanced security requirements for applications. Keeping this in view, we have discussed the attacks in FL and reviewed several privacy-preserving techniques incorporated in FL.

According to prior research, sharing local model updates to the collaborator server in FL can leak sensitive information [21]. For example, in [158], the authors have discussed the model training process. In that process, adversaries can partially extract each client's training data based on their uploaded model parameter. A recent work depicts how those attackers can extract training data from model parameters in a few iterations. Such issues make FL vulnerable to privacy attacks such as Poisoning attacks [159] and Inference attacks that include membership inference attacks [160], model inversion attacks [161], and reconstruction attacks. The current FL system faces two types of attacks. The first is an insider attack launched by the FL server. The clients in the FL system fall under the insider attacks category- for example, *Sybil Attacks* [25] and *Byzantine Attacks,162*. The second is outsider attacks launched by the final users of FL systems and by intruders.

- Membership Inference Attack: The main aim of membership inference attacks is to determine whether the input samples to the learning model come from the training dataset or not. In the FL approach, the adversary aims to determine if a specific input sample belongs to the personal training data of only a single party or if it belongs to any party [162]. In the FL, attackers can conduct passive and active membership inference attacks. In passive attacks, attackers perform the inference by observing updated model parameters without changing anything in the global or local training process. Inactive attacks, attackers can carry out stronger attacks against other clients by tampering with the FL model [163].

- Poisoning Attack: In the FL framework, the coordinating server is susceptible to inspecting the original data or training process at the local node. Thus, this situation prohibits the transparency of the model training process. Moreover, it imposes model poising attacks. Throughout the training phase, the poisoning attacks can be carried out on the model called model poisoning and on data called data poisoning attacks [164]. Model poisoning attacks target model parameters or insert the backdoor attacks into the global model before sending them to the coordinating server [25]. At a very high level, both the data and model poisoning attacks try to change the behavior of the trained model.

Membership inference attacks and poisoning attacks show the need to protect model parameters in the FL training process. Therefore, there is a need to use privacy mechanisms to protect client data effectively in the FL system [150].

3.5. RQ5: Privacy-preserving mechanisms in federated learning

Recent work on FL has demonstrated that FL may fail to provide a strong privacy guarantee. Therefore, for designing a robust FL system, there is a need to use privacy-preserving techniques to protect privacy at two-level- first at the training dataset and another at the exchange of local model parameters [150]. The various privacy-preserving methods have integrated with FL to deal with privacy threats/attacks [165].

- Differential Privacy (DP): DP was proposed in 2006 by Dwork et al. [166]. DP is the most widely used privacy technique due to its algorithmic simplicity and small system overhead. Communication between a coordinating server and clients is the trickiest element in the FL scheme. In such a situation, to provide effective communication between the central server and clients DP mechanism is commonly used before sharing model parameters. In the DP mechanism, a certain amount of random noise is added to data or the model updates before being exchanged to the central server [167]. DP mechanism is also used before sharing the algorithm updates or computational results [168]. DP upsurges the level of privacy in the FL framework [169]; still, it often yields lower data utility or substantial loss in global model performance [170]. Furthermore, owing to the random noise present in the training process, the FL system may develop less accurate data models. Still, a trade-off exists between data utility and privacy guarantee [166].
- Homomorphic Encryption: It is an attractive privacy-preserving cryptographic method adopted in many FL systems that can perform specialized calculations (e.g., addition) on encrypted data or ciphertext without decrypting it first [171]. Based on the computational operations and encryption, HE consists of different types, such as partial HE, fully homomorphic encryption [172], and somewhat HE. In the FL system, the HE technique paillier helps securely aggregate model parameters [173]. In addition, some research studies have used the additive property of partial HE to prevent attacks on locally computed models [174,175]. HE provides potential privacy for cross-silos FL by performing easy and complex computation operations (e.g., exponentiation, modular multiplication). However, the computation of complex functions is expensive to compute. In HE, performing complex operations increases significant computational overhead [150]. The authors in [176] have designed privacy-preserving FL architecture that protects the data privacy and integrity of the global model. They have used Trusted Execution Environment (TTE) to create a training-integrity protocol to detect causative attacks.
- Secure Multi-party Computation: It is also known as secure/privacy-preserving computation or Multi-Party Computation (MPC). It was proposed in 1986 by Yao [177]. With SMPC, multiple parties can perform distributed computing tasks in a protected manner. Parties can jointly perform computation tasks on their private input data. A single party cannot learn the personal data of the other party. In SMPC, after computation, each party can only obtain the final output and its inputs [150]. The SMPC protects the model parameters in the FL system before exchanging them to a central server. The FL system only encrypts the model parameters, as there is no need to encrypt all input data [29]. SMPC helps to eliminate the trade-off between privacy and data usability. But still, it is susceptible to inference attacks. Another concern in SMPC implementation is computational overhead that leads to longer training time. However, there exists a trade-off between data privacy and efficiency. In SMPC, the continuous transfer of encrypted and decrypted data between multiple parties may have a higher communication overhead [178].

3.6. RQ6: The convergence of federated learning and blockchain

Many researchers have integrated blockchain technology and a federated learning approach for different use cases. In Table 8, we have summarized the relevant research studies that have integrated blockchain and federated learning for various use cases. In [179], the authors have designed a blockchain-based protocol for secure data sharing in federated learning. They have developed secure communication between the FL client and the FL server. In [180], the authors have discussed the application of blockchain and FL in vehicular (IoT) networks. Integrating federated learning in vehicular networks makes offloading the trained models to vehicles more secure and reliable. In [181], the authors have used a blockchain network as a coordinating server to exchange local model updates between devices. In [182], the authors proposed a Galaxy Federated Learning (GFL) architecture incorporating the Ethereum blockchain and federated learning. In addition, they have developed a ring-decentralized federated learning algorithm to improve network robustness and bandwidth utilization. In recent research [183], the authors have developed a blockchain-enabled asynchronous FL-based IoT anomaly detection model. This work devised a DP-GAN algorithm (Generative Adversarial Nets) to preserve the model parameter privacy.

3.6.1. Federated learning and blockchain for healthcare scenario

The adoption of federated learning techniques and blockchain in the medical sector carries enormous benefits and promises. These technologies ensure secure storage, exchange, and utilization of health data. In the COVID-19 era, distributing accurate and trustworthy information is very important; for this purpose, few authors applied FL and blockchain to design robust models to share COVID-19 patient information in a privacy-preserving manner [192,200,201]. In [202], the authors have proposed a patient-centric blockchain and AI-based model to fight against COVID-19. In [203], the authors have proposed a blockchain and federated learning framework to collect and share COVID-19 patient data among several hospitals while maintaining data privacy. Few authors focused on designing a trustworthy healthcare model based on FL and blockchain. These architectures focused on the privacy protection of IoHT, i.e. (Internet of Health Things) data [204,205], and designing IoMT solutions [164]. Similarly, in [206], the authors have proposed a blockchain-empowered FL architecture to enhance fairness in FL tasks and enable accountability. They have presented the data sampler algorithm to increase the model accuracy.

By understanding the enormous potential of these technologies, we have integrated them into the telemedicine system. In Fig. 7, our proposed architecture shows the merging of blockchain and federated learning for the telemedicine system. This study adopted a private

Table 8
Summarization of relevant studies implementing blockchain and federated learning.

Study references	Blockchain platform	Learning methods	Privacy methods	Remarks
Wu et al., [184]	Hyperledger fabric	Deep neural network	Homomorphic encryption	A privacy-aware blockchain-based decentralized FL framework is proposed to avoid a single point of failure.
Lu et al. [185]	Permissioned blockchain	–	Differential privacy	Blockchain and FL-based intelligent and trustworthy data-sharing model is designed for Industrial IoT.
Weng et al., [186]	Corda	Stochastic gradient descent	Non-interactive zero-knowledge	A deep learning privacy-preserving incentive mechanism is developed to assure the auditability and privacy of the training process.
Fan et al. [187]	Public and Consortium blockchain	–	–	A hybrid blockchain-based transparent resource trading platform is proposed to facilitate auditable and autonomous auctions among edge nodes.
Toyoda et al., [188]	Public blockchain	–	–	A mechanism-design-based FL protocol is designed that helps to reward the users based on their contribution.
Liu et al., [189]	Permissioned blockchain	Neural network	–	A peer-to-peer payment-based network for federated learning is designed to provide proper profit distribution.
Arachchige et al., [190]	Ethereum	Stochastic gradient descent	Differential privacy	A trustworthy and privacy-preserving Industrial IoT system is developed.
Kang et al., [191]	Consortium blockchain	Stochastic gradient descent	–	A reliable and trusted client selection scheme for FL tasks is proposed in a mobile network.
Mugunthan et al., [26]	Ethereum	Linear regression	Differential privacy	A privacy-preserving auditing mechanism is designed to reward the agents based on model contribution
Aich et al., [192]	Blockchain	–	–	To build a generalized and robust AI model with secure data access for COVID-19 patient data.
Wang et al., [193]	Proof-of-work	–	–	A proposed secure decentralized multiparty learning platform that was resistant to Byzantine attacks is proposed.
Kang et al., [194]	Consortium and public blockchain	Distributed stochastic gradient descent		A communication-efficient blockchain-based federated edge learning system is developed to manage high-quality model updates.
Korkmaz et al., [195]	Ethereum private blockchain	–	–	A fully decentralized FL model is designed to store and aggregate model updates.
Wang et al., [196]	Blockchain	Stochastic gradient descent	Differential privacy	A privacy-preserving FL system is presented to provide efficient data transmission for Unmanned aerial vehicles (UAV) in mobile crowdsensing.
Qu et al. [197]	Public blockchain	Stochastic variance reduced gradient	–	A blockchain and FL-based system are designed for efficient and secure fog computing communication resilient to poisoning attacks.
Passerat-Palmbach et al., [9]	Ethereum	–	Secure encrypted virtualization memory.	To introduce the blockchain FL-based architecture to provide fine-grained access policies and privacy-preserving audit mechanisms.
Demertzis et al., [198]	Blockchain	–	–	A blockchain-based FL framework is presented to focus on threat defense in smart cities.
Ma et al. [199]	Permissioned blockchain	Logistic regression	Secure multi-party computation	Transparent model contribution evaluation.
Zhao et al. [139]	Consortium blockchain	–	Differential privacy	A blockchain-based FL model is designed to assist home appliance manufacturers in predicting customer requirements.

blockchain platform, i.e., Hyperledger Fabric blockchain. In this diagram, hospitals A is primary care clinic, and hospitals B and C are remote specialist hospitals. Hospital C acts as a miner or coordinator hospital. The primary care clinician collects the patient's health data at the initial level. Health data is stored in a hospital's database using a proper privacy-preserving mechanism. Patient-centric smart contract

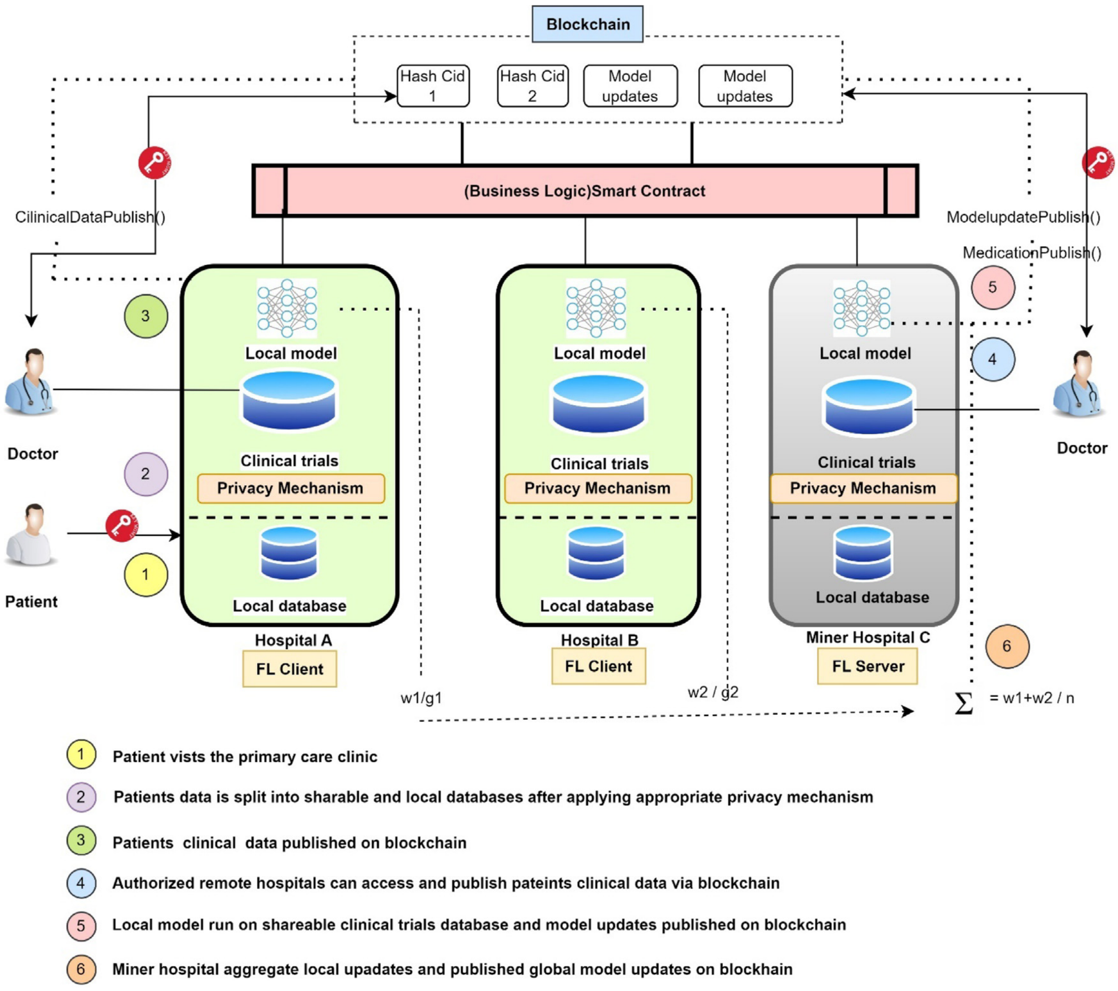

Blockchain
Hash Cid 1
Hash Cid 2
Model updates
Model updates
(Business Logic)Smart Contract
CilinicalDataPublish()
ModelupdatePublish()
MedicationPublish()
Local model
Clinical trials
Privacy Mechanism
Local database
Hospital A
FL Client
Hospital B
FL Client
Miner Hospital C
FL Server
Doctor
Patient
Doctor
w1/g1
w2 / g2
Σ = w1+w2 / n
1 Patient vists the primary care clinic
2 Patients data is split into sharable and local databases after applying appropriate privacy mechanism
3 Patients clinical data published on blockchain
4 Authorized remote hospitals can access and publish pateints clinical data via blockchain
5 Local model run on shareable clinical trials database and model updates published on blockchain
6 Miner hospital aggregate local upadates and published global model updates on blokhain

Fig. 7. The proposed telemedicine architecture integrating blockchain and federated learning. The remote hospitals can access the patient clinical data and global model updates via blockchain.

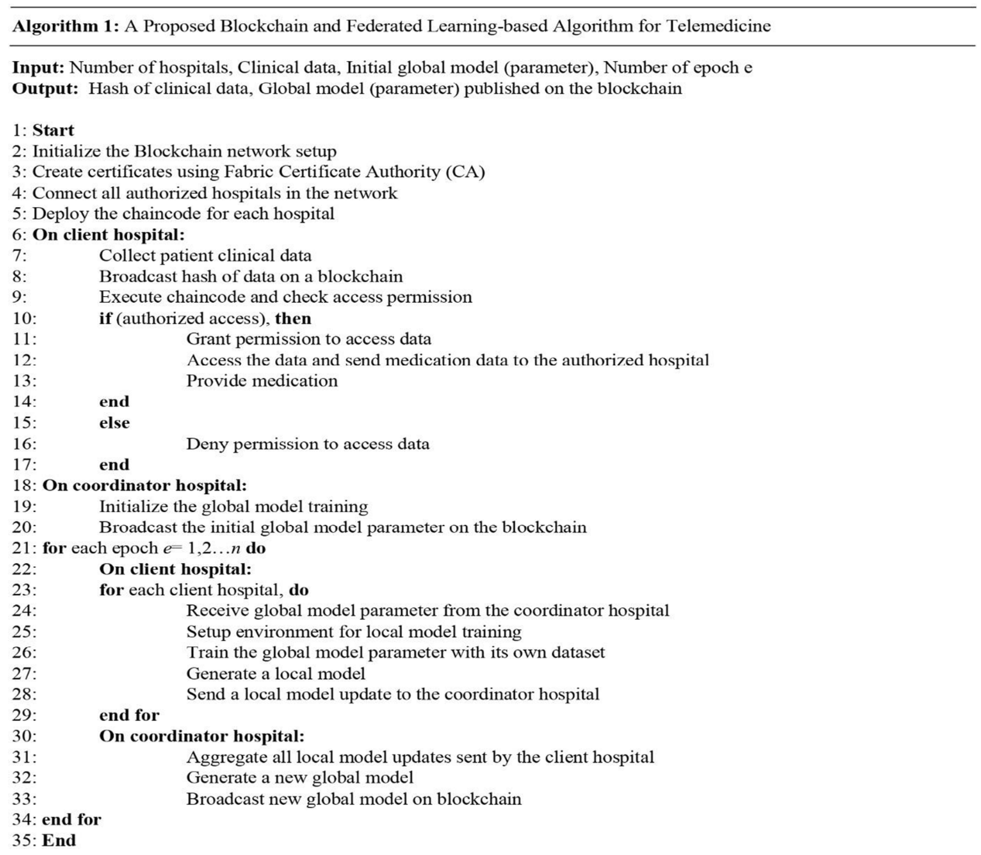
logic is applied before sharing data with remote hospitals to achieve secure data transmission. With federated learning, decentralized and collaborative learning is performed. Global models update is shared in a trustworthy and safe manner. By integrating blockchain and federated learning, health data is securely transmitted and stored and can be used to perform effective data analytics. Algorithm 1 illustrates the detailed workflow of our proposed blockchain and FL-based telemedicine system.

4. Discussion and future scope

This survey helps to highlight the benefits and issues in the current remote healthcare system. It explores the significance of promising technologies such as blockchain and federated learning to strengthen the remote healthcare system. Compared to the previous studies, this survey discussed several privacy-preserving methods incorporated with blockchain and federated learning to design a privacy-centric telemedicine system. The main objective is to highlight the issues faced while designing patient-centric privacy-preserving telemedicine systems and how blockchain and federated learning have the potential to overcome those issues. This survey discussed the privacy issues/attacks in federated learning and explored the existing privacy-preserving techniques that facilitate achieving potential privacy.

4.1. Summarization of research questions

- RQ1: In the COVID-19 pandemic, tremendous growth is observed in adopting the telemedicine system. Telemedicine has become the latest efficient way of communicating and accessing healthcare. Despite the advancement in telemedicine, it still faces challenges that need to be handled urgently. Telemedicine is still in its development phase. Unauthorized data access, data privacy, lack of trust, data breach, and lack of a patient-centric approach are the hurdles that need to be considered to integrate telemedicine systems in healthcare fully. There is a need for a trustworthy, robust telemedicine platform that ensures data privacy and easy availability or accessibility of data. In this regard, it is essential to adopt advanced technologies with telemedicine systems to design reliable systems. Blockchain and telemedicine share a mutual vision to develop a decentralized and reliable system. The blockchain facilitates an efficient way to store and share electronic health records in a decentralized manner.
Similarly, the adoption of federated learning in telemedicine is a hot research topic. It helps to design a collaborative and accurate diagnosis model that aids in achieving precision medicine. However, the sustained use of blockchain and federated learning in telemedicine systems is still under development. In the future, much more research and the maturation of these technologies will be necessary before the framework can be used securely and safely across the globe.
- RQ2: Blockchain has several fascinating features that can be valuable for healthcare applications. The decentralized nature of blockchain helps create applications without needing to depend on any centralized authority. Decentralization helps create a transparent healthcare workflow that lets patients know how their



Algorithm 1: A Proposed Blockchain and Federated Learning-based Algorithm for Telemedicine

Input: Number of hospitals, Clinical data, Initial global model (parameter), Number of epoch e
Output: Hash of clinical data, Global model (parameter) published on the blockchain

```
Start
Initialize the Blockchain network setup
Create certificates using Fabric Certificate Authority (CA)
Connect all authorized hospitals in the network
Deploy the chaincode for each hospital
On client hospital:
        Collect patient clinical data
        Broadcast hash of data on a blockchain
        Execute chaincode and check access permission
        if (authorized access), then
                Grant permission to access data
                Access the data and send medication data to the authorized hospital
                Provide medication
        end
        else
                Deny permission to access data
        end
On coordinator hospital:
        Initialize the global model training
        Broadcast the initial global model parameter on the blockchain
for each epoch $e$= 1,2…$n$ do
        On client hospital:
        for each client hospital, do
                Receive global model parameter from the coordinator hospital
                Setup environment for local model training
                Train the global model parameter with its own dataset
                Generate a local model
                Send a local model update to the coordinator hospital
        end for
        On coordinator hospital:
                Aggregate all local model updates sent by the client hospital
                Generate a new global model
                Broadcast new global model on blockchain
end for
End
```

health data is shared and accessed in the network. Immutability helps to ensure the validity and integrity of sensitive health records. Traceability, transparency, and data availability are key features of blockchain that enhance its applicability to developing trustworthy healthcare applications. Regarding data privacy, despite the encryption mechanism employed with the blockchain, there is a concern that it is possible in public blockchain to reveal the patient's identity by linking sufficient information related to that patient. In addition, a privacy leakage can occur in blockchain even though users only perform transactions with their private and public keys. The private keys in the blockchain are also susceptible to potential compromise, resulting in a lack of authorized access to health data. Due to this, patient data privacy is a core concern when integrating blockchain into the healthcare industry. In the future, the challenge of data privacy will be an open research issue to enhance the health stakeholder's confidence to boost the adoption of blockchain in healthcare applications.

- RQ3: This study highlights the privacy-related challenges in the blockchain and explores several privacy-preserving mechanisms deployed with blockchain to ensure privacy guarantees. It becomes possible to achieve a strong privacy guarantee by deploying different encryption schemes (e.g., Attribute-based encryption, proxy re-encryption, and identity encryption) and other mechanisms like homomorphic encryption and ZKP with blockchain. Identity-based encryption improves key distribution. In this mechanism, the user's identity is used to generate a public key; thus, there is no need to obtain a user public key to transfer encrypted data. Proxy Re-encryption is suitable for data access control and is a feasible solution to provide secure access delegation. Attribute-based encryption guarantees fine-grained access policies that help to define authorized users. Blockchain-based smart contracts help to guarantee proper access control. Attribute-based Signature (ABS) benefits attribute-based messaging and anonymous authentication systems. Ring signature is a feasible solution to solve the issues with multiparty computations. Mixing makes it challenging to correlate the transaction history. In addition, some other privacy-preserving mechanisms, such as differential privacy, zero-knowledge proof, and homomorphic encryption, are also deployed with blockchain to provide a strong privacy guarantee. However, no privacy-preserving mechanism is free from vulnerabilities. Each privacy-preserving method has its shortcomings. The drawback of attribute-based encryption is that the data owner must use each authorized user's public key to encrypt the data. This mechanism is not suitable for some real-world applications. The high cost required for data encryption and decryption is another challenge the encryption schemes face. High computational complexity is the main challenge in adopting zero-knowledge proof and homomorphic encryption. In some use cases, zero-knowledge proof depends on a third party, while homomorphic encryption requires an extended processing time. The challenging issues with smart contracts are contract correctness, designing careful control flow, improving execution efficiency, proliferation, and redeployment of contracts that need to consider for better privacy preservation. Thus, there is a need to consider the current benefits and issues with these privacy-preserving mechanisms before deploying them with blockchain for healthcare applications.
- RQ4: The main reason behind the widespread adoption of federated learning is that it allows collaborative learning that facilitates efficient machine learning while ensuring legal compliance and privacy between multiple hospitals. FL addresses data privacy and data governance issues that usually exist in health data aggregation. With the FL technique, machine learning models

run in a distributed and heterogeneous manner while minimizing the risk of data transfer. Unlike centralized learning, FL has few valuable features, such as ensuring privacy since the hospitals never share their private datasets. It possesses lower latency as hospitals can make predictions locally and less power consumption since models run on local hospital data. Thus, FL offers large datasets to build a better predictive global model through multi-site collaboration and provides easy scalability. Furthermore, minimum resources are required in the FL to aggregate models; thus, deployment becomes more economical. However, the core challenges of FL, such as lack of coordinating side trust, potential privacy, and traceability, must be addressed before adopting FL in the healthcare domain.

- RQ5: According to the latest research studies, federated learning is susceptible to several privacy threats, such as membership attacks, inference attacks, and poisoning attacks. Several privacy methods were integrated with FL, such as SMPC, Homomorphic encryption, and Differential privacy for potential privacy. Most recent studies primarily focused on differential privacy and SMPC for privacy-preserving FL. Each method might resolve the privacy issues, but they still have shortcomings. For example, differential privacy suffers accuracy issues, and SMPC and HE lead to higher communication and computational overheads. However, these existing privacy-preserving methods, such as Differential privacy, impose lower data utility, Secure Multi-party Computation, impose a high computational overhead, and are susceptible to inference attacks. With these methods, FL achieves strong privacy, but it loses efficiency as well as accuracy. Thus, there is a need to consider the current issues with DP, SMPC, and HE before designing robust FL systems. Therefore, further research is still required to eliminate the trade-off between data privacy and accuracy. Developing a practical FL system with a potential privacy guarantee is still very challenging. In the future, even combining various privacy techniques with blockchain and FL may lead to a potential privacy guarantee. The ultimate goal is to design a secure, efficient, and accurate federated learning system with a privacy guarantee. Privacy-preserving FL is still a challenging research area.
- RQ6: More recently, blockchain and federated learning technology are independently making a tremendous technological revolution in healthcare industries. The ethical challenges in a medical setting are data privacy, which means preserving patient identity; data transparency means the patient must know how their data are accessed; and consent means patients have the right to control their data. In this regard, blockchain is mainly used in healthcare to facilitate decentralized, secure storage and controlled access to health data. On the other hand, federated learning allows gaining insights from data across isolated hospitals and medical institutes to generate a collaborative model with a privacy guarantee. Integrating blockchain and federated learning is very beneficial in addressing challenges present in the medical context.

  Furthermore, blockchain ensures auditability and verifiability in federated learning to improve the correctness and efficiency of training procedures. These two technologies are complementary to each other and have the potential to resolve traditional healthcare's core challenges. With this convergence, it is possible to securely share and analyze data and models in a trustworthy manner. As the convergence of these two technologies is still under development, there is a need further to explore this promising research field in an integrated way. Despite this, federated learning is vulnerable to inference attacks, and it is not easy to achieve strong privacy. Blockchain also fails to achieve a complete privacy guarantee. Blockchain and naïve federated learning systems are susceptible to advanced data privacy threats. Thus, to design a privacy-centric healthcare architecture, it is necessary to incorporate a suitable privacy-preserving mechanism with these technologies to enhance its adaptability in healthcare. However, blockchain and federated learning offer an initial level of privacy, but it offers a stronger privacy guarantee in combination with various privacy methods. In the near future, there is a need to explore these two emerging technologies to produce reliable modern healthcare services to improve care quality. The exciting future research topic is integrating federated learning and blockchain technology with appropriate privacy-preserving mechanisms in telemedicine systems. This integration helps develop a cost-effective, reliable, and trustworthy decision-making platform. Furthermore, designing a blockchain-based federated learning framework is a promising way to boost the overall standard of healthcare.

4.2. Limitation

Our SLR has recognized a few limitations. First, this SLR analyzes the research studies published in IEEE Xplore, Web of Science, Science Direct, ArXiv, and Scopus, which may result in the incompleteness of relevant literature. However, as stated earlier, we only focused on journal articles and conference papers, which meant we could not retrieve the more relevant information published as book chapters or lecture notes. As a result, this study may miss a few relevant research works that have not been searched in the grey literature.

5. Conclusion

The COVID-19 pandemic has taught us a few very important lessons in a hard way. On one side, it has exposed vulnerabilities of the existing healthcare systems; on the other side, it has also shown the potential of available technologies, such as telemedicine, to rapidly achieve universal healthcare coverage that too at a fraction of the cost compared to that of the brick-and-mortar model of healthcare. The use of an online web-based portal CoWIN, to coordinate and administer more than two billion vaccine doses by India is one such example, which clearly demonstrates how digital technologies could be game changers for healthcare. This indicates how the digital divide between developed and developing nations is rapidly reducing. It would not be an exaggeration to suggest that the stage has been set for digital technologies to take the next big step in healthcare.

The new digital dawn, however, is not without issues. This new digital age has its own set of problems. Given the sensitive nature of data generated and processed in the healthcare domain, it is crucial to diligently deal with all the issues pretending to be data in this domain. We found from the literature that for effective deployment of telemedicine systems, secure storage, privacy-preservation, and authorized access to health data with the consent of patients are identified as the main data-related challenges. Several approaches have been proposed to solve these issues; however, it is not possible to solve these issues using conventional telemedicine architectures, which were proposed decades ago. Moreover, the rapid rate of technological development and ever-increasing computation power, with quantum computing being just in the corner, also makes it futile to solve these issues using old methods.

Blockchain and Federated learning are emerging technologies and are actively pursued by researchers across the globe. In recent years, both federated learning and blockchain advancements have gained enormous attention, and they have shown to be path-breaking technologies in their own regard. Integrating these two powerful technologies could provide an excellent opportunity to build a highly secure and accurate collaborative model in various domains, especially in healthcare.

In this review, we have provided a systematic and in-depth overview of telemedicine, blockchain, and federated learning in the healthcare domain using well-defined research queries. This review systematically explores the benefits and limitations of blockchain and federated learning. We have also discussed the privacy-preserving issues in blockchain and federated learning and have reviewed the several privacy-preserving methods incorporated with these technologies to design privacy-centric applications. Finally, we have proposed a generic framework for merging the blockchain and federated learning-based approaches for telemedicine-based applications. To summarize, this research survey highlights the future opportunity to integrate blockchain and federated-based technologies with suitable privacy techniques in healthcare to create a highly secure and accurate collaborative model.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article

References

[1] J.J. Hathaliya, S. Tanwar, An exhaustive survey on security and privacy issues in healthcare 4.0, Comput. Commun. 153 (2020) 311–335, http://dx.doi.org/10.1016/j.comcom.2020.02.018.

[2] E. Monaghesh, A. Hajizadeh, The role of telehealth during COVID-19 outbreak: a systematic review based on current evidence, BMC Public Health 20 (2020) 1193, http://dx.doi.org/10.1186/s12889-020-09301-4.

[3] World Health Organization (Ed.), Telemedicine: Opportunities and Developments in Member States: Report on the Second Global Survey on EHealth, World Health Organization, Geneva, Switzerland, 2010.

[4] J.P. Burnham, S.A. Fritz, L.H. Yaeger, G.A. Colditz, Telemedicine infectious diseases consultations and clinical outcomes: A systematic review, Open Forum Infect Dis. 6 (2019) http://dx.doi.org/10.1093/ofid/ofz517.

[5] S.A. Nusrat, J. Ferdous, S.B. Ajmat, A. Ali, G. Sorwar, Telemedicine system design using blockchain in Bangladesh, in: 2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering, CSDE, 2019, pp. 1–5, http://dx.doi.org/10.1109/CSDE48274.2019.9162401.

[6] V. Casola, A. Castiglione, K.R. Choo, C. Esposito, Healthcare-related data in the cloud: Challenges and opportunities, IEEE Cloud Comput. 3 (2016) 10–14, http://dx.doi.org/10.1109/MCC.2016.139.

[7] G.J. Annas, HIPAA regulations — A new era of medical-record privacy? N. Engl. J. Med. 348 (2003) 1486–1490, http://dx.doi.org/10.1056/NEJMlim035027.

[8] J. Cusick, The General Data Protection Regulation (GDPR): What Organizations Need to Know, CT Corporation Resource Center, 2018.

[9] J. Passerat-Palmbach, T. Farnan, R. Miller, M.S. Gross, H.L. Flannery, B. Gleim, A blockchain-orchestrated federated learning architecture for healthcare consortia, 2019, arXiv:1910.12603 [cs]. http://arxiv.org/abs/1910.12603 (accessed November 11, 2020).

[10] M. Hiwale, S. Phanasalkar, K. Kotecha, Using blockchain and distributed machine learning to manage decentralized but trustworthy disease data, Sci. Technol. Libr. (2021) 1–24, http://dx.doi.org/10.1080/0194262X.2020.1859046.

[11] J. Brogan, I. Baskaran, N. Ramachandran, Authenticating health activity data using distributed ledger technologies, Comput. Struct. Biotechnol. J. 16 (2018) 257–266, http://dx.doi.org/10.1016/j.csbj.2018.06.004.

[12] M. Mettler, Blockchain technology in healthcare: The revolution starts here, in: 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom), 2016, pp. 1–3, http://dx.doi.org/10.1109/HealthCom.2016.7749510.

[13] A. Hasselgren, K. Kralevska, D. Gligoroski, S.A. Pedersen, A. Faxvaag, Blockchain in healthcare and health sciences—A scoping review, Int. J. Med. Inform. 134 (2020) 104040, http://dx.doi.org/10.1016/j.ijmedinf.2019.104040.

[14] A. Dubovitskaya, P. Novotny, Z. Xu, F. Wang, Applications of blockchain technology for data-sharing in oncology: Results from a systematic literature review, Oncology 98 (2020) 403–411, http://dx.doi.org/10.1159/000504325.

[15] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: a survey, Int. J. Web Grid Serv. (2018) https://www.inderscienceonline.com/doi/abs/10.1504/IJWGS.2018.095647 (accessed February 4, 2021).

[16] C.C. Agbo, Q.H. Mahmoud, J.M. Eklund, Blockchain technology in healthcare: A systematic review, Healthcare 7 (2019) 56, http://dx.doi.org/10.3390/healthcare7020056.

[17] J. Bernal Bernabe, J.L. Canovas, J.L. Hernandez-Ramos, R. Torres Moreno, A. Skarmeta, Privacy-preserving solutions for blockchain: Review and challenges, IEEE Access 7 (2019) 164908–164940, http://dx.doi.org/10.1109/ACCESS.2019.2950872.

[18] P. Durneva, K. Cousins, M. Chen, The current state of research, challenges, and future research directions of blockchain technology in patient care: Systematic review, J. Med. Internet Res. 22 (2020) e18619, http://dx.doi.org/10.2196/18619.

[19] F. Casino, T.K. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues, Telemat. Inform. 36 (2019) 55–81, http://dx.doi.org/10.1016/j.tele.2018.11.006.

[20] J. Xu, B.S. Glicksberg, C. Su, P. Walker, J. Bian, F. Wang, Federated learning for healthcare informatics, J. Healthc. Inform. Res. (2020) http://dx.doi.org/10.1007/s41666-020-00082-4.

[21] H. McMahan, E. Moore, D. Ramage, S. Hampson, B.A. y Arcas, Communication-efficient learning of deep networks from decentralized data, in: AISTATS, 2017.

[22] H.B. Desai, M.S. Ozdayi, M. Kantarcioglu, BlockFLA: Accountable federated learning via hybrid blockchain architecture, 2020, arXiv:2010.07427 [cs]. http://arxiv.org/abs/2010.07427 (accessed November 12, 2020).

[23] Q. Li, Z. Wen, B. He, Federated learning systems: Vision, hype and reality for data privacy and protection, 2019, arXiv.

[24] T. Li, A.K. Sahu, A. Talwalkar, V. Smith, Federated learning: Challenges, methods, and future directions, IEEE Signal Process. Mag. 37 (2020) 50–60, http://dx.doi.org/10.1109/MSP.2020.2975749.

[25] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, V. Shmatikov, How to backdoor federated learning, 2019, arXiv:1807.00459 [cs]. http://arxiv.org/abs/1807.00459 (accessed March 8, 2021).

[26] V. Mugunthan, R. Rahman, L. Kagal, BlockFLow: An accountable and privacy-preserving solution for federated learning, 2020, arXiv:2007.03856 [cs, stat]. http://arxiv.org/abs/2007.03856 (accessed November 17, 2020).

[27] N. Rieke, J. Hancox, W. Li, F. Milletarì, H.R. Roth, S. Albarqouni, S. Bakas, M.N. Galtier, B.A. Landman, K. Maier-Hein, S. Ourselin, M. Sheller, R.M. Summers, A. Trask, D. Xu, M. Baust, M.J. Cardoso, The future of digital health with federated learning, Npj Digit. Med. 3 (2020) http://dx.doi.org/10.1038/s41746-020-00323-1.

[28] Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, B. He, A survey on federated learning systems: Vision, hype and reality for data privacy and protection, 2019, arXiv:1907.09693 [cs, stat]. http://arxiv.org/abs/1907.09693 (accessed November 18, 2020).

[29] V. Mothukuri, R.M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, G. Srivastava, A survey on security and privacy of federated learning, Future Gener. Comput. Syst. 115 (2021) 619–640, http://dx.doi.org/10.1016/j.future.2020.10.007.

[30] K. Salah, M.H.U. Rehman, N. Nizamuddin, A. Al-Fuqaha, Blockchain for AI: Review and open research challenges, IEEE Access 7 (2019) 10127–10149, http://dx.doi.org/10.1109/ACCESS.2018.2890507.

[31] Y. Qu, M.P. Uddin, C. Gan, Y. Xiang, L. Gao, J. Yearwood, Blockchain-enabled federated learning: A survey, ACM Comput. Surv. 55 (2022) 70:1–70:35, http://dx.doi.org/10.1145/3524104.

[32] D.C. Nguyen, M. Ding, Q.-V. Pham, P.N. Pathirana, L.B. Le, A. Seneviratne, J. Li, D. Niyato, H.V. Poor, Federated learning meets blockchain in edge computing: Opportunities and challenges, IEEE Internet Things J. 8 (2021) 12806–12825, http://dx.doi.org/10.1109/JIOT.2021.3072611.

[33] K.D. Pandl, S. Thiebes, M. Schmidt-Kraepelin, A. Sunyaev, On the convergence of artificial intelligence and distributed ledger technology: A scoping review and future research agenda, IEEE Access 8 (2020) 57075–57095, http://dx.doi.org/10.1109/ACCESS.2020.2981447.

[34] S. Vyas, R. Yadav, Converging blockchain and machine learning for healthcare, 2019, pp. 709–711, http://dx.doi.org/10.1109/AICAI.2019.8701230.

[35] S. Singh, P.K. Sharma, B. Yoon, M. Shojafar, G.H. Cho, I.-H. Ra, Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city, Sustain. Cities Soc. 63 (2020) 102364, http://dx.doi.org/10.1016/j.scs.2020.102364.

[36] K. Ba, S. Charters, Guidelines for performing systematic literature reviews in software engineering, 2007, p. 2.

[37] B. Kitchenham, P. Brereton, A systematic review of systematic review process research in software engineering, Inf. Softw. Technol. 55 (2013) 2049–2075, http://dx.doi.org/10.1016/j.infsof.2013.07.010.

[38] W. Mohamed, M.M. Abdellatif, Telemedicine: An IoT application for healthcare systems, in: Proceedings of the 2019 8th International Conference on Software and Information Engineering, Association for Computing Machinery, New York, NY, USA, 2019, pp. 173–177, http://dx.doi.org/10.1145/3328833.3328881.

[39] P. Baudier, G. Kondrateva, C. Ammi, V. Chang, F. Schiavone, Patients' perceptions of teleconsultation during COVID-19: A cross-national study, Technol. Forecast. Soc. Change (2020) 120510, http://dx.doi.org/10.1016/j.techfore.2020.120510.

[40] Telemedicine Market Share Report | Global 2020–2026 Industry Data, Global Market Insights, Inc., 2021, (n.d.). https://www.gminsights.com/industry-analysis/telemedicine-market (accessed February 8, 2021).

[41] L. Provenzi, S. Grumi, R. Borgatti, Alone with the kids: Tele-medicine for children with special healthcare needs during COVID-19 emergency, Front. Psychol. 11 (2020) 2193, http://dx.doi.org/10.3389/fpsyg.2020.02193.

[42] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, Z. Wang, Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system, IEEE Access 7 (2019) 88012–88025, http://dx.doi.org/10.1109/ACCESS.2019.2925625.

[43] I. Hussain, S.J. Park, Big-ECG: Cardiographic predictive cyber-physical system for stroke management, IEEE Access 9 (2021) 123146–123164, http://dx.doi.org/10.1109/ACCESS.2021.3109806.

[44] I. Hussain, S.J. Park, HealthSOS: Real-time health monitoring system for stroke prognostics, IEEE Access 8 (2020) 213574–213586, http://dx.doi.org/10.1109/ACCESS.2020.3040437.

[45] M.S. Islam, I. Hussain, M.M. Rahman, S.J. Park, M.A. Hossain, Explainable artificial intelligence model for stroke prediction using EEG signal, Sensors (Basel) 22 (2022) 9859, http://dx.doi.org/10.3390/s22249859.

[46] I. Hussain, S. Young, S.-J. Park, Driving-induced neurological biomarkers in an advanced driver-assistance system, Sensors 21 (2021) 6985, http://dx.doi.org/10.3390/s21216985.

[47] L. Brunese, F. Mercaldo, A. Reginelli, A. Santone, A blockchain based proposal for protecting healthcare systems through formal methods, Procedia Comput. Sci. 159 (2019) 1787–1794, http://dx.doi.org/10.1016/j.procs.2019.09.350.

[48] A. Donawa, I. Orukari, C.E. Baker, Scaling blockchains to support electronic health records for hospital systems, in: 2019 IEEE 10th Annual Ubiquitous Computing, Electronics Mobile Communication Conference, UEMCON, 2019, pp. 0550–0556, http://dx.doi.org/10.1109/UEMCON47517.2019.8993101.

[49] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. (n.d.) 9.

[50] T.K. Dasaklis, F. Casino, C. Patsakis, Blockchain meets smart health: Towards next generation healthcare services, in: 2018 9th International Conference on Information, Intelligence, Systems and Applications, IISA, 2018, pp. 1–8, http://dx.doi.org/10.1109/IISA.2018.8633601.

[51] M. Hiwale, V. Varadarajan, R. Walambe, K. Kotecha, NikshayChain: A blockchain-based proposal for tuberculosis data management in India, Technologies 11 (2023) 5, http://dx.doi.org/10.3390/technologies11010005.

[52] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, M. Imran, An overview on smart contracts: Challenges, advances and platforms, Future Gener. Comput. Syst. 105 (2020) 475–491, http://dx.doi.org/10.1016/j.future.2019.12.019.

[53] T.-T. Kuo, H.-E. Kim, L. Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications, J. Am. Med. Inform. Assoc. 24 (2017) 1211–1220, http://dx.doi.org/10.1093/jamia/ocx068.

[54] M. Kang, E. Park, B.H. Cho, K.-S. Lee, Recent patient health monitoring platforms incorporating internet of things-enabled smart devices, Int. Neurourol. J. 22 (2018) S76–S82, http://dx.doi.org/10.5213/inj.1836144.072.

[55] M.J. Christ, R. Nikolaus Permana Tri, W. Chandra, W. Gunawan, Exploring blockchain in healthcare industry, in: 2019 International Conference on ICT for Smart Society, ICISS, 2019, pp. 1–4, http://dx.doi.org/10.1109/ICISS48059.2019.8969791.

[56] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, A. Abd-alrazaq, The benefits and threats of blockchain technology in healthcare: A scoping review, Int. J. Med. Inform. 142 (2020) 104246, http://dx.doi.org/10.1016/j.ijmedinf.2020.104246.

[57] T. Hewa, M. Ylianttila, M. Liyanage, Survey on blockchain based smart contracts: Applications, opportunities and challenges, J. Netw. Comput. Appl. (2020) 102857, http://dx.doi.org/10.1016/j.jnca.2020.102857.

[58] S.G. Alonso, J. Arambarri, M. López-Coronado, I. de la Torre Díez, Proposing new blockchain challenges in ehealth, J. Med. Syst. 43 (2019) http://dx.doi.org/10.1007/s10916-019-1195-7.

[59] J. Jayabalan, N. Jeyanthi, Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy, J. Parallel Distrib. Comput. 164 (2022) 152–167, http://dx.doi.org/10.1016/j.jpdc.2022.03.009.

[60] R. Kumar, N. Marchang, R. Tripathi, Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain, in: 2020 International Conference on COMmunication Systems & NETworkS, COMSNETS, 2020, pp. 1–5, http://dx.doi.org/10.1109/COMSNETS48256.2020.9027313.

[61] J.H. Beinke, C. Fitte, F. Teuteberg, Towards a stakeholder-oriented blockchain-based architecture for electronic health records: Design science research study, J. Med. Internet Res. 21 (2019) e13585, http://dx.doi.org/10.2196/13585.

[62] A.H. Mayer, C.A. da Costa, R. da R. Righi, Electronic health records in a blockchain: A systematic review, Health Inform. J. 26 (2020) 1273–1288, http://dx.doi.org/10.1177/1460458219866350.

[63] R.N. Nortey, L. Yue, P.R. Agdedanu, M. Adjeisah, Privacy module for distributed electronic health records(EHRs) using the blockchain, in: 2019 IEEE 4th International Conference on Big Data Analytics, ICBDA, 2019, pp. 369–374, http://dx.doi.org/10.1109/ICBDA.2019.8713188.

[64] H.-A. Lee, H.-H. Kung, J.G. Udayasankaran, B. Kijsanayotin, A.B. Marcelo, L.R. Chao, C.-Y. Hsu, An architecture and management platform for blockchain-based personal health record exchange: Development and usability study, J. Med. Internet Res. 22 (2020) e16748, http://dx.doi.org/10.2196/16748.

[65] A. Yazdinejad, G. Srivastava, R.M. Parizi, A. Dehghantanha, K.-K.R. Choo, M. Aledhari, Decentralized authentication of distributed patients in hospital networks using blockchain, IEEE J. Biomed. Health Inform. 24 (2020) 2146–2156, http://dx.doi.org/10.1109/JBHI.2020.2969648.

[66] S.L. Cichosz, M.N. Stausholm, T. Kronborg, P. Vestergaard, O. Hejlesen, How to use blockchain for diabetes health care data and access management: An operational concept, J. Diabetes Sci. Technol. (2018) http://dx.doi.org/10.1177/1932296818790281.

[67] Y. Zhuang, L.R. Sheets, Y.-W. Chen, Z.-Y. Shae, J.J.P. Tsai, C.-R. Shyu, A patient-centric health information exchange framework using blockchain technology, IEEE J. Biomed. Health Inform. 24 (2020) 2169–2176, http://dx.doi.org/10.1109/JBHI.2020.2993072.

[68] A. Ali, M.A. Almaiah, F. Hajjej, M.F. Pasha, O.H. Fang, R. Khan, J. Teo, M. Zakarya, An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network, Sensors 22 (2022) 572, http://dx.doi.org/10.3390/s22020572.

[69] M.A. Almaiah, F. Hajjej, A. Ali, M.F. Pasha, O. Almomani, A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS, Sensors 22 (2022) 1448, http://dx.doi.org/10.3390/s22041448.

[70] A. Ali, H.A. Rahim, M.F. Pasha, R. Dowsley, M. Masud, J. Ali, M. Baz, Security, Privacy, And reliability in digital healthcare systems using blockchain, Electronics 10 (2021) 2034, http://dx.doi.org/10.3390/electronics10162034.

[71] A. Ali, H.A. Rahim, J. Ali, M.F. Pasha, M. Masud, A.U. Rehman, C. Chen, M. Baz, A novel secure blockchain framework for accessing electronic health records using multiple certificate authority, Appl. Sci. 11 (2021) 9999, http://dx.doi.org/10.3390/app11219999.

[72] F. Zerka, V. Urovi, A. Vaidyanathan, S. Barakat, R.T.H. Leijenaar, S. Walsh, H. Gabrani-Juma, B. Miraglio, H.C. Woodruff, M. Dumontier, P. Lambin, Blockchain for privacy preserving and trustworthy distributed machine learning in multicentric medical imaging (C-DistriM), IEEE Access 8 (2020) 183939–183951, http://dx.doi.org/10.1109/ACCESS.2020.3029445.

[73] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, Y. Zhang, A smart-contract-based access control framework for cloud smart healthcare system, IEEE Internet Things J. 8 (2021) 5914–5925, http://dx.doi.org/10.1109/JIOT.2020.3032997.

[74] G. Tripathi, M.A. Ahad, S. Paiva, S2HS- a blockchain based approach for smart healthcare system, Healthcare 8 (2020) 100391, http://dx.doi.org/10.1016/j.hjdsi.2019.100391.

[75] M. Debe, K. Salah, R. Jayaraman, J. Arshad, Blockchain-based verifiable tracking of resellable returned drugs, IEEE Access 8 (2020) 205848–205862, http://dx.doi.org/10.1109/ACCESS.2020.3037363.

[76] Y.R. Park, E. Lee, W. Na, S. Park, Y. Lee, J.-H. Lee, Is blockchain technology suitable for managing personal health records? Mixed-methods study to test feasibility, J. Med. Internet Res. 21 (2019) e12533, http://dx.doi.org/10.2196/12533.

[77] Sheela. K., C. Priya, Enabling the efficiency of blockchain technology in tele-healthcare with enhanced EMR, in: 2020 International Conference on Computer Science, Engineering and Applications, ICCSEA, IEEE, Gunupur, India, 2020, pp. 1–6, http://dx.doi.org/10.1109/ICCSEA49143.2020.9132922.

[78] M.M. Madine, A.A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. Pesic, S. Ellahham, Blockchain for giving patients control over their medical records, IEEE Access 8 (2020) 193102–193115, http://dx.doi.org/10.1109/ACCESS.2020.3032553.

[79] A.E.B. Tomaz, J.C.D. Nascimento, A.S. Hafid, J.N.D. Souza, Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain, IEEE Access 8 (2020) 204441–204458, http://dx.doi.org/10.1109/ACCESS.2020.3036811.

[80] A. Clim, R.D. Zota, R. Constantinescu, Data exchanges based on blockchain in m-health applications, Procedia Comput. Sci. 160 (2019) 281–288, http://dx.doi.org/10.1016/j.procs.2019.11.088.

[81] T. Motohashi, T. Hirano, K. Okumura, M. Kashiyama, D. Ichikawa, T. Ueno, Secure and scalable mhealth data management using blockchain combined with client hashchain: System design and validation, J. Med. Internet Res. 21 (2019) e13385, http://dx.doi.org/10.2196/13385.

[82] H. Huang, P. Zhu, F. Xiao, X. Sun, Q. Huang, A blockchain-based scheme for privacy-preserving and secure sharing of medical data, Comput. Secur. 99 (2020) 102010, http://dx.doi.org/10.1016/j.cose.2020.102010.

[83] G.S. Aujla, A. Jindal, A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring, IEEE J. Sel. Areas Commun. 39 (2021) 491–499, http://dx.doi.org/10.1109/JSAC.2020.3020655.

[84] L. Ismail, H. Materwala, Y. Sharaf, BlockHR – a blockchain-based healthcare records management framework: Performance evaluation and comparison with client/server architecture, in: 2020 International Symposium on Networks, Computers and Communications, ISNCC, 2020, pp. 1–8, http://dx.doi.org/10.1109/ISNCC49221.2020.9297216.

[85] E.M. Abou-Nassar, A.M. Iliyasu, P.M. El-Kafrawy, O.-Y. Song, A.K. Bashir, A.A.A. El-Latif, DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems, IEEE Access 8 (2020) 111223–111238, http://dx.doi.org/10.1109/ACCESS.2020.2999468.

[86] R. Akkaoui, X. Hei, W. Cheng, EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange, IEEE Access 8 (2020) 113467–113486, http://dx.doi.org/10.1109/ACCESS.2020.3003575.

[87] V. Jaiman, V. Urovi, A consent model for blockchain-based health data sharing platforms, IEEE Access 8 (2020) 143734–143745, http://dx.doi.org/10.1109/ACCESS.2020.3014565.

[88] C.-T. Li, D.-H. Shih, C.-C. Wang, C.-L. Chen, C.-C. Lee, A blockchain based data aggregation and group authentication scheme for electronic medical system, IEEE Access 8 (2020) 173904–173917, http://dx.doi.org/10.1109/ACCESS.2020.3025898.

[89] A.F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J.M.R.S. Tavares, V.H.C. de Albuquerque, A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform, Cognit. Syst. Res. 52 (2018) 1–11, http://dx.doi.org/10.1016/j.cogsys.2018.05.004.

[90] P. Li, C. Xu, H. Jin, C. Hu, Y. Luo, Y. Cao, J. Mathew, Y. Ma, ChainSDI: A software-defined infrastructure for regulation-compliant home-based healthcare services secured by blockchains, IEEE Syst. J. 14 (2020) 2042–2053, http://dx.doi.org/10.1109/JSYST.2019.2937930.

[91] N.A. Asad, Md.T. Elahi, A.A. Hasan, M.A. Yousuf, Permission-based blockchain with proof of authority for secured healthcare data sharing, in: 2020 2nd International Conference on Advanced Information and Communication Technology, ICAICT, 2020, pp. 35–40, http://dx.doi.org/10.1109/ICAICT51780.2020.9333488.

[92] A.R. Lee, M.G. Kim, I.K. Kim, SHAREChain: Healthcare data sharing framework using blockchain-registry and FHIR, in: 2019 IEEE International Conference on Bioinformatics and Biomedicine, BIBM, 2019, pp. 1087–1090, http://dx.doi.org/10.1109/BIBM47256.2019.8983415.

[93] P. Ndayizigamiye, S. Dube, Potential adoption of blockchain technology to enhance transparency and accountability in the public healthcare system in South Africa, in: 2019 International Multidisciplinary Information Technology and Engineering Conference, IMITEC, 2019, pp. 1–5, http://dx.doi.org/10.1109/IMITEC45504.2019.9015920.

[94] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, S. Ellahham, A blockchain-based approach for drug traceability in healthcare supply chain, IEEE Access 9 (2021) 9728–9743, http://dx.doi.org/10.1109/ACCESS.2021.3049920.

[95] U. Goel, R. Ruhl, P. Zavarsky, Using healthcare authority and patient blockchains to develop a tamper-proof record tracking system, in: 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security, IDS, 2019, pp. 25–30, http://dx.doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00016.

[96] O. Attia, I. Khoufi, A. Laouiti, C. Adjih, An IoT-blockchain architecture based on hyperledger framework for healthcare monitoring application, in: 2019 10th IFIP International Conference on New Technologies, Mobility and Security, NTMS, 2019, pp. 1–5, http://dx.doi.org/10.1109/NTMS.2019.8763849.

[97] A. Abugabah, N. Nizamuddin, A.A. Alzubi, Decentralized telemedicine framework for a smart healthcare ecosystem, IEEE Access 8 (2020) 166575–166588, http://dx.doi.org/10.1109/ACCESS.2020.3021823.

[98] H. Kordestani, K. Barkaoui, W. Zahran, HapiChain: A blockchain-based framework for patient-centric telemedicine, in: 2020 IEEE 8th International Conference on Serious Games and Applications for Health (SeGAH), IEEE, Vancouver, BC, Canada, 2020, pp. 1–6, http://dx.doi.org/10.1109/SeGAH49190.2020.9201726.

[99] A. Celesti, A. Ruggeri, M. Fazio, A. Galletta, M. Villari, A. Romano, Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital IoT clouds, Sensors 20 (2020) 2590, http://dx.doi.org/10.3390/s20092590.

[100] R. Gupta, A. Shukla, S. Tanwar, Aayush: A smart contract-based telesurgery system for healthcare 4.0, in: 2020 IEEE International Conference on Communications Workshops (ICC Workshops), 2020, pp. 1–6, http://dx.doi.org/10.1109/ICCWorkshops49005.2020.9145044.

[101] R. Gupta, U. Thakker, S. Tanwar, M.S. Obaidat, K.-F. Hsiao, BITS: A blockchain-driven intelligent scheme for telesurgery system, in: 2020 International Conference on Computer, Information and Telecommunication Systems, CITS, 2020, pp. 1–5, http://dx.doi.org/10.1109/CITS49457.2020.9232662.

[102] R. Gupta, S. Tyagi, S. Tanwar, M. Obaidat, B. Sadoun, HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0, 2019, http://dx.doi.org/10.1109/CITS.2019.8862127.

[103] K. Mannaro, G. Baralla, A. Pinna, S. Ibba, A blockchain approach applied to a teledermatology platform in the sardinian region (Italy), Information 9 (2018) 44, http://dx.doi.org/10.3390/info9020044.

[104] S. Juyal, S. Sharma, A. Harbola, A.S. Shukla, Privacy and security of IoT based skin monitoring system using blockchain approach, in: 2020 IEEE International Conference on Electronics, Computing and Communication Technologies, CONECCT, 2020, pp. 1–5, http://dx.doi.org/10.1109/CONECCT50063.2020.9198409.

[105] Y. Ji, J. Zhang, J. Ma, C. Yang, X. Yao, BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems, J. Med. Syst. 42 (2018) http://dx.doi.org/10.1007/s10916-018-0998-2.

[106] R.M. Patil, R. Kulkarni, Universal storage and analytical framework of health records using blockchain data from wearable data devices, in: 2020 2nd International Conference on Innovative Mechanisms for Industry Applications, ICIMIA, 2020, pp. 311–317, http://dx.doi.org/10.1109/ICIMIA48430.2020.9074909.

[107] S. Son, J. Lee, M. Kim, S. Yu, A.K. Das, Y. Park, Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain, IEEE Access 8 (2020) 192177–192191, http://dx.doi.org/10.1109/ACCESS.2020.3032680.

[108] M.A. Rahman, M. Rashid, S. Barnes, M.S. Hossain, E. Hassanain, M. Guizani, An IoT and blockchain-based multi-sensory in-home quality of life framework for cancer patients, in: 2019 15th International Wireless Communications Mobile Computing Conference, IWCMC, 2019, pp. 2116–2121, http://dx.doi.org/10.1109/IWCMC.2019.8766496.

[109] O. Dib, C. Huyart, K. Toumi, A novel data exploitation framework based on blockchain, Perv. Mob. Comput. 61 (2020) 101104, http://dx.doi.org/10.1016/j.pmcj.2019.101104.

[110] M.U. Hassan, M.H. Rehmani, J. Chen, Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions, Future Gener. Comput. Syst. 97 (2019) 512–529, http://dx.doi.org/10.1016/j.future.2019.02.060.

[111] R. Henry, A. Herzberg, A. Kate, Blockchain access privacy: Challenges and directions, IEEE Secur. Priv. 16 (2018) 38–45, http://dx.doi.org/10.1109/MSP.2018.3111245.

[112] M. Zhang, S. Wang, P. Zhang, L. He, X. Li, S. Zhou, Protecting data privacy for permissioned blockchains using identity-based encryption, in: 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference, ITNEC, 2019, pp. 602–605, http://dx.doi.org/10.1109/ITNEC.2019.8729244.

[113] E.J. De Aguiar, B.S. Faiçal, B. Krishnamachari, J. Ueyama, A survey of blockchain-based strategies for healthcare, ACM Comput. Surv. 53 (2020) 1–27, http://dx.doi.org/10.1145/3376915.

[114] A. Battah, M. Madine, H. Alzaabi, I. Yaqoob, K. Salah, R. Jayaraman, Blockchain-based multi-party authorization for accessing IPFS encrypted data, 2020, http://dx.doi.org/10.36227/techrxiv.12788306.v1.

[115] L. Guo, H. Xie, Y. Li, Data encryption based blockchain and privacy preserving mechanisms towards big data, J. Vis. Commun. Image Represent. 70 (2020) 102741, http://dx.doi.org/10.1016/j.jvcir.2019.102741.

[116] A. Shamir, Identity-based cryptosystems and signature schemes, in: CRYPTO, 1984, http://dx.doi.org/10.1007/3-540-39568-7_5.

[117] M. Mambo, E. Okamoto, Proxy cryptosystems: Delegation of the power to decrypt ciphertexts, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E80-A (1997) 54–63.

[118] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Healthchain: A blockchain-based privacy preserving scheme for large-scale health data, IEEE Internet Things J. 6 (2019) 8770–8781, http://dx.doi.org/10.1109/JIOT.2019.2923525.

[119] H.T.T. Truong, M. Almeida, G. Karame, C. Soriente, Towards secure and decentralized sharing of IoT data, in: 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 176–183, http://dx.doi.org/10.1109/Blockchain.2019.00031.

[120] Y. Du, J. Liu, Z. Guan, H. Feng, A medical information service platform based on distributed cloud and blockchain, in: 2018 IEEE International Conference on Smart Cloud (SmartCloud), 2018, pp. 34–39, http://dx.doi.org/10.1109/SmartCloud.2018.00014.

[121] M. Blaze, G. Bleumer, M. Strauss, Divertible protocols and atomic proxy cryptography, 1998, pp. 127–144, http://dx.doi.org/10.1007/BFb0054122.

[122] D. Nuez, I. Agudo, J. and Lopez, Proxy re-encryption, J. Netw. Comput. Appl. 87 (2017) 193–209, http://dx.doi.org/10.1016/j.jnca.2017.03.005.

[123] V. Mahore, P. Aggarwal, N. Andola, Raghav, S. Venkatesan, Secure and privacy focused electronic health record management system using permissioned blockchain, in: 2019 IEEE Conference on Information and Communication Technology, 2019, pp. 1–6, http://dx.doi.org/10.1109/CICT48419.2019.9066204.

[124] D.K. Meena, R. Dwivedi, S. Shukla, Preserving patient's privacy using proxy re-encryption in permissioned blockchain, in: 2019 Sixth International Conference on Internet of Things: Systems, Management and Security, IOTSMS, 2019, pp. 450–457, http://dx.doi.org/10.1109/IOTSMS48152.2019.8939226.

[125] S. Cui, M.R. Asghar, G. Russello, Towards blockchain-based scalable and trustworthy file sharing. (n.d.) 2.

[126] Y. Wang, A. Zhang, P. Zhang, H. Wang, Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain, IEEE Access 7 (2019) 136704–136719, http://dx.doi.org/10.1109/ACCESS.2019.2943153.

[127] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, 2006, http://eprint.iacr.org/2006/309 (accessed November 11, 2020).

[128] Y. Rahulamathavan, R.C.-. Phan, M. Rajarajan, S. Misra, A. Kondoz, Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption, in: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS, 2017, pp. 1–6, http://dx.doi.org/10.1109/ANTS.2017.8384164.

[129] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: 2007 IEEE Symposium on Security and Privacy (SP '07), 2007, pp. 321–334, http://dx.doi.org/10.1109/SP.2007.11.

[130] Q. Su, R. Zhang, R. Xue, P. Li, Revocable attribute-based signature for blockchain-based healthcare system, IEEE Access 8 (2020) 127884–127896, http://dx.doi.org/10.1109/ACCESS.2020.3007691.

[131] The idea of smart contracts | Satoshi Nakamoto institute, 2021, (n.d.). https://nakamotoinstitute.org/the-idea-of-smart-contracts/ (accessed February 8, 2021).

[132] L. Hirtan, P. Krawiec, C. Dobre, J.M. Batalla, Blockchain-based approach for e-health data access management with privacy protection, in: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD, 2019, pp. 1–7, http://dx.doi.org/10.1109/CAMAD.2019.8858469.

[133] L. Garg, E. Chukwu, N. Nasser, C. Chakraborty, G. Garg, Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model, IEEE Access 8 (2020) 159402–159414, http://dx.doi.org/10.1109/ACCESS.2020.3020513.

[134] G.G. Dagher, J. Mohler, M. Milojkovic, P.B. Marella, Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustain. Cities Soc. 39 (2018) 283–297, http://dx.doi.org/10.1016/j.scs.2018.02.014.

[135] J. Li, M.H. Au, W. Susilo, D. Xie, K. Ren, Attribute-based signature and its applications, in: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, Association for Computing Machinery, New York, NY, USA, 2010, pp. 60–69, http://dx.doi.org/10.1145/1755688.1755697.

[136] H. Guo, W. Li, E. Meamari, C.-C. Shen, M. Nejad, Attribute-based multi-signature and encryption for EHR management: A blockchain-based solution, 2020, arXiv:2002.11078 [cs]. http://arxiv.org/abs/2002.11078 (accessed February 4, 2021).

[137] R.L. Rivest, A. Shamir, Y. Tauman, How to leak a secret, in: C. Boyd (Ed.), Advances in Cryptology — ASIACRYPT 2001, Springer, Berlin, Heidelberg, 2001, pp. 552–565, http://dx.doi.org/10.1007/3-540-45682-1_32.

[138] X. Li, Y. Mei, J. Gong, F. Xiang, S. Zhixin, A blockchain privacy protection scheme based on ring signature, IEEE Access PP (2020) 1, http://dx.doi.org/10.1109/ACCESS.2020.2987831.

[139] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, Y. Liu, Privacy-preserving blockchain-based federated learning for IoT devices, 2020, arXiv:1906.10893 [cs, eess]. http://arxiv.org/abs/1906.10893 (accessed November 11, 2020).

[140] A. Zhang, X. Lin, Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain, J. Med. Syst. 42 (2018) 140, http://dx.doi.org/10.1007/s10916-018-0995-5.

[141] A. Nagar, Privacy-preserving blockchain based federated learning with differential data sharing, 2019, arXiv:1912.04859 [cs]. http://arxiv.org/abs/1912.04859 (accessed March 28, 2021).

[142] D.L. Chaum, Untraceable electronic mail, return addresses, and digital pseudonyms, Commun. ACM 24 (1981) 84–90, http://dx.doi.org/10.1145/358549.358563.

[143] R. Xiao, W. Ren, T. Zhu, K.R. Choo, A mixing scheme using a decentralized signature protocol for privacy protection in bitcoin blockchain, IEEE Trans. Dependable Secure Comput. (2019) 1, http://dx.doi.org/10.1109/TDSC.2019.2938953.

[144] O. Goldreich, Y. Oren, Definitions and properties of zero-knowledge proof systems, J. Cryptol. 7 (1994) 1–32, http://dx.doi.org/10.1007/BF00195207.

[145] U. Fiege, A. Fiat, A. Shamir, Zero knowledge proofs of identity, in: Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing, Association for Computing Machinery, New York, NY, USA, 1987, pp. 210–217, http://dx.doi.org/10.1145/28395.28419.

[146] A. Ulhaq, O. Burmeister, COVID-19 imaging data privacy by federated learning design: A theoretical framework, 2020, arXiv:2010.06177 [cs]. http://arxiv.org/abs/2010.06177 (accessed February 20, 2021).

[147] J.L. Raisaro, F. Marino, J. Troncoso-Pastoriza, R. Beau-Lejdstrom, R. Bellazzi, R. Murphy, E.V. Bernstam, H. Wang, M. Bucalo, Y. Chen, A. Gottlieb, A. Harmanci, M. Kim, Y. Kim, J. Klann, C. Klersy, B.A. Malin, M. Méan, F. Prasser, L. Scudeller, A. Torkamani, J. Vaucher, M. Puppala, S.T.C. Wong, M. Frenkel-Morgenstern, H. Xu, B.M. Musa, A.G. Habib, T. Cohen, A. Wilcox, H.M. Salihu, H. Sofia, X. Jiang, J.P. Hubaux, SCOR: A secure international informatics infrastructure to investigate COVID-19, J. Am. Med. Inform. Assoc.: JAMIA 27 (2020) 1721–1726, http://dx.doi.org/10.1093/jamia/ocaa172.

[148] M.N. Galtier, C. Marini, Substra: a framework for privacy-preserving, traceable and collaborative machine learning, 2019, arXiv:1910.11567 [cs]. http://arxiv.org/abs/1910.11567 (accessed February 4, 2021).

[149] Y. Guo, F. Liu, Z. Cai, L. Chen, N. Xiao, FEEL: A federated edge learning system for efficient and privacy-preserving mobile healthcare, 2020, http://dx.doi.org/10.1145/3404397.3404410.

[150] N. Truong, K. Sun, S. Wang, F. Guitton, Y. Guo, Privacy preservation in federated learning: An insightful survey from the GDPR perspective, 2021, arXiv:2011.05411 [cs]. http://arxiv.org/abs/2011.05411 (accessed March 9, 2021).

[151] Q. Yang, Y. Liu, T. Chen, Y. Tong, Federated machine learning: Concept and applications, 2019, arXiv:1902.04885 [cs]. http://arxiv.org/abs/1902.04885 (accessed March 29, 2021).

[152] Federated learning for image classification | TensorFlow federated, TensorFlow, 2021, (n.d.). https://www.tensorflow.org/federated/tutorials/federated_learning_for_image_classification (accessed March 6, 2021).

[153] FATE — FATE documentation, 2021, (n.d.). https://fate.readthedocs.io/en/latest/ (accessed March 6, 2021).

[154] K. Yang, Y. Shi, Y. Zhou, Z. Yang, L. Fu, W. Chen, Federated machine learning for intelligent IoT via reconfigurable intelligent surface, IEEE Netw. 34 (2020) 16–22, http://dx.doi.org/10.1109/MNET.011.2000045.

[155] M. Hao, H. Li, G. Xu, Z. Liu, Z. Chen, Privacy-aware and resource-saving collaborative learning for healthcare in cloud computing, 2020, http://dx.doi.org/10.1109/ICC40277.2020.9148979.

[156] T.-D. Cao, T. Truong-Huu, H. Tran, K. Tran, A federated learning framework for privacy-preserving and parallel training, 2020, arXiv:2001.09782 [cs]. http://arxiv.org/abs/2001.09782 (accessed February 18, 2021).

[157] W. Zhang, T. Zhou, Q. Lu, X. Wang, C. Zhu, H. Sun, Z. Wang, S.K. Lo, F.-Y. Wang, Dynamic fusion based federated learning for COVID-19 detection, 2020, arXiv:2009.10401 [cs]. http://arxiv.org/abs/2009.10401 (accessed February 19, 2021).

[158] H. Chen, H. Li, G. Xu, Y. Zhang, X. Luo, Achieving privacy-preserving federated learning with irrelevant updates over E-health applications, in: ICC 2020-2020 IEEE International Conference on Communications, ICC, 2020, pp. 1–6, http://dx.doi.org/10.1109/ICC40277.2020.9149385.

[159] O. Choudhury, A. Gkoulalas-Divanis, T. Salonidis, I. Sylla, Y. Park, G. Hsu, A. Das, Anonymizing data for privacy-preserving federated learning, 2020, arXiv:2002.09096 [cs]. http://arxiv.org/abs/2002.09096 (accessed February 18, 2021).

[160] R. Shokri, M. Stronati, C. Song, V. Shmatikov, Membership inference attacks against machine learning models, in: 2017 IEEE Symposium on Security and Privacy, SP, 2017, pp. 3–18, http://dx.doi.org/10.1109/SP.2017.41.

[161] M. Fredrikson, S. Jha, T. Ristenpart, Model inversion attacks that exploit confidence information and basic countermeasures, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ACM, Denver Colorado USA, 2015, pp. 1322–1333, http://dx.doi.org/10.1145/2810103.2813677.

[162] C.A. Choquette-Choo, F. Tramer, N. Carlini, N. Papernot, Label-only membership inference attacks, 2021, arXiv:2007.14321 [cs, stat]. http://arxiv.org/abs/2007.14321 (accessed March 8, 2021).

[163] L. Lyu, H. Yu, Q. Yang, Threats to federated learning: A survey, 2020, arXiv:2003.02133 [cs, stat]. http://arxiv.org/abs/2003.02133 (accessed March 2, 2021).

[164] X. Chen, C. Liu, B. Li, K. Lu, D. Song, Targeted backdoor attacks on deep learning systems using data poisoning, 2017, arXiv:1712.05526 [cs]. http://arxiv.org/abs/1712.05526 (accessed March 29, 2021).

[165] V. Valli Kumari, R.P. Reddy Sadi, (K, l)f-anonymity: A federated learning approach for personalized privacy preserving data publishing, J. Adv. Res. Dyn. Control Syst. 12 (2020) 250–262, http://dx.doi.org/10.5373/JARDCS/V12SP6/SP20201030.

[166] C. Dwork, Differential privacy: A survey of results, in: M. Agrawal, D. Du, Z. Duan, A. Li (Eds.), Theory and Applications of Models of Computation, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 1–19, http://dx.doi.org/10.1007/978-3-540-79228-4_1.

[167] R. Hu, Y. Guo, H. Li, Q. Pei, Y. Gong, Privacy-preserving personalized federated learning, in: ICC 2020-2020 IEEE International Conference on Communications, ICC, 2020, pp. 1–6, http://dx.doi.org/10.1109/ICC40277.2020.9149207.

[168] G.A. Kaissis, M.R. Makowski, D. Rückert, R.F. Braren, Secure, privacy-preserving and federated machine learning in medical imaging, Nat. Mach. Intell. 2 (2020) 305–311, http://dx.doi.org/10.1038/s42256-020-0186-1.

[169] N. Rodríguez-Barroso, G. Stipcich, D. Jiménez-López, J.A. Ruiz-Millán, E. Martínez-Cámara, G. González-Seco, M.V. Luzón, M.A. Veganzones, F. Herrera, Federated learning and differential privacy: Software tools analysis, the sherpa.ai FL framework and methodological guidelines for preserving data privacy, Inform. Fusion 64 (2020) 270–292, http://dx.doi.org/10.1016/j.inffus.2020.07.009.

[170] O. Choudhury, A. Gkoulalas-Divanis, T. Salonidis, I. Sylla, Y. Park, G. Hsu, A. Das, Differential privacy-enabled federated learning for sensitive health data, 2020, arXiv:1910.02578 [cs]. http://arxiv.org/abs/1910.02578 (accessed February 20, 2021).

[171] L. Zhang, Y. Zheng, R. Kantoa, A review of homomorphic encryption and its applications, in: Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, BEL, 2016, pp. 97–106.

[172] K.G. Kogos, K.S. Filippova, A.V. Epishkina, Fully homomorphic encryption schemes: The state of the art, in: 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2017, pp. 463–466, http://dx.doi.org/10.1109/EIConRus.2017.7910591.

[173] Y. Liu, Y. Kang, C. Xing, T. Chen, Q. Yang, Secure federated transfer learning, IEEE Intell. Syst. 35 (2020) 70–82, http://dx.doi.org/10.1109/MIS.2020.2988525.

[174] M. Alloghani, M.M. Alani, D. Al-Jumeily, T. Baker, J. Mustafina, A. Hussain, A.J. Aljaaf, A systematic review on the status and progress of homomorphic encryption technologies, J. Inf. Secur. Appl. 48 (2019) 102362, http://dx.doi.org/10.1016/j.jisa.2019.102362.

[175] C. Zhang, S. Li, J. Xia, W. Wang, F. Yan, Y. Liu, BatchCrypt: Efficient homomorphic encryption for cross-silo federated learning. (n.d.) 15.

[176] Y. Chen, F. Luo, T. Li, T. Xiang, Z. Liu, J. Li, A training-integrity privacy-preserving federated learning scheme with trusted execution environment, Inform. Sci. 522 (2020) 69–79, http://dx.doi.org/10.1016/j.ins.2020.02.037.

[177] A.C. Yao, How to generate and exchange secrets, in: 27th Annual Symposium on Foundations of Computer Science (Sfcs 1986), 1986, pp. 162–167, http://dx.doi.org/10.1109/SFCS.1986.25.

[178] C. Zhao, S. Zhao, M. Zhao, Z. Chen, C.-Z. Gao, H. Li, Y. Tan, Secure multi-party computation: Theory, practice and applications, Inform. Sci. 476 (2019) 357–372, http://dx.doi.org/10.1016/j.ins.2018.10.024.

[179] Q. Zhang, P. Palacharla, M. Sekiya, J. Suga, T. Katagiri, Demo: A blockchain based protocol for federated learning. (n.d.) 2.

[180] A.R. Javed, M.A. Hassan, F. Shahzad, W. Ahmed, S. Singh, T. Baker, T.R. Gadekallu, Integration of blockchain technology and federated learning in vehicular (IoT) networks: A comprehensive survey, Sensors (Basel) 22 (2022) 4394, http://dx.doi.org/10.3390/s22124394.

[181] H. Kim, J. Park, M. Bennis, S.-L. Kim, Blockchained on-device federated learning, IEEE Commun. Lett. 24 (2019) http://dx.doi.org/10.1109/LCOMM.2019.2921755.

[182] Y. Hu, W. Xia, J. Xiao, C. Wu, GFL: A decentralized federated learning framework based on blockchain, 2020, arXiv:2010.10996 [cs]. http://arxiv.org/abs/2010.10996 (accessed November 12, 2020).

[183] L. Cui, Y. Qu, G. Xie, D. Zeng, R. Li, S. Shen, S. Yu, Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures, IEEE Trans. Ind. Inform. 18 (2022) 3492–3500, http://dx.doi.org/10.1109/TII.2021.3107783.

[184] X. Wu, Z. Wang, J. Zhao, Y. Zhang, Y. Wu, Fedbc: Blockchain-based decentralized federated learning, in: 2020 IEEE International Conference on Artificial Intelligence and Computer Applications, ICAICA, 2020, pp. 217–221, http://dx.doi.org/10.1109/ICAICA50127.2020.9182705.

[185] Y. Lu, X. Huang, Y. Dai, S. Maharjan, Y. Zhang, Blockchain and federated learning for privacy-preserved data sharing in industrial IoT, IEEE Trans. Ind. Inform. 16 (2020) 4177–4186, http://dx.doi.org/10.1109/TII.2019.2942190.

[186] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, W. Luo, DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive, IEEE Trans. Dependable Secure Comput. (2019) 1, http://dx.doi.org/10.1109/TDSC.2019.2952332.

[187] S. Fan, H. Zhang, Y. Zeng, W. Cai, Hybrid blockchain-based resource trading system for federated learning in edge computing, IEEE Internet Things J. 8 (2021) 2252–2264, http://dx.doi.org/10.1109/JIOT.2020.3028101.

[188] K. Toyoda, J. Zhao, A.N.S. Zhang, P.T. Mathiopoulos, Blockchain-enabled federated learning with mechanism design, IEEE Access 8 (2020) 219744–219756, http://dx.doi.org/10.1109/ACCESS.2020.3043037.

[189] Y. Liu, S. Sun, Z. Ai, S. Zhang, Z. Liu, H. Yu, FedCoin: A peer-to-peer payment system for federated learning, 2020, arXiv:2002.11711 [cs, stat]. http://arxiv.org/abs/2002.11711 (accessed April 5, 2021).

[190] P.C.M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, M. Atiquzzaman, A trustworthy privacy preserving framework for machine learning in industrial IoT systems, IEEE Trans. Ind. Inform. 16 (2020) 6092–6102, http://dx.doi.org/10.1109/TII.2020.2974555.

[191] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, M. Guizani, Reliable federated learning for mobile networks, IEEE Wireless Commun. 27 (2020) 72–80, http://dx.doi.org/10.1109/MWC.001.1900119.

[192] S. Aich, N.K. Sinai, S. Kumar, M. Ali, Y.R. Choi, M.-I. Joo, H.-C. Kim, Protecting personal healthcare record using blockchain federated learning technologies, in: 2021 23rd International Conference on Advanced Communication Technology, ICACT, 2021, pp. 109–112, http://dx.doi.org/10.23919/ICACT51234.2021.9370566.

[193] Q. Wang, Y. Guo, X. Wang, T. Ji, L. Yu, P. Li, AI at the edge: Blockchain-empowered secure multiparty learning with heterogeneous models, IEEE Internet Things J. 7 (2020) 9600–9610, http://dx.doi.org/10.1109/JIOT.2020.2987843.

[194] J. Kang, Z. Xiong, C. Jiang, Y. Liu, S. Guo, Y. Zhang, D. Niyato, C. Leung, C. Miao, Scalable and communication-efficient decentralized federated edge learning with multi-blockchain framework, 2020, arXiv:2008.04743 [cs]. http://arxiv.org/abs/2008.04743 (accessed April 5, 2021).

[195] C. Korkmaz, H.E. Kocas, A. Uysal, A. Masry, O. Ozkasap, B. Akgun, Chain FL: Decentralized federated machine learning via blockchain, in: 2020 Second International Conference on Blockchain Computing and Applications, BCCA, 2020, pp. 140–146, http://dx.doi.org/10.1109/BCCA50787.2020.9274451.

[196] Y. Wang, Z. Su, N. Zhang, A. Benslimane, Learning in the air: Secure federated learning for UAV-assisted crowdsensing, IEEE Trans. Netw. Sci. Eng. (2020) 1, http://dx.doi.org/10.1109/TNSE.2020.3014385.

[197] Y. Qu, L. Gao, T.H. Luan, Y. Xiang, S. Yu, B. Li, G. Zheng, Decentralized privacy using blockchain-enabled federated learning in fog computing, IEEE Internet Things J. 7 (2020) 5171–5183, http://dx.doi.org/10.1109/JIOT.2020.2977383.

[198] K. Demertzis, Blockchained federated learning for threat defense. (n.d.) 12.

[199] S. Ma, Y. Cao, L. Xiong, Transparent contribution evaluation for secure federated learning on blockchain, 2021, arXiv:2101.10572 [cs]. http://arxiv.org/abs/2101.10572 (accessed April 4, 2021).

[200] O. Samuel, A.B. Omojo, A.M. Onuja, Y. Sunday, P. Tiwari, D. Gupta, G. Hafeez, A.S. Yahaya, O.J. Fatoba, S. Shamshirband, IoMT: A COVID-19 healthcare system driven by federated learning and blockchain, IEEE J. Biomed. Health Inform. PP (2022) http://dx.doi.org/10.1109/JBHI.2022.3143576.

[201] Z. Wang, L. Cai, X. Zhang, C. Choi, X. Su, A COVID-19 auxiliary diagnosis based on federated learning and blockchain, Comput. Math. Methods Med. 2022 (2022) 1–12, http://dx.doi.org/10.1155/2022/7078764.

[202] M.Y. Jabarulla, H.-N. Lee, A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications, Healthcare 9 (2021) 1019, http://dx.doi.org/10.3390/healthcare9081019.

[203] R. Kumar, A.A. Khan, S. Zhang, W. Wang, Y. Abuidris, W. Amin, J. Kumar, Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging, 2020, arXiv:2007.06537 [cs, eess]. http://arxiv.org/abs/2007.06537 (accessed November 17, 2020).

[204] M.A. Rahman, M.S. Hossain, M.S. Islam, N.A. Alrajeh, G. Muhammad, Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach, IEEE Access 8 (2020) 205071–205087, http://dx.doi.org/10.1109/ACCESS.2020.3037474.

[205] Y. Liu, W. Yu, Z. Ai, G. Xu, L. Zhao, Z. Tian, A blockchain-empowered federated learning in healthcare-based cyber physical systems, IEEE Trans. Netw. Sci. Eng. (2022) 1, http://dx.doi.org/10.1109/TNSE.2022.3168025.

[206] S.K. Lo, Y. Liu, Q. Lu, C. Wang, X. Xu, H.-Y. Paik, L. Zhu, Towards trustworthy AI: Blockchain-based architecture design for accountability and fairness of federated learning systems, IEEE Internet Things J. (2022) 1, http://dx.doi.org/10.1109/JIOT.2022.3144450.