BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **24**, No 1
Sofia • 2024 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2024-0003

A Review on State-of-Art Blockchain Schemes for Electronic Health Records Management

Jayapriya Jayabalan, N. Jeyanthi

School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Tamilnadu 632014, India
E-mails: jayapriya.jayabalan2018@vitstudent.ac.in njeyanthi@vit.ac.in

Abstract: *In today's world, Electronic Health Records* (*EHR*) *are highly segregated and available only within the organization with which the patient is associated. If a patient has to visit another hospital there is no secure way for hospitals to communicate and share medical records. Hence, people are always asked to redo tests that have been done earlier in different hospitals. This leads to monetary, time, and resource loss. Even if the organizations are ready to share data, there are no secure methods for sharing without disturbing data privacy, integrity, and confidentiality. When health data are stored or transferred via unsecured means there are always possibilities for adversaries to initiate an attack and modify them. To overcome these hurdles and secure the storage and sharing of health records, blockchain, a very disruptive technology can be integrated with the healthcare system for EHR management. This paper surveys recent works on the distributed, decentralized systems for EHR storage in healthcare organizations.*

Keywords: *Blockchain, EHR management, Data sharing, Privacy and security.*

1. Introduction

Blockchain is a decentralized, distributed peer-to-peer ledger system where consensus mechanisms are used to arrive at a collective agreement on the state of the ledger. Blockchain offers open verification by all participants rather than individual isolated operations using strong networking concepts like decentralization and cryptographic techniques. This potential can be leveraged for securing EHR in healthcare organizations. Once health records have been fed into a blockchain network, there is no way anyone can modify or delete records that protect the integrity of data. Each record is associated with a signature and key, hence no unauthorized user can feed data into the network or retrieve data from the network. EHRs from existing systems migrated to powerful blockchain technology can provide a universal solution for secure storage and sharing of medical data. Blockchain possesses a bunch of characteristics and properties which make the implementation of such a system feasible. Blockchain primitives and several other characteristics demonstrated in the below section showcase the efficiency of blockchain implementation in healthcare infrastructure. Blockchain integrated with IoT can be used in powerful applications like medical IoT, where user data is collected from IoT devices for diagnosis, verification, and research.

2. Blockchain – characteristics

Blockchain can be defined as a distributed, decentralized, peer-to-peer network which is an append-only ledger-like structure [1]. The network has several nodes from different geographical locations that have equal rights in the system rather than having special privileges or rights compared to other nodes. There exists no centralized server or third-party authority, each party in the network will have a copy of the data. The network is designed in such a way that all nodes participate in the routing process. Nodes will be actively participating in the process of learning about their neighbors and making connections for effective communication of messages, their verification, confirmation, and synchronization. This smooth topology of blockchain provides the base for its decentralized nature. Account addresses are created using public key cryptography, which acts as digital aliases for users. Messages are exchanged flexibly using a "smart contract". While executing new transactions or smart contracts, the collective ledger will compose them incessantly into a linked list of blocks.

What makes blockchain tamper-resistant? Each block will have a pointer to the previous block by recording its hash, timestamp, and list of transactions that occurred at the same timestamp. A List of transactions is stored in the form of a Merkle tree [2]. The First block in the chain is called a "genesis block". Each of the transactions generated will be added to some new block eventually and broadcasted to peers. All participating nodes collectively agree on a fresh block, to be incorporated. Lastly, this ledger will be harmonized among the peer nodes, which is then branded immutable. Blockchain is synonymous with a list of blocks linked cryptographically to form a chain where data is stored after proper verification and validation; changes happening in the system are synchronized globally by following consensus protocols. A cryptographically linked list of blocks together with consensus mechanisms makes the blockchain system a tamper-resistant digital stage for storing, passing, and retrieving data [1].

2.1. Classification of blockchain

Blockchain can be classified into different types: public, private, and consortium based on the permission/access required to join or leave the network [3, 4]. Initial implementations like Bitcoin and some cryptocurrencies were public blockchains, which granted access to a huge figure of users. Nodes can join or leave at any time, without special privileges or access. Some establishments like banking vertical favor having their own private or consortium blockchain instead of a public or permissionless blockchain. Unlike public blockchains, a group of reliable, trustworthy participants participates in both cases. An illustration of the broad-level classification of blockchain is provided in Fig. 1.

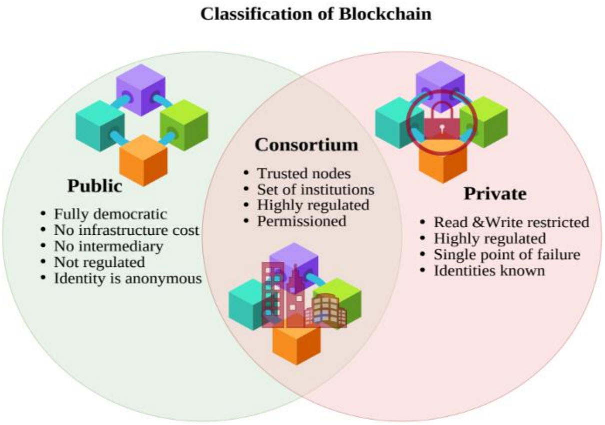

Fig. 1. Classification of blockchain

Public Blockchain. It is open to any number of participants. All nodes can be involved in block generation and verification. Consensus is reached once participating nodes have verified and confirmed the validity of the block. These types of systems may use Proof-of-Work (PoW) or Proof-of-stake protocol and work well with a large number of participating nodes [4]. They are decentralized trustless systems that are protected by the application of cryptography and economic incentives [3], for example, Bitcoin.

Consortium Blockchain. Consensus achieved by a preferred set of trusted user nodes. A consortium may consist of several nodes each one from a predefined set of institutions [5]. For consensus to be reached a minimum number of institutions must approve the block, to be added to the blockchain. They are not wholly decentralized, but rather partly decentralized [3].

Private Blockchain. The authority for the generation of new blocks and adding to the network always lies with one organization. Some privileges may be given to public users [3]. Since consent over the blockchain is given to one establishment, alone it may be called a centralized organization [4]. “Private blockchain” can be generalized as a term that includes all blockchain systems that are not completely public [5].

2.2. Key characteristics of Public Blockchain

Blockchain systems are decentralized, which holds several characteristics like autonomy, distributed, immutable, and contractual nature [6-9].

Decentralized. A key feature with no centralized authority that maintains the network; rather a collection of nodes together maintains it. Rather than a centralized governing authority, a private key can be used to control transactions. The decentralized structure empowers users with authority over their resources [10]. Some advantages are fewer catastrophes, user enablement, fewer failures, no centralized power, zero swindles, transparency, and legitimacy.

Enhanced security. No user will amend any physiognomies of the network for their advantage. In addition to decentralization, cryptography sets a coating of defense in the system [11]. The information available on the network is a cryptographic digest hiding the true nature of data. All the blocks contain a hash of the previous block as a pointer, except the Genesis block. Each block also, when hashed will produce a unique hash value itself. Hence trying to meddle with data results in changing all hash values of the following blocks until the last block is added, which is nearly impossible.

Distributed ledger. Blockchain networks for example Bitcoin are built on top of the Peer-to-Peer networks, where every signed transaction will be advertised to direct peers within one hop [2, 10]. Neighbors will corroborate transactions and relay them further, only when they consider the transactions valid, otherwise, they are discarded.

Incorruptible. Immutability is one of the blockchain characteristics that help to maintain a permanent, unalterable network. This upholds the transparency in the system and makes it free from corruption [10, 11]. Another feature is that, once a block is added to the ledger, no one can modify, delete, or create a different version of the truth without redoing the consensus process.

Consensus protocol. Consensus mechanisms help nodes come to a collective agreement on making a decision swiftly and moderately faster. When masses of nodes are endorsing a transaction, an agreement is undeniably essential for a system to work without any hassle. Consensus is accountable for the working of trustless networks in a trustful way [12]. Nodes may not trust their peers, but they trust the cryptographic algorithm, which is the heart of the system. [10].

Faster settlements. Conventional banking systems work very slowly when it comes to international transactions. Blockchain network saves precious user time by reducing the processing time from days to minutes [10]. Smart contract functionality available in the blockchain systems will further enable users to settle contracts in a faster manner rather than physical contracts.

2.3. Blockchain – applications

The notion of blockchain rose from the fundamental substructure of the Bitcoin network, which later broke the frontiers and made it practical beyond the implementation of cryptocurrency applications [13]. Few of the applications are found in the Internet of Things, Supply chain management systems, Identity Management Systems, Public key Infrastructure [14], etc. Automation of physical device management and synchronization of data in the Internet of Things applications can be made at ease and effective by using blockchain [15, 16].

Nowadays product traceability and tracking of ownership information in Supply chain management systems have become an onerous task. Blockchain can be efficiently used in such systems for transparency in structure and tracking ownership [17-19]. The use of centralized servers for Identity Management and Public Key Infrastructure can be effectively replaced by decentralization via blockchain implementation [20-23]. Some potential applications of blockchain in real-world scenarios are shown in Fig. 2.

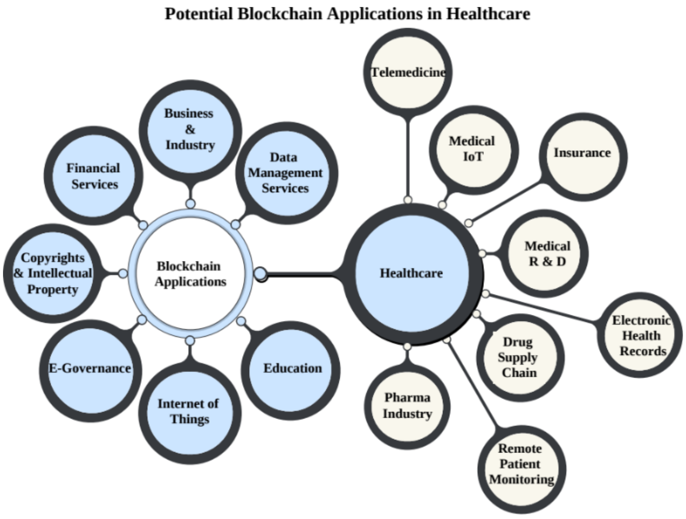

Fig. 2. Blockchain applications

Numerous blockchain applications provide Application Programming Interfaces (APIs) paving the way for innumerable real-world scenarios. APIs are built for different use cases using diverse underlying technologies but the users need not understand what is going on in the background. They can directly access APIs and interact with them [1]. The immutability and Integrity of blockchains help in building several other applications apart from Bitcoin. Some of them are deployed as online document management applications, exclusive rights protection systems [24], distributed information networks [25], healthcare [26], IoT applications [16], etc.

2.4. Blockchain in healthcare

Blockchain technology holds numerous traits that draw the attention of the healthcare industry towards it. This technology is expected to provide breakthrough solutions for healthcare records management, data sharing, and various other medical research-related works. Some key aspects that help the implementation of healthcare solutions in blockchain infrastructure are decentralization, immutability, auditability, improved privacy, and security. There may exist several pluses of blockchain that may excite the healthcare industry for the development of applications with blockchain integration, but the very vital and step-forward feature available in such implementation is patient-centric data access management. In the present scenario, medical data access is restricted to healthcare players like hospitals, insurance providers, and some other third parties involved in processing. But such data should also be accessible to owners, in this case, patients, who are subjects other than healthcare entities. This is known as patient-centric access management, which contrasts with the traditional approach of an institution-centric healthcare management system. A comparison of the traditional healthcare system with the blockchain model is provided in Fig. 3.

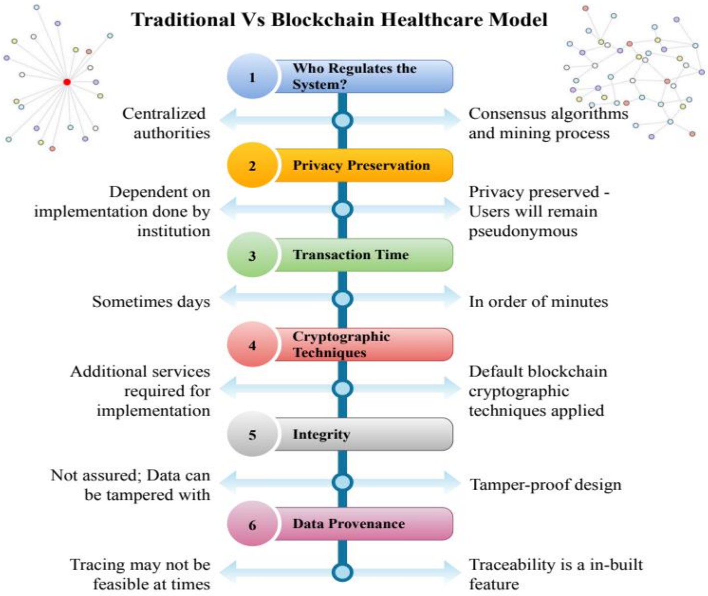
Traditional Vs Blockchain Healthcare Model
1
Who Regulates the System?
Centralized authorities
Consensus algorithms and mining process
2
Privacy Preservation
Dependent on implementation done by institution
Privacy preserved - Users will remain pseudonymous
3
Transaction Time
Sometimes days
In order of minutes
4
Cryptographic Techniques
Additional services required for implementation
Default blockchain cryptographic techniques applied
5
Integrity
Not assured; Data can be tampered with
Tamper-proof design
6
Data Provenance
Tracing may not be feasible at times
Traceability is a in-built feature

Fig. 3. Traditional vs. Blockchain healthcare model

Though the system has several advantages, some technical challenges like data privacy, security, scalability, availability, governance, etc. need to be considered. One such system that may facilitate a solution for the above-mentioned challenges is blockchain. The system will allow patients, the owners of data to provide access to valid entities. They may allow access to part of the data that is required by the healthcare provider such as hospitals, physicians, or medical research organizations, ensuring data privacy. Once the requirement is over, they may revoke access. Also, medical systems lay in silos in various hospitals and institutions. Implementation of blockchain can help patients or other authorized users to interconnect with all healthcare providers and get the required data automatically. This will help in minimizing duplication of data and wastage of resources. The size of medical data may be huge which may affect the scalability of the application. However, there is a solution in which only metadata regarding medical records will be stored in blockchain. A general flow of data from existing EHR systems to blockchain networks is illustrated in Fig. 4.

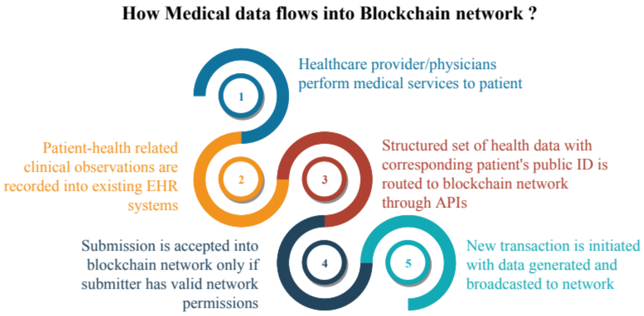
How Medical data flows into Blockchain network ?
1
Healthcare provider/physicians perform medical services to patient
2
Patient-health related clinical observations are recorded into existing EHR systems
3
Structured set of health data with corresponding patient's public ID is routed to blockchain network through APIs
4
Submission is accepted into blockchain network only if submitter has valid network permissions
5
New transaction is initiated with data generated and broadcasted to network

Fig. 4. Health data flow into blockchain network

3. Related work

The advantages of healthcare systems deployment on blockchain platforms have been validated in [27], which recommends new architectures for the prospective scheme of blockchain-based EHR management systems. However, there is a lack of details about the standards to be followed for implementation. A survey has been done on modern and recent ideas on secure sharing of health information, and privacy-preserving schemes using blockchain [28]. The existing works classify them only based on permissioned and permissionless approaches and their characteristics. There is no elaborate study on preserving privacy. In [29], the work focussed on contemporary approaches used in healthcare implementations and examined blockchain technology in healthcare. The author throws light on key benefits and challenges. Work [30] talks about various smart healthcare information systems built on blockchain and proposes new architectures, however, lack standards, protocols, and implementation details. Model in [31] proposes to integrate existing healthcare IT systems as-is with the blockchain network. The existing system continues to hold health information in its proprietary databases while mirroring copies of data in the blockchain network. The blockchain systems will allow patients to have ownership of their data and can contribute to their health information. Network resources have been wasted by storing data in proprietary databases. This does not address the decentralization needs. Immutability property is also challenged by using centralized databases, which leads to inconsistency between centralized institutional databases and blockchain networks. An investigation of the integration of blockchain features in present-day healthcare infrastructure has been done [32]. It analyses the necessities and challenges in safeguarding EHR storage using such decentralized approaches.

4. Classification of State-of-Art EHR implementation in blockchain

In this paper, a popular use case of blockchain implementation in healthcare systems has been taken into consideration, i.e., EHR Management system. This system involves patients' health data generation, storage, processing, and retrieval mechanisms. A detailed study of various research works related to EHR Management using blockchain has been presented in the below state-of-art survey. Selected papers in this survey talk about several aspects of blockchain in Healthcare system implementation like decentralization, immutability, scalability, security, patient-centric access, on-chain, and off-chain storage, etc.

4.1. Based on Frameworks & Fundamentals

Permissioned blockchain infrastructure has been utilized in schemes proposed in [33-36, 28, 37]. The author proposes a permissioned blockchain with fine-grained access control for the patient-centric model [33]. Although this provides a necessary security feature, there is a critical gap, as the user has to share their password with other users like doctors, nurses, or healthcare providers to see shared data for diagnosis or further treatment. This leads to vulnerabilities like key leaks as it involves trust in humans. If a password/key has leaked, there is no mechanism available for password/key updates. Limited block size leads to delays in the authentication and retrieval process. The system is also vulnerable to replay and offline dictionary attacks.

The permission blockchain system proposed in [34] allows users only when they are invited and verified by the system. Although lightweight architecture, scalability, and accountability weigh positively, there is probable centralization due to cloud services. Permissioned blockchain deployment leads to likely bias. Examination of communication protocol, authentication protocol, and algorithms is not comprehensive. Paper [35] talks about implementing permissioned blockchain infrastructure for managing EHR and sharing medical treatment information between stakeholders. Only approved users will access the system through role-based access control. Decentralization in blockchain has been leveraged in this system. Though the system has proposed practicable approaches, usage of permissioned blockchain by allowing certain people to have higher authority may lead to bias and corruption.

Permissioned blockchains have been leveraged for EHR storage and sharing in [38]. Confidentiality is ensured by an access control mechanism using cipher text-based attribute encryption. Privacy is ensured using a combination of blockchain and polynomial equations to attain random construction of keywords. Capabilities of Hyperledger Composer and Fabric have been used to implement a healthcare network easily accessible during emergencies or disasters have been proposed [37]. Emergency Access Control Management System (EACMS) has been implemented as a permissioned blockchain framework. A system for sharing and integration of EHR data has been proposed by authors in [39]. Every hospital in the network will participate in EHR transactions through a dedicated blockchain node integrated with its internal EHR system. Patients, doctors, and other hospital entities initiate data-sharing transactions using a web interface. A permissioned open-source blockchain framework has been built using Hyperledger Fabric. HL7 Fast Healthcare Interoperability Resources (FHIR) standard was adopted during data sharing.

A consortium blockchain framework has been proposed by authors in [50-52]. A similar model for handling health data by patients, hospitals, healthcare entities, researchers, and practitioners has been proposed in [50]. The system efficiently uses smart contracts for medical records sharing, review, and auditing. Blockchain technology has been combined with Parallel Health Systems (PHS) for accurate diagnosis and effective treatment of disease. PHS which is a combination of artificial systems, computational experiments, and a parallel execution approach is deployed for descriptive, predictive, and prescriptive intelligence in healthcare systems. In [53], a Private blockchain-based model within each hospital in the network has been proposed. The system uses proxy re-encryption technology for data communication between doctors from various networking hospitals. Disease diagnosis or any other transaction related to the patient will be broadcasted by doctors within the network. Each hospital will have a unique server node that will act as a super node. All other nodes will update their data based on the confirmation provided by the super node. Credit scoring is done for hospitals and doctors to prevent misbehaving. However, this system is vulnerable to corruption, and fraud by ill-intended entities.

Blockchain mechanism integrated with IoT has been proposed for EHR management, with private blockchain and swarm exchange as the backbone [40]. Several open-source tools like GnuPG, Goland, and IPFS have been utilized for development. IoT-based body sensor nodes for measuring body temperature, pulse, and oxygen level have been integrated with a blockchain network for EHR transmission and swarm exchange. A public blockchain system has been implemented in [54] which provides a flexible access-control mechanism for EHR placed in off-chain storage called “Data Lake”. Paper [51] proposes disease diagnosis improvements in electronic health infrastructure by implementing blockchain techniques. It is an integration of public and consortium blockchains using definite data structures and consensus protocols. The cost of adding a transaction to a block in the network is linearly proportional to the length of data, making the system vulnerable to turnaround delays and latency. A miner verifier algorithm is proposed however not analyzed. A comparison of blockchain usage in healthcare has been analyzed based on frameworks used and their fundamental technology. Table 1 presents the comparative study for such research works in the related domain.

Blockchain has been used efficiently in [55], for fine-grained access control and sharing of data from IoT devices by patients. The system proposes to use two separate blockchains for patients’ data (UserChain) and doctor diagnosis data (DocChain). UserChain is a public blockchain, whereas DocChain is a consortium chain. It preserves the privacy of data by encrypting them and providing access to the patients only. Patients maintain access control for their data, by providing access to doctors when required and revoking them later. This access control mechanism enhances the system against tampering and alteration, preventing medical disputes due to tampering with records. It has the inherent disadvantage of assuming that a secure channel exists between the IoT device and the user node, which may not be true. The system assumes that adversaries cannot control more than 51% of resources to perform a 51% attack. In DocChain which is a consortium chain, it is assumed that no more than *f* nodes will be malicious which does not hold always, leading to Byzantine Failures. Trust plays a major role in DocChain which assumes that all doctors play by rules. A hybrid model using private and consortium blockchain has been proposed for secure storage and sharing of EHR data [41]. A consortium blockchain is used to safeguard storage indexes of health data while actual data is stored in a private blockchain. EHR data are encrypted using a public key with a keyword searchable option.

Blockchain integration with edge nodes has been proposed for the development of a hybrid EHR management architecture [42]. Actual EHR data is encrypted using multi-authority Attribute-Based Encryption (ABE) and stored in edge nodes while an Attribute-Based Multi-Signature Scheme (ABMS) is utilized for authenticating users' credentials. The Hyperledger fabric platform was used for blockchain development and the Hyperledger Ursa library for developing the ABMS module.

Multiple frameworks and tools for developing and testing blockchain-based healthcare systems have been explored in [43]. The performance of those systems has been measured using hyperledger fabric, composer, docker, caliper, and Wireshark capture tool.

Table 1. Frameworks and fundamentals of existing schemes

Work	Type of blockchain	Framework	Interface	Participating nodes	Cryptographic techniques
[39]	Permissioned blockchain	Hyperledger fabric	A web-based interface will be used for patients and doctors to initiate EHR-sharing transactions	Each hospital will provide a blockchain node integrated with its own EHR system to form the blockchain network	The system uses public key infrastructure-based asymmetric encryption and digital signatures to secure shared EHR data
[40]	Private Blockchain	None mentioned	Swarm HTTP API, Swarm Core API	Swarm nodes used by patients and doctors, miner nodes	Hybridized key encryption, SHA-3 Algorithm
[41]	Private and Consortium blockchain	Not mentioned	Not implemented	Server nodes generate searchable keywords and feed the new block into the consortium blockchain; Third-party nodes like doctors from other hospitals, insurance agencies, etc.	Public-key encryption with appropriate keyword search
[42]	Permissioned consortium blockchain	Hyperledger fabric, hyperledger composer, hyperledger Ursa library	Not implemented	Patient nodes, Hospitals, Edge nodes, Smart sensors	Multi-authority CP-ABE (Cyphertext Policy-Attribute-Based Encryption) mechanism, Multi-authority ABMS(Attribute-Based Multi-Signature) mechanism
[43]	Permissioned and consortium-managed blockchain	Hyperledger Fabric	Client application or SDK, Membership Service Provider	Each hospital will provide a blockchain node integrated with its own EHR system to form the blockchain network	Certificate Authority generated key pairs; Symmetric Key (Mechanism not defined properly)
[44]	Private blockchain	Ethereum, Dodgecoin, and Bitcoin protocols are compared	Not implemented	Not Defined	None mentioned
[45]	Not mentioned if Ethereum is public or private	Ethereum	Client interface - Javascript (Node.js) for web application, Vue.js UI technology	Not defined properly	Keccak-256 cryptographic hash function, Elliptic Curve Digital Signature Algorithm (ECDSA)
[46]	Permissioned Consortium blockchain	Hyperledger Fabric, Hyperledger Sandbox, and Hyperledger Composer	Blockchain API	Network with two organizations with one peer each	Cryptographic techniques like encryption and signatures are not defined
[47]	Permissioned blockchain	Hyperledger Fabric	Fabric SDK	Hospital nodes within permissioned Blockchain, Orderer Service who finalizes the transaction, Patient Nodes, and Doctor Nodes	Attribute-based and homomorphic cryptosystem
[48]	Permissioned blockchain	Hyperledger Fabric	Not implemented	Medical Center and Network Admin	The system uses public key infrastructure–based asymmetric encryption and digital signatures to secure shared EHR data
[49]	Private blockchain	Custom-developed Blockchain using POJO in Java	Not implemented	Server nodes(mining nodes), doctors, patients(full nodes), separare verifier nodes, insurance agency(light nodes)	RSA for Key generation, HMAC-SHA1 for Hashing, Identity-based Encryption to generate a bilinear map

Data accessibility between multiple providers has been improved using the access control policy algorithm. Enhanced results have been achieved scaled based on latency metrics, throughput, and turn-around time.

Some selected blockchain protocols were simulated for EHR data sharing and analyzed using a discrete event simulation tool [44]. A comparison between Ethereum, Dogecoin, and Bitcoin has been done and the results proved that the Ethereum framework is better for EHR transactions. The scalability of the systems has been studied and results are obtained.

The Ethereum blockchain platform has been integrated with conventional EHR systems excluding any third-party systems [45]. This cross-platform system enables stakeholders like healthcare providers, and individual physicians to access patient-health data from various electronic devices, only when they have the patient's consent. All nodes in the system act as heavy-weight nodes with patients' data stored in each of them. The effectiveness of the system is shown by testing using Ganache based on dimensions like privacy, security, throughput, and cross-platform independence.

4.1.1. Consensus mechanism

A lightweight blockchain architecture helps reduce computational and communication overhead by using the canal to allow secure, confidential transactions within the group of participants [56]. Divides the network participants into clusters maintaining one copy of the ledger per cluster. The Head BlockChain Manager (HBCM) acts as a Certificate Authority providing valid digital identity to participants to join the network. This model proposes the deployment of Two HBCMs, one acting as primary and the other a replica. Ledger for clusters of the hospital will be maintained by only one cluster node and queried by others. Transactions are broadcasted to BCMs which verifies them and marks them as valid or invalid transactions. The system uses Practical Byzantine Fault Tolerance (PBFT) rather than for achieving consensus. The usage of HBCM to provide digital identity leads to centralization in the system. Canals make it feasible for the participants to perform erroneous or corrupted transactions. Data centralization in BCMs makes it a single point of failure. The system assumes less than $n/3$ faulty nodes in the network, to achieve PBFT consensus hence there is a potential failure of the system in case $n/3$ or greater than $n/3$ faulty nodes. Attacks like data modification and dropping attacks are possible once the adversary takes control of BCMs.

Blockchain and machine learning approaches have been adopted in EHR to help research and improve the quality of healthcare. A novel Proof-of-Information algorithm on top of a successful PoW Algorithm has been projected in [57]. Using machine learning approaches efficiency and accuracy are supposedly improved. PoW though powerful incurs computational and resource overhead. Hence alternate mechanisms like Proof-of-Interoperability [58], Proof-of-Conformance [51], and Proof-of-Authorization [52] have been deployed.

In [59], the authors propose a hybrid blockchain for secure storage and sharing of EHR. Each participating node falls into one of the following categories: Orderers, Endorsers, and Committers. A variant of the PBFT Algorithm has been used for achieving consensus and asymmetric encryption has been used in the encryption and decryption of data. The access control mechanism for third-party has not been established properly. Performance is severely impacted due to the usage of an asymmetric encryption algorithm. Delegated Proof-of-Stake (DPoS) has been used in [53]. Based on disease symptoms identified for different patients from different hospitals, a symptom-matching method has been devised. DPoS mechanism eliminates the need to vote and elect a delegate, reducing resources and communication overhead.

4.1.2. Smart contracts

Traditional healthcare system lacks various features like privacy, security, scalability, and universal protocol/standards. The model in [60] demonstrates a decentralized blockchain-based approach for providing a scalable solution for clinical records storage and retrieval. It is dissociated from the previously obtainable blockchain framework for the healthcare system and instead emphasizes the design of smart contracts and other modules that actively interface with the blockchain. There is an advantage of greater compatibility since it allows networking with any prevailing blockchains that provision carrying out smart contracts execution. Even though it proposes a token-based access exchange mechanism, the approach for harmonization between various stakeholders has not been established properly. There is a delay in accessing patients' data in addition to inadequate scalability attesting to major drawbacks in the system.

The ability of blockchain-based system implementation models for healthcare systems to privacy protection of sensitive patient medical data has been investigated in [61]. This framework while maintaining the privacy of patients' data ensures that fair access to EHR has been provided to various stakeholders like patients, healthcare providers, and third parties. It provides possession and ultimate governance of data to patients. Smart contracts utility in the Ethereum blockchain has been set up in this system for intensified access control management and mystification of patients' records through data obfuscation. Advanced cryptographic practices have been employed to further augment security. The system tightly treadles who can access which data and licenses secure transmission of records, curtailing the ability of unapproved players to derive private health information. The finest part is auditability, allowing tracking of data usage. System fine-tunes all necessities of secure EHR systems, however, provides the highest authority to some nodes. This weakness clues to potential bias, scams, and exploitation due to hierarchy. The usage of HTTPS to send query link information in a private transaction is another acknowledged factor making the system vulnerable. The proposed mechanism is also defenseless to Denial-of-Service (DoS) attacks.

Ethereum has been used to develop a real-world Data Preservation System (DPS) on a blockchain platform [62]. The system enables users to preserve their data in time without end and tampering with records can be always verified in case there is distrust. User privacy is guaranteed through the integration of various practical storage methods and cryptographic techniques. Though the system guarantees privacy and security, the prospect of data loss and tampering with records is not studied comprehensively.

The system proposed in [50] efficiently uses smart contracts for EHR sharing, review, and auditing. Various attacks have been analyzed in some of the works related to data storage, privacy, and security [63, 65]. It involves a wireless body area network and a PSN area, which has several body sensors for collecting medical data from the patient. Medical sensors securely communicate between them using association protocol, which lets only authenticated sensors participate. Though system implementation looks feasible, there is no information regarding the consensus protocol used to achieve agreement in adding blocks to the chain. Smart contracts functionality has not been investigated as well.

Health data transfers between various parties in healthcare networks have been established using smart contracts functionality [64]. The system proposed here is a peer-to-peer EHR storage network that addresses various security components like validation of authenticated users, permission to authorized users, and access control mechanisms. Though the author proposes an encryption mechanism, interoperability, and key management, implementation details are missing. In the system proposed in [37], patients can provide access to their EHR during emergencies based on smart contracts. They define both emergency conditions and time duration for data access by other parties in a permissioned blockchain. It discusses how blockchain technology, and smart contracts, could help in some typical scenarios related to data access, data management, and data interoperability for the specific healthcare domain. The authors then propose the implementation of large-scale information architecture to access EHR. Smart contracts are being used as information mediators in the healthcare blockchain networks. However, the paper claims to frame the architecture to solve privacy, scalability, and availability issues.

Authors in [66], propose a decentralized architecture for EHR management built on blockchain technology, Ethereum, and implementation of the prototype "MedRec". Smart contracts functionality in Ethereum has been designed for three functionalities: to create a link between the health information of patients stored in the systems of different healthcare providers; for third-party access to patient health information; and authentication verification. Registrar contracts are defined to map nodes to their Ethereum addresses. The patient-provider relationship contract defines ownership of patients' health information by defining access control permissions and pointers to patients' data. A summary contract is designed to control a list of PPR references for its activities with client nodes such as other patients and hospitals. Some nodes may have higher authority breaking the purpose of decentralization.

A reliable EHR management system was constructed [67] using blockchain. Smart contracts have been deployed to control the accessibility of the EHR to doctors in the system. It is a theoretical proposal and does not study the feasibility of the proposed system in quantifiable real-world settings. Availability, scalability, and identity management have been analyzed. Javascript-based smart contracts have been developed for patient-centric blockchain-based EHR systems [46]. The security of the model has been guaranteed using hyperledger fabric and composer technology.

Various parameters such as latency, throughput, and computational resources have been bench-marked using the hyperledger caliper tool.

Table 2. Comparison of implementation standards of existing schemes

Work	Prototype developed?	Tested realtime?	Records format	Client interface & contracts	Benchmarkingtool	Parameters examined
[39]	Yes, opensource permissioned blockchain on hyperledger fabric	Yes, the distributed environment at Stony Brook University	Key-value pairs (JSON)	HTML, Javascript, CSS, Open Source Bootstrap Libraries, Chaincode	None	None
[40]	Partial, working tested via terminal; No interface developed	Partial	.txt, .docx, .pdf, .png, .tiff, .jpg files	GnuPG, IPFS, and Golang	None	Swarm: loading, exchange, listening, announcement, availability; Analysis of IoT elements
[41]	No	Tested on PC, mobile phone	None mentioned	None	None	Computation cost; No other parameters were examined
[42]	Yes, two primary modules (ABMS module, blockchain module)	Yes	Key-value pairs (JSON)	Chaincode, Rust language used by hyperledger Ursa	Hyperledger Ursa BLS	Signing and verification time based on varying number of attributes and length of attributes
[43]	Yes, hyperledger fabric, composer, and docker container used	No	None mentioned	Chaincode, Java, Go, Node.js	Hyperledger caliper, Wireshark capture engine	Latency, throughput, Round Trip Time (RTT)
[44]	No	Simulation model tested	None mentioned	None	Discrete event simulation tool, Analytic hierarchy process technique	Scalability in terms of number of transactions(sent, received, failed), nodes, cost
[45]	Only model overview and testing conditions provided	None	JSON	Solidity for smart contracts, Node.js for web application, Vue.js UI technology, Truffle Suite, Web3js, Visual Studio Code	None	Execution time
[46]	Yes, permissioned blockchain on hyperledger fabric	Yes, network with two peers	Key-value pairs (JSON)	Java, Go, node.js, Chaincode	Hyperledger Caliper	Latency, throughput, CPU usage, traffic in and out, memory consumption, disk write/read, network I/O
[47]	Yes, hyperledger fabric version 1.0	No	Plain text file .txt	Java Pairing-Based Cryptography library (jPBC), Java version 8.0, Chaincode for smart contracts	None	Running time for different data sizes, number of attributes, encryption, and decryption efficiency
[48]	Yes, permissioned blockchain on hyperledger fabric	No	None mentioned	Chaincode	Dolev-Yao (DY) model to analyze security protocols, AVISPA tool	Communication and computation cost, security properties
[49]	POJO(Java), details not provided	Partial, EHR encryption & decryption tested	None mentioned	POJO in Java	None	Data retrieval time, details on comparison missing

Implementation details of recent work in blockchain integration with the healthcare domain have been studied extensively, and the comparison is produced in Table 2.

4.2. Based on storage standards

The transformation from a traditional system to a blockchain-based system for dynamics like mechanisms on access rights, data availability, and faster accessibility was studied in [68]. Proposed off-chain and on-chain storage and retrieval of patient data, ensure that patients are wardens of their EHR. They can authorize the release of their data and share them with entities they approve of. The system enables greater interoperability, a patient-driven, and institution-centric approach through access rights management, aggregation of patient health records, immutability, and easy accessibility. When there is a large volume of clinical data, the system may not be scalable; hence it may not efficiently provide services to larger institutions with huge patient flow. Multiple stakeholders are involved, but incentive mechanisms for them have not been aligned.

Since blockchain systems need to limit the storage of data on-chain to reduce computational and resource overheads, some research has been done on off-chain storage mechanisms. One such proposal was done in [69] for off-chain storage of EHR. The system proved to be scalable due to the off-chain nature of data storage. Though the system has several advantages like improved scalability, off-chain storage, granular access control, etc., immutability properties of blockchain have been beaten by update and delete records functionality paving the way to tampering with records. Doctors and nurses are granted special access to make changes in patient records which may lead to corruption and fraudulent activities. Hospital administrative staff providing access to users may lead to a single point of failure or corruption through tampering with records through unintended access.

Healthcare data management which combines off-chain and on-chain storage and verification on a blockchain platform has been proposed in [70]. Two separate chains are loosely coupled to provide storage for different kinds of EHR The system satisfies both privacy and authenticity through a combination of on-chain and off-chain verification methods. Two separate chains used for EHR and Personal Health data prove to be redundant. Data integrity property is not preserved.

Due to the limited scalability of blockchain and on-chain storage, a very useful design of off-chain storage has been implemented in [54]. A public blockchain system has been implemented which provides a flexible access-control mechanism for EHR that is placed in off-chain storage called “Data Lake”. These Data Lakes are scalable storage that can store a wide range of medical data like scanned images, reports, etc. Data stored in Data Lake are safeguarded using cryptographic techniques like encryption and digital signatures. This architecture also supports data analytics, data mining, and machine learning capabilities.

A proposal has been made for a scheme to protect EHRs by storing them on off-chain storage coupled with blockchain infrastructure [71]. Owners are allowed to effectively control their data through Access Control Lists. Data storage in store (off-chain) and retrieval is considered one type of transaction and providing access to data to other users or services is considered to be another type of transaction. Though the work emancipates the usage of a centralized storage scheme by blockchain, it does not discuss how keys will be effectively managed. Practicality and scalability are not measured as there is no open-source implementation available. Various institutions participating in the healthcare system need to interact with each other for effective functioning.

In [58], a blockchain-based approach has been proposed for inter-institutional collaboration in the storage and sharing of EHR. A new design for transactions and block structure has been suggested for aiding protected and fast access to health data stored off-chain. PoW though powerful incurs a lot of computational and resource overhead. Hence an alternate mechanism for consensus called Proof-of-Interoperability is offered which evades the usage of expensive computational resources.

Table 3. Comparison of On-chain and Off-chain storage

Work	Metadata storage	On-Chain or Off-Chain	Cloud service	Data storage
[39]	A hybrid data management approach, where only management metadata will be stored on the chain	EHR data will be encrypted and stored off-chain in HIPAA-compliant cloud-based Storage	Amazon AWS S3	CouchDB for on-chain metadata management
[40]	Hash values stored On-Chain	IPFS	No	On-Chain
[41]	Not mentioned	EHR in private hospital blockchain; Indexes on a consortium blockchain	No	None mentioned
[42]	ABMS authentication events and EHR access activities (including EHR addresses and other information) stored as transactions on the blockchain	Hybrid architecture – ABMS authentication events and EHR access activities stored on-chain and ABE-encrypted EHR data stored off-chain on edge nodes	No	Edge node used for EHR data storage; No specific database mentioned
[43]	Health records stored on-chain	On-chain	No	On-chain
[44]	Not mentioned	None	No	None mentioned
[45]	Not mentioned	Not mentioned	No	None mentioned
[46]	Centralized Hospital DB	Centralized Hospital DB	No	DB details not mentioned
[47]	On-chain	IPFS and On-chain storage	No	IPFS and On-chain storage
[48]	Network admin uses on-chain storage	Off-chain cloud storage	Yes	On-chain
[49]	Health records stored on-chain	On-chain	No	On-chain

New block creation and addition to the network involves transaction dispersal, block confirmation, return of block after signing, and a new block distribution phase. Proof-of-Interoperability also conforms to Fast Healthcare Interoperability Resources (FHIR) organizational and semantic requirements. Each participating node will get an equal opportunity for mining by random miner algorithm. Though the author has been successful in proposing a method for the creation of blocks, mining, and consensus algorithms, there are no details about how the health data is structured in the implementation. It also lacks implementation details on the storage and retrieval process, and keyword searches adopted. Table 3 compares various implementations in recent years based on storage methodologies followed. It provides technical details on whether data is stored on-chain or off-chain or in a hybrid model along with practical implementation details about cloud and other databases usage.

4.2.1. Cloud integration with blockchain

Few models have been introduced in [72, 33] for improving the seclusion of patients' data by letting patients own, control, and share their data based on need. Apart from improving the privacy of patient data, the model proposed in [72] served as a steadfast model by using blockchain to control the possession of patient data. It used a unified Indicator-Centric Schema (ICS) for organizing EHR simply and nigh on perfectly. Though work by [72, 33] is privacy-preserving, the intervention of third-party cloud services providers leads to centralization and involvement of trust factor, which risks the security of patients' data. The system has a very limited block size which may lead to deferment and latency in authentication, storage, and retrieval processes when the number of users in the system upsurges. Secure sharing of documents using visual cryptography in cloud architecture has been proposed which might be used as a privacy-preserving model for data storage [73].

Sensitive patient data stored in cloud networks always possesses various challenges like the implementation of worthwhile access control mechanisms [34]. The proposed model addresses the key challenge raised due to access control. It also preserves immutability and autonomy through the use of permissioned blockchain. Permissioned blockchain systems allow users only when they are invited and verified by the system. Although lightweight architecture, scalability, and accountability weigh positive characteristics, there is probable centralization due to cloud services. Permissioned blockchain deployment also leads to likely bias. The examination of communication protocol, authentication protocol, and algorithms is not comprehensive.

Healthcare management systems in the literature made use of several encryption techniques like symmetric encryption, public key encryption, attribute-based encryption, etc. One such model using searchable symmetric encryption and attribute-based encryption mechanisms has been proposed in [74] for sharing patient health records based on blockchain while preserving data integrity, privacy, and fine-grained access control. Blockchain has been effectively used to manage keys avoiding a single point of failure risk in centralized key management. The involvement of a third-party cloud provider during file operations (update, delete) in the personal health records management module opens a question of trust whether the provider performs file operations based on the patient’s request and requirement. Integration of Cloud service providers presents the risk of third-party intervention.

Blockchain and Cloud technologies are well equipped to solve the problem of privacy and scalability issues in healthcare management systems, though they lead to some centralization issues. A storage scheme for managing personal health data has been proposed based on blockchain and cloud storage integration [75]. This system establishes a framework for medical data storage as well as secure sharing of data to other stakeholders. Implementation of fine-grained access control and patients’ ownership of their data proves that patients’ data is protected from unauthorized access. Off-chain storage of data is encouraged in this model by storing only index information in the blockchain, making it scalable. However, the involvement of Cloud service providers leads to reliance on the trust factor of third parties.

A user-centric structure for sharing health information on a permissioned blockchain network has been proposed [36]. Data privacy for patients' health data and identity management for users are implemented using membership services in the hyperledger fabric framework. A channel formation scheme has been used in addition to these membership services. Patients' data from wearable devices like medical IoT devices will be collected and synchronized to a cloud service which will eventually be shared with healthcare providers. Usage of the cloud leads to third-party involvement, centralization, and possible single point of failure.

Currently, cloud is being used extensively for data storage and retrieval in various applications. In [76] cloud-based services have been integrated with blockchain for implementing EHR sharing methods with provisions for access control, management, and interoperability between service providers. Large-scale health information management architecture MeDShare has been designed leveraging smart contracts as peacekeepers for information shared. Data privacy and accessibility issues have been addressed using blockchain and cloud service integration. The MeDShare system seems to provide comparable performance relative to existing implementations. Auditability and traceability have been improved by the use of cloud services as data guardians. Though usage of cloud services along with blockchain lessens the risk of data privacy concerns, it introduces the possibility of centralization and a single point of failure.

Model in [52] introduced blockchain-based EHR storage and sharing protocol which integrated consortium blockchain with cloud service providers. An entity that requests data can search the chosen keyword to obtain appropriate health records and get re-encryption cipher text from the cloud server after the patient's approval. Cryptographic techniques like searchable encryption and conditional proxy re-encryption have been utilized for security, privacy, and access control. A Proof-of-Authorization consensus protocol has been developed to ensure achieving consensus in the system.

4.2.2. IPFS storage integration with blockchain

Various technologies like blockchain, Inter Planetary File System (IPFS) and cloud platforms have been used to provide an integrated solution for healthcare data management systems. One such system has been proposed in [77], where blockchain, IPFS, and mobile cloud platform potentials have been leveraged to provide reliable access control through smart contracts. The evaluation method demonstrates considerable performance improvements and analysis of security policies, ensuring minimum network latency, and improved security, and privacy of patient health records. Overall framework proves to be scalable; however, the usage of Amazon cloud services makes the system centralized. This system involves trust factors in third-party like cloud service providers and fails to be tamper resistant when the provider cannot be trusted completely. IPFS storage structure has been integrated with blockchain for developing scalable storage for medical information, which enhanced privacy and secure sharing techniques. Cryptographic primitive has been improvised into an enhancement called SHDPCPC-CP-ABE [47]. Homomorphic and pallier cryptosystem techniques were applied for fine-grained access control and to preserve the privacy of medical insurance claims.

4.3. Based on information security standards

Some implementations of blockchain EHRs that exist today provide fine-grained access control for patients by providing them ownership of their data. Fine-grained access control which lets users provide permission to other users and revoke them on demand has been introduced in [74, 75, 55]. A few implementations from recent years have been compared based on information security aspects, and details are provided in Table 4 (Here "✓" is "yes", "✗" is "no").

Table 4. Comparison of Information security aspects for existing schemes

Work	Privacy	Security	Integrity	Availability	Authenticity	Confidentiality	Immutability	Robustness	Granular access control	Identity management
[39]	✓	✓	✓	✓	✓	✓	✓	✗	Yes, patient-centric	Pseudonym for patients
[40]	✓	✓	✓	✓	✓	✓	✓	✗	Yes, patient-centric	Pseudonym for patients
[41]	✓	✓	✓	✗	✓	✓	✗	✗	Yes, controlled by the system manager	Users are not anonymous as the system manager can map the identity to the individual using an ID stored in the DB
[42]	✓	✓	✓	✗	✓	✓	✓	✗	Yes, patient-centric	No pseudonymity, Global identification number issued by hospital maps to the user directly
[43]	✓	✓	✓	✗	✓	✓	✓	✗	✗	None mentioned
[44]	✗	✗	✗	✗	✗	✗	✗	✗	✗	None mentioned
[45]	✓	✓	✓	✗	✓	✓	✓	✗	✗	None mentioned
[46]	✓	✓	✓	✗	✓	✓	✓	✓	Yes, patient-centric	No pseudonymity, Patient, and Doctor's IDs are stored in hospital DB as plain text
[47]	✓	✓	✓	✓	✓	✓	✗	✓	Yes, Doctors share medical records with third parties rather than patients. Not patient-centric	No pseudonymity, the orderer generates a transaction with the patient's identity
[48]	✓	✓	✓	✓	✓	✓	✓	✗	Yes, done by the network administrator	Masked identity for patients and health centers, X.509 certificates
[49]	✓	✓	✓	✗	✓	✓	✓	✗	Yes, patient-centric	No de-identification of patient information

[73] Blockchain technology has been used for fine-grained access control in the management of patient data collected from IoT device users. This system is fully decentralized as it does not involve any third party like cloud service providers. The system meticulously implements pseudonymous addresses for users, thus preserving privacy for patient data, although it lacks privacy protection for data generated by doctors. The integrity of the system is highly affected as there is latency in the

confirmation of blocks generated. Each block generated has to wait for about 60 minutes to get confirmed in a blockchain network. A patient-centric model in [33] guarantees pseudonymity by the practice of cryptographic utilities to guard the privacy of patients' medical data. Protects several aspects of data fortification like accountability, integrity, pseudonymity, security, and privacy. Coarse-grained access control of the system lets users encrypt their data and store them on a permissioned blockchain.

A flexible query-based, coarse-grained access control mechanism for enhancing authorization procedure has been proposed in [78]. The authorization model is designed with the ability to approve different granular levels of access for users, despite upholding the compatibility and sustenance of the fundamental data structure of the blockchain framework. On no account there is a need for dependence on Public Key Infrastructure (PKI), consequently limiting the computation overheads. Restricted block size in the structure leads to an unendurable delay in the authentication process and storage or retrieval process. Poor scalability impacts system throughput.

The proposed implementation in [38] minimizes the possibility of chosen keyword attacks due to the usage of random keywords. Results show that the system poses a high turnaround data retrieval efficacy, limited storage cost, and fine-grained access control. Although the system has several advantages, data retrieval time is linearly proportional to several attributes. As the number of attributes increases, data retrieval time increases decreasing search efficiency and affecting turnaround. In the literature [79], a framework for handling EHR and the distribution of data among stakeholders for cancer care has been proposed. The system is claimed to be privacy-preserving, a secured network with high availability, and coarse-grained access control on patient medical data. It claims to considerably lessen communication overheads for data sharing, improve progressive resolution making for patient treatment, and reduce cost overheads. The system does not take into consideration the data integrity portion of security implementation.

Healthcare management systems in the literature made use of several encryption techniques like symmetric encryption, public key encryption, attribute-based encryption, etc. Some models using Attribute-based Encryption have been proposed by authors in [74], and [38]. The work proposed in [80] implements a method called "Signcryption" which combines the goodness of digital signatures and encryption in a distinct rational phase commendably alleviating the overhead involved in processing and communication. This method is proved to be far better than customary schemes which follow the sign first and then encrypt technique. Symmetric key encryption is used for encrypting the EHR; again output will be encrypted with an attribute key set. As a next step, encrypted health data and encrypted symmetric key will be signed with a private key, thus protecting via double encryption.

Attribute-Based Signature (ABS) scheme is useful in anonymous user authentication and attribute-based messaging structures. Model in [81] proposes such a mechanism for attribute-based signing along with the additional capability of signing by multiple authorities. Multiple Authority – Attribute-Based Signature (MA-ABS) scheme proposed in this work uses a combination of powerful signature mechanisms and blockchain technology to resist collusion attacks. It also proves selective predicate attacks to be unsuccessful. The identity-based Signature scheme with multiple authorities proposed in this work [82] uses a combination of powerful signature mechanisms and blockchain technology to resist collusion attacks. The system claims to have an efficient signature scheme and verification algorithm compared to existing schemes in blockchain-based storage for EHR, though it is not thoroughly analyzed.

Blockchain has been clubbed with Attribute-Based Encryption for a flexible and efficient telemedicine system in literature [83]. This system is controlled by multi-authority, provisioning on-demand access to health information. Patients need to remember private keys to access their data which may not be suitable for the user of all ages. Sometimes users may forget keys leading to permanent loss of access to their data. If they store it somewhere, there is a high chance that someone else can gain access to it without the knowledge of the user.

Health data signals which are collected from the patients using Body Sensor Networks are stored on a health system implemented on blockchain. Keys are used in encrypting data collected from patients. Fuzzy vault technology has been proposed to protect the keys using a light backup and retrieval scheme for key management. The system, however, lacks details about the blockchain network and its working method. No implementation has been done for the proposed blockchain health network. Body sensor networks have been used as a lightweight technique for the management of keys like backup and recovery. BSN has been used in health blockchain scheme which claims to provide high-security features and performance measures.

Cloud infrastructure has been utilized for secure storage and transmission of health data using elliptic curve cryptography [48]. Application simulation has been done to analyze application-related protocols and security. A mutual authentication method has been utilized for providing a secure infrastructure. Blockchain Security Framework (BSF) has been proposed for effective and secure storage of EHR in a decentralized manner [49]. The proposed model has extensive access to consistent patient records maintained with integrity and security against external attacks. Patients own their health information and provide access to stakeholders like participating institutions or doctors.

5. Research gap and proposed framework

Several attempts have been made to study and integrate the best capabilities of blockchain with healthcare infrastructure in recent years. Though some have attained intermittent solutions there is still a need for thorough research for fail-safe, secure, and scalable methodologies to be implemented in real-time in large-scale healthcare networks. Some proposed systems are prone to a single point of failure, attacks, and severely biased third-party storage clouds. Few of the proposed works do not address scalability issues which is a huge limitation when considering healthcare networks. The latest research works from recent years have been selected and their shortfalls have been displayed, which can be enhanced to provide better solutions in the future. Table 5 provides a list of recent works, their limitations, and future work proposed.

To overcome the research gaps in earlier works, a blockchain-based framework has been designed that addresses data privacy and security concerns in storing patient data without compromising the decentralized feature of blockchain and the scalability of the EHR management model. The proposed work aims at a patient-centric model for accessing EHR stored in Blockchain, integrated with the IPFS network. The new framework comprises different entities as follows, several decentralized nodes/systems, blockchain consensus, and cryptographic algorithms.

Table 5. Limitations of state-of-art schemes

Work	Limitations	Future work proposed
[39]	Implementation and testing are done in a single hospital rather than a group of collaborating hospital nodes A single point of failure of the system can occur if only a single orderer and single CA are employed In case of emergencies, there is no "break-glass" mechanism for bypassing the access control policy No recovery mechanism is defined in case the patient loses the key used for unlocking his/her data	Setup a pilot network with real-time testing of health data and optimize throughput, decision-making, and cost
[40]	The current system works over a local environment; has to be deployed over a larger network Blockchain created is for small-time use and is not feasible for a large-scale network The process is being run via the terminal; no user interface for patients Block is mined by virtual nodes, not actual miners	Resource trading can be investigated along with the industrial IoT to deliver EHR messages as a resource for business ecosystem development Integrating more lightweight IoT devices, protocols, and platforms with the proposed system
[41]	System prone to 51% attacks The user is not anonymous as the System Manager can map the identity to an individual using the ID stored in the DB No information was provided about the Database or storage where data will be lying The mining process is not defined as who will participate in the mining process, who will be full nodes, or who will be lightweight nodes Details on implementation, framework deployed, and testing not provided sufficiently The system Manager acts as a single point of failure as he is the gateway for creating secret keys and storing data after encryption Not patient-centric	None provided
[42]	Evaluation is done on blockchain module not presented clearly ABMS module was analyzed only based on a varying number of attributes and attribute lengths; Security features and other computational overheads were not analyzed	None provided
[43]	Single point of Failure – The admin has full access to the system, including write, read, update, and removal of participants Admin provides access to patients, clinicians, and other users for the records in Blockchain Immutability property is not preserved. The clinician is provided the right to update the EHR	None provided
[44]	Only the scalability aspect of the system has been studied The simulation model proposed lacks concrete results In the illustrated model, the number of transactions is 0. Lacks real-time simulation data	Reuse of proposed framework for study on other key factors such as privacy, security, governance, or interoperability
[45]	Additional overhead due to the resources required to mine a new block and broadcast to all nodes on the networks Admin acts as the governing body for registrations leading to a single point of failure	Scalability issues to be addressed Computational overhead in mining and broadcasting nodes needs to be addressed.

Table 5 (continued)

Work	Limitations	Future work proposed
[46]	Fault Tolerance not addressed Network with two organizations with one peer each is considered for testing A centralized Hospital Database used Cryptographic Techniques like encryption and signatures are not defined	The authors aim to extend the work of Kafka and PBFT ordering services with fault tolerance
[47]	Compatibility with existing medical data management systems not studied Orderer generates blocks with patient identity, patient identity not pseudonymous Storage and retrieval of EHR from IPFS not studied	Study the compatibility of the system with existing medical infrastructure
[48]	Lack of implementation details Network admin and cloud provider may act as a single point of failure	Develop a set of realistic protocols and test them
[49]	Client interface not defined properly; lack of End-to-End development of prototype Lack of details on blockchain framework such as verification process, mining, etc. Patients and doctors may not have the capacity to run full nodes in the client systems	Application of framework in other domains such as supply chain, logistics, IoT

Model overview: When patients visit the hospital, each patient's data will be uploaded by hospital nodes to temporary storage in the hospital network. Later data will be encrypted and moved to IPFS storage. A symmetric key created by the patient is used to encrypt data before storing it in IPFS. Output hash returned from IPFS will act as a pointer to encrypted patient health data, which is stored in the blockchain network. Patient health data will not be available to doctors/hospitals until the patient provides them access. The symmetric key used for encryption will be shared with doctor nodes for the decryption of patient data. This symmetric key will be shared via a key transaction which will be encrypted using the doctor's public key, which will make sure only the doctor can decrypt and get the symmetric key. The doctor will not be able to save physically the key or share it with anyone, hence it will remain safe. In addition, patients can generate a new symmetric key if they feel that the key is no safer. Below Fig. 5 gives an overview of the proposed framework.

The blockchain network in the model will ensure data privacy and security along with decentralized control. IPFS storage will enable the scalability feature of the system. Patient-centric access model will ensure ownership of health data to patients only, with limited/time-based access to doctors and other institutional nodes.

6. Road map for blockchain-based healthcare systems

Blockchain is an emerging, disruptive technology that shows positive signs in the future of decentralized healthcare systems. Though the technology is very promising, it may not be applied in healthcare systems abruptly. Thorough experiments and pilot projects are required before the real-time implementation of fully decentralized blockchain-based healthcare systems. Initially, it should start with small pivot projects being rolled out. Pilot projects should be using dummy patient data or non-critical data from existing EHR systems. Later it should be transitioned to a fully decentralized, patient-centric health records management system.

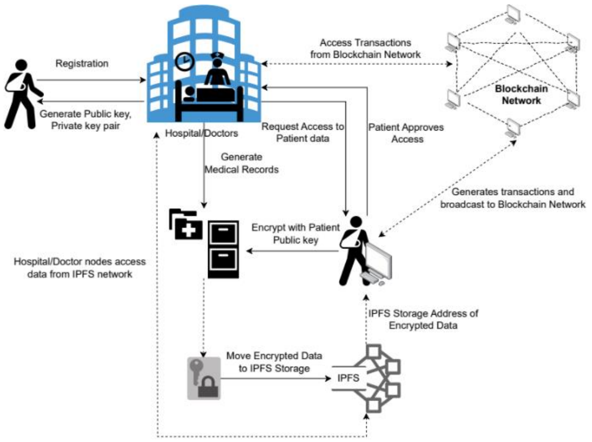
Registration
Generate Public key, Private key pair
Hospital/Doctors
Access Transactions from Blockchain Network
Blockchain Network
Request Access to Patient data
Patient Approves Access
Generate Medical Records
Generates transactions and broadcast to Blockchain Network
Encrypt with Patient Public key
Hospital/Doctor nodes access data from IPFS network
IPFS Storage Address of Encrypted Data
Move Encrypted Data to IPFS Storage
IPFS

Fig. 5. Proposed framework

As the transition happens, centralization of health data and duplication will be reduced. The amount of patient data handled, participating healthcare providers, and other stakeholders like the patient, doctors, and research institutions will increase. When the transition is complete, the entire healthcare infrastructure will be decentralized and the patient will hold ownership of their data. The scalability of the system will be high as the network is decentralized. A sample road map for transition is provided in Fig. 6 below.

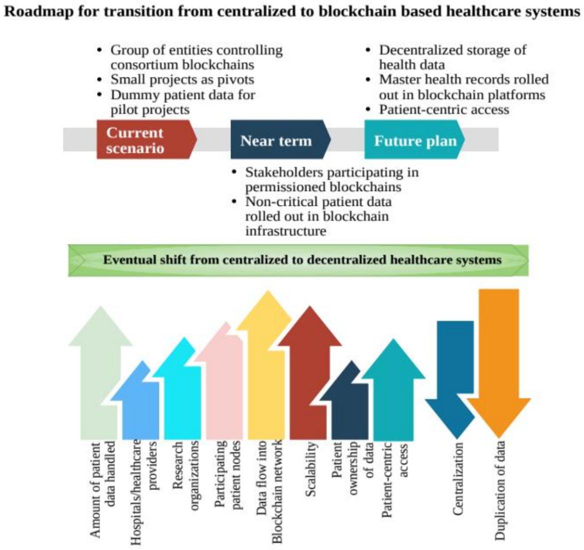
Roadmap for transition from centralized to blockchain based healthcare systems
• Group of entities controlling consortium blockchains
• Small projects as pivots
• Dummy patient data for pilot projects
• Decentralized storage of health data
• Master health records rolled out in blockchain platforms
• Patient-centric access
Current scenario
Near term
Future plan
• Stakeholders participating in permissioned blockchains
• Non-critical patient data rolled out in blockchain infrastructure
Eventual shift from centralized to decentralized healthcare systems
Amount of patient data handled
Hospitals/healthcare providers
Research organizations
Participating patient nodes
Data flow into Blockchain network
Scalability
Patient ownership of data
Patient-centric access
Centralization
Duplication of data

Fig. 6. Roadmap – Transition to Blockchain Healthcare Model

7. Conclusion

Blockchain technology is a persistently refining technology rather than accomplished technology that possesses multiple technical challenges that must be solved before it can be fully embraced for healthcare applications. The healthcare industry has a lot of applications that can leverage the potential of blockchain, however, the latter has not matured that much today nor is a magic potion available that can be applied to reap all its identified benefits. Several aspects need to be addressed before applying it worldwide. Some of the technical challenges revolve around transparency, confidentiality, speed, and scalability. In a public blockchain, the data is transparent to all the network participants which may pose a risk to confidentiality. This can however be addressed by storing only the hash of the metadata on-chain and storing the actual data off-chain, such as IPFS.

References

1. Feng, Q., D. He, S. Zeadally, M. K. Khan, N. Kumar. A Survey on Privacy Protection in Blockchain System. – Journal of Network and Computer Applications, Vol. **126**, 2019, pp. 45-58.
2. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Technical Report, Manubot, 2019.
3. Classification of Blockchains. Online, Last accessed 8 January 2024. **https://en.bitcoinwiki.org/wiki/Classification-of-blockchains**
4. Farah, N. A. A. Blockchain Technology: Classification, Opportunities, and Challenges. – International Research Journal of Engineering and Technology (IRJET), Vol. **5**, 2018, No 5.
5. Public, Private, Consortium Blockchains. Online, Last accessed 08 January 2024. **https://www.coursera.org/lecture/blockchain-foundations-and-use-cases/lesson-2-public-private-consortium-blockchains-hDSxZ**
6. Swan, M. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., 2015.
7. Pilkington, M. Blockchain Technology: Principles and Applications. – In: Research Handbook on Digital Transformations, Edward Elgar Publishing, 2016.
8. Underwood, S. Blockchain Beyond Bitcoin. Commun. – ACM, Vol. **59**, 2016, No 11, pp. 15-17. ISSN: 0001-0782. DOI: 10.1145/2994581.
9. Radziwill, N. Blockchain Revolution: How the Technology behind Bitcoin is Changing Money, Business, and the World. – The Quality Management Journal, Vol. **25**, 2018, No 1, pp. 64-65.
10. Introduction to Blockchain Features. Online, Last accessed 8 January 2024. **https://101blockchains.com/introduction-to-blockchain-features/**
11. 6 Key Features of Blockchain. Online, Last accessed 8 January 2024. **https://thefintechway.com/6-key-features-of-blockchain/**
12. Jayapriya, J., N. Jeyanthi. Proof of Virtue: Nonce-Free Hash Generation in Blockchain. – In Managing Security Services in Heterogeneous Networks, CRC Press, 2020, pp. 63-74.
13. Bitcoin. Online, Last accessed 8 January 2024. **https://bitcoin.org/en/**
14. Radeva, I., I. Popchev. Blockchain-Enabled Supply-Chain in Crop Production Framework. – Cybernetics and Information Technologies, Vol. **22**, 2022, No 1, pp. 151-170.
15. Dorri, A., S. S. Kanhere, R. Jurdak. Blockchain in Internet of Things: Challenges and Solutions. – arXiv preprint arXiv:1608.05187, 2016.
16. Sudha, K. S., N. Jeyanthi. A Review on Privacy Requirements and Application Layer Security in Internet of Things (IoT). – Cybernetics and Information Technologies, Vol. **21**, 2021, No 3, pp. 50-72.
17. Kim, H. M., M. Laskowski. Toward an Ontology-Driven Blockchain Design for Supply-Chain Provenance. – Intelligent Systems in Accounting, Finance and Management, Vol. **25**, 2018, No 1, pp. 18-27.
18. Korpela, K., J. Hallikas, T. Dahlberg. Digital Supply Chain Transformation toward Blockchain Integration. – In: Proc. of 50th Hawaii International Conference on System Sciences, 2017.

19. Abeyratne, S. A., R. P. Monfared. Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. – International Journal of Research in Engineering and Technology, Vol. **5**, 2016, No 9, pp. 1-10.

20. Ali, M., J. Nelson, R. Shea, M. J. Freedman. Blockstack: A Global Naming and Storage System Secured by Blockchains. – In: Proc. of {USENIX 2016} Annual Technical Conference ({USENIX}{ATC}'16), 2016, pp. 181-194.

21. Fromknecht, C., D. Velicanu, S. Yakoubov. A Decentralized Public Key Infrastructure with Identity Retention. – IACR Cryptology ePrint Archive, Vol. **2014**, 2014, No 803.

22. Ebrahimi, A. Identity Management Service Using a Blockchain Providing Certifying Transactions between Devices. 1 August 2017. US Patent 9,722,790.

23. Qin, B., J. Huang, Q. Wang, X. Luo, B. Liang, W. Shi. CECOIN: A Decentralized PKI Mitigating M-i-T-M Attacks. – In: Future Generation Computer Systems. Elsevier, 2017.

24. Binded – Copyright Made Simple. Online, Last accessed 8 January 2024.
https://binded.com/

25. Maidsafe – The New Decentralized Internet. Online, Last accessed 8 January 2024.
https://www.maidsafe.net/

26. Jayabalan, J., N. Jeyanthi. Scalable Blockchain Model Using Off-Chain IPFS Storage for Healthcare Data Security and Privacy. – Journal of Parallel and Distributed Computing, Vol. **164**, 2022, pp. 152-167. ISSN 0743-7315.
DOI: https://doi.org/10.1016/j.jpdc.2022.03.009.
https://www.sciencedirect.com/science/article/pii/S0743731522000648

27. Esposito, C., A. De Santis, G. Tortora, H. Chang, K.-K. R. Choo. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? – IEEE Cloud Computing, Vol. **5**, 2018, No 1, pp. 31-37.

28. Jin, H., Y. Luo, P. Li, J. Mathew. A Review of Secure and Privacy-Preserving Medical Data Sharing. – IEEE Access, Vol. **7**, 2019, pp. 61656-61669.

29. Kassab, M. H., J. DeFranco, T. Malas, P. Laplante, V. V. G. Neto, et al. Exploring Research in Blockchain for Healthcare and a Roadmap for the Future. – In: IEEE Transactions on Emerging Topics in Computing. 2019.

30. Kuo, T.-T., H.-E. Kim, L. Ohno-Machado. Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications. – Journal of the American Medical Informatics Association, Vol. **24**, 2017, No 6, pp. 1211-1220.

31. Drew, I. Moving toward a Blockchain-Based Method for the Secure Storage of Patient Records. – In: Proc. of ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, Maryland, United States: ONC/NIST, 2016, pp. 1-11.

32. Kumar, T., V. Ramani, I. Ahmad, A. Braeken, E. Harjula, M. Ylianttila. Blockchain Utilization in Healthcare: Key Requirements and Challenges. – In: Proc. of 20th IEEE International Conference on e-Health Networking, Applications and Services (Healthcom'18), IEEE, 2018, pp. 1-7.

33. Omar, A. A., M. S. Rahman, A. Basu, S. Kiyomoto. Medibchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. – In: Proc. of International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, 2017, pp. 534-543.

34. Xia, Q., E. B. Sifah, A. Smahi, S. Amofa, X. Zhang. BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. – Information, Vol. **8**, 2017, No 2, 44.

35. Kim, K., S.-phil Hong. A Trusted Sharing Model for Patient Records Based on Permissioned Blockchain. – Journal of Internet Computing and Services, Vol. **18**, 2017, pp. 75-84.

36. Liang, X., J. Zhao, S. Shetty, J. Liu, D. Li. Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications. – In: Proc. of 28th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'17), IEEE, 2017, pp. 1-5.

37. Rajput, A. R., Q. Li, M. T. Ahvanooey, I. Masood. EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain. – IEEE Access, Vol. **7**, 2019, pp. 84304-84317.

38. Niu, S., L. Chen, J. Wang, F. Yu. Electronic Health Record Sharing Scheme with Searchable Attribute-Based Encryption on Blockchain. – IEEE Access, 2019.
39. Dubovitskaya, A., F. Baig, Z. Xu, R. Shukla, P. S. Zambani, A. Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, et al. Action-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care. – Journal of Medical Internet Research, Vol. **22**, 2020, No 8, e13598.
40. Ray, P. P., B. Chowhan, N. Kumar, A. Almogren. BIOTHR: Electronic Health Record Servicing Scheme in Iot-Blockchain Ecosystem. – IEEE Internet of Things Journal, 2021.
41. Shamshad, S., K. Mahmood, S. Kumari, C.-M. Chen, et al. A Secure Blockchain-Based e-Health Records Storage and Sharing Scheme. – Journal of Information Security and Applications, Vol. **55**, 2020, 102590.
42. Guo, H., W. Li, E. Meamari, C.-C. Shen, M. Nejad. Attribute-Based Multi-Signature and Encryption for EHR Management: A Blockchain-Based Solution. – In: Proc. of IEEE International Conference on Blockchain and Cryptocurrency (ICBC'20), IEEE, 2020, pp. 1-5.
43. Tanwar, S., K. Parekh, R. Evans. Blockchain-Based Electronic Healthcare Record System for Healthcare 4.0 Applications. – Journal of Information Security and Applications, Vol. **50**, 2020, 102407.
44. Garrido, A., L. J. R. López, N. B. Álvarez. A Simulation-Based AHP Approach to Analyze the Scalability of EHR Systems Using Blockchain Technology in Healthcare Institutions. – Informatics in Medicine Unlocked, Vol. **24**, 2021, 100576.
45. Fatokun, T., A. Nag, S. Sharma. Towards a Blockchain Assisted Patient Owned System for Electronic Health Records. – Electronics, Vol. **10**, 2021, No 5, 580.
46. Singh, A. P., N. R. Pradhan, A. K. Luhach, S. Agnihotri, N. Z. Jhanjhi, S. Verma, U. Ghosh, D. S. Roy, et al. A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications. – IEEE Transactions on Industrial Informatics, Vol. **17**, 2020, No 8, pp. 5779-5789.
47. Li, F., K. Liu, L. Zhang, S. Huang, Q. Wu. EHRchain: A Blockchain-Based EHR System Using Attribute-Based and Homomorphic Cryptosystem. – IEEE Transactions on Services Computing, 2021.
48. Kim, M. H., S. J. Yu, J. Y. Lee, Y. H. Park, Y. H. Park. Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain. – Sensors, Vol. **20**, 2020, No 10, 2913.
49. Abunadi, I., R. L. Kumar. BSF-HER: Blockchain Security Framework for Electronic Health Records of Patients. – Sensors, Vol. **21**, 2021, No 8, 2865.
50. Wang, S., J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, F.-Y. Wang. Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. – IEEE Transactions on Computational Social Systems, Vol. **5**, 2018, No 4, pp. 942-950.
51. Zhang, A., X. Lin. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. – Journal of Medical Systems, Vol. **42**, 2018, No 8, 140.
52. Wang, Y., A. Zhang, P. Zhang, H. Wang. Cloud-Assisted EHR Sharing with Security and Privacy Preservation via Consortium Blockchain. – IEEE Access, Vol. **7**, 2019, pp. 136704-136719.
53. Liu, X., Z. Wang, C. Jin, F. Li, G. Li. A Blockchain-Based Medical Data Sharing and Protection Scheme. – IEEE Access, Vol. **7**, 2019, pp. 118943-118953.
54. Linn, L. A., M. B. Koo. Blockchain for Health Data and Its Potential Use in Health it and Health Care Related Research. – In: Proc. of ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, Maryland, US, ONC/NIST, 2016, pp. 1-10.
55. Xu, J., 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 of Things Journal, Vol. **6**, 2019, No 5, pp. 8770-8781.
56. Ismail, L., H. Materwala, S. Zeadally. Lightweight Blockchain for Healthcare. – IEEE Access, Vol. **7**, 2019, pp. 149935-149951.
57. Kuo, T.-T., L. Ohno-Machado. Modelchain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. – arXiv preprint arXiv:1802.01746, 2018.

58. Peterson, K., R. Deeduvanu, P. Kanjamala, K. Boles. A Blockchain-Based Approach to Health Information Exchange Networks. – In: Proc. of NIST Workshop Blockchain Healthcare, Vol. **1**, 2016, pp. 1-10.
59. Fan, K., S. Wang, Y. Ren, H. Li, Y. Yang. Medblock: Efficient and Secure Medical Data Sharing via Blockchain. – Journal of Medical Systems, Vol. **42**, 2018, No 8, 136.
60. Zhang, P., J. White, D. C. Schmidt, G. Lenz, S. T. Rosenbloom. Fhirchain: Applying Blockchain to Securely and Scalably Share Clinical Data. – Computational and Structural Biotechnology Journal, Vol. **16**, 2018, pp. 267-278.
61. Dagher, G. G., J. Mohler, M. Milojkovic, P. B. Marella. ANCILE: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. – Sustainable Cities and Society, Vol. **39**, 2018, 283-297.
62. Li, H., L. Zhu, M. Shen, F. Gao, X. Tao, S. Liu. Blockchain-Based Data Preservation System for Medical Data. – Journal of Medical Systems, Vol. **42**, 2018, No 8, 141.
63. Jeyanthi, P. N. TSCBA-A Mitigation System for ARP Cache Poisoning Attacks. – Cybernetics and Information Technologies, Vol. **18**, 2018, No 4, pp. 75-93.
64. McFarlane, C., M. Beer, J. Brown, N. Prendergast. Patientory: A Healthcare Peer-to-Peer EMR Storage Network V1. – Entrust, Inc., Addison, TX, USA, 2017.
65. Prabadevi, B., N. Jeyanthi. Security Solution for ARP Cache Poisoning Attacks in Large Data Center Networks. – Cybernetics and Information Technologies, Vol. **17**, 2017, No 4, pp.69-86.
66. Azaria, A., A. Ekblaw, T. Vieira, A. Lippman. Medrec: Using Blockchain for Medical Data Access and Permission Management. – In: Proc. of 2nd International Conference on Open and Big Data (OBD’16), IEEE, 2016, pp. 25-30.
67. Ramani, V., T. Kumar, A. Bracken, M. Liyanage, M. Ylianttila. Secure and Efficient Data Accessibility in Blockchain Based Healthcare Systems. – In: Proc. of IEEE Global Communications Conference (GLOBECOM’18), IEEE, 2018, pp. 206-212.
68. Gordon, W. J., C. Catalini. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. – Computational and Structural Biotechnology Journal, Vol. **16**, 2018, pp. 224-230.
69. Shahnaz, A., U. Qamar, A. Khalid. Using Blockchain for Electronic Health Records. – IEEE Access, Vol. **7**, 2019, pp. 147782-147795.
70. Jiang, S., J. Cao, H. Wu, Y. Yang, M. Ma, J. He. BLOCHIE: A Blockchain-Based Platform for Healthcare Information Exchange. – In: Proc. of International IEEE Conference on Smart Computing (SmartComp’18), IEEE, 2018, pp. 49-56.
71. Zyskind, G., O. Nathan, et al. Decentralizing Privacy: Using Blockchain to Protect Personal Data. – In: Proc. of IEEE Security and Privacy Workshops, IEEE, 2015, pp. 180-184.
72. Yue, X., H. Wang, D. Jin, M. Li, W. Jiang. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. – Journal of Medical Systems, Vol. **40**, 2016, No 10, 218.
73. Brindha, K., N. Jeyanthi. Secured Document Sharing Using Visual Cryptography in Cloud Data Storage. – Cybernetics and Information Technologies, Vol. **15**, 2015, No 4, pp. 111-123.
74. Wang, S., D. Zhang, Y. Zhang. Blockchain-Based Personal Health Records Sharing Scheme with Data Integrity Verifiable. – IEEE Access, Vol. **7**, 2019, pp. 102887-102901.
75. Chen, Y., S. Ding, Z. Xu, H. Zheng, S. Yang. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. – Journal of Medical Systems, Vol. **43**, 2019, No 1.
76. Xia, Q., E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, M. Guizani. Medshare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. – IEEE Access, Vol. **5**, 2017, pp. 14757-14767.
77. Nguyen, D. C., P. N. Pathirana, M. Ding, A. Seneviratne. Blockchain for Secure EHR Sharing of Mobile Cloud Based e-Health Systems. – IEEE Access, Vol. **7**, 2019, pp. 66792-66806.
78. Zhang, X., S. Poslad. Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR). – In: Proc. of IEEE International Conference on Communications (ICC’18), IEEE, 2018, pp. 1-6.

79. Dubovitskaya, A., Z. Xu, S. Ryu, M. Schumacher, F. Wang. Secure and Trustable Electronic Medical Records Sharing Using Blockchain. – In: AMIA Annual Symposium Proceedings, American Medical Informatics Association, Vol. **2017**, 2017, p. 650.
80. Yang, H., B. Yang. A Blockchain-Based Approach to the Secure Sharing of Healthcare Data. – In: Proc. of Norwegian Information Security Conference, 2017.
81. Guo, R., H. Shi, Q. Zhao, D. Zheng. Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems. – IEEE Access, Vol. **6**, 2018, pp. 11676-11686.
82. Tang, F., S. Ma, Y. Xiang, C. Lin. An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records. – IEEE Access, Vol. **7**, 2019, pp. 41678-41689.
83. Guo, R., 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, Vol. **7**, 2019, pp. 88012-88025.

Received: 08.08.2022; Second Version: 28.12.2023; Third Version: 09.01.2024;
Accepted: 18.01.2024