Computers & Security 97 (2020) 101966

Contents lists available at ScienceDirect

Computers & Security

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

Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey

Shuyun Shi[a,b], Debiao He[a,b,*], Li Li[a], Neeraj Kumar[c,d], Muhammad Khurram Khan[e], Kim-Kwang Raymond Choo[f]

[a] School of Cyber Science and Engineering, Wuhan University, Wuhan, China
[b] Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin, China
[c] Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, India
[d] Department of Computer Science and Information Engineering, Asia University, Taiwan
[e] Center of Excellence in Information Assurance, College of Computer & Information Sciences, King Saud University, Saudi Arabia
[f] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, USA

ARTICLE INFO

Article history:
Received 5 February 2020
Revised 8 July 2020
Accepted 14 July 2020
Available online 15 July 2020

Keywords:
Blockchain
Healthcare
Electronic health record system
Security
Privacy

ABSTRACT

Due to the popularity of blockchain, there have been many proposed applications of blockchain in the healthcare sector, such as electronic health record (EHR) systems. Therefore, in this paper we perform a systematic literature review of blockchain approaches designed for EHR systems, focusing only on the security and privacy aspects. As part of the review, we introduce relevant background knowledge relating to both EHR systems and blockchain, prior to investigating the (potential) applications of blockchain in EHR systems. We also identify a number of research challenges and opportunities.

1. Introduction

There is an increasing interest in digitalizing healthcare systems by governments and related industry sectors, partly evidenced by various initiatives taking place in different countries and sectors. For example, the then U.S. president signed into law the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as part of the American Recovery and Reinvestment Act of 2009. HITECH is designed to encourage broader adoption of electronic health records (EHRs), with the ultimate aim of benefiting patients and society. The potential benefits associated with EHR systems (e.g. public healthcare management, online patient access, and patients medical data sharing) have also attracted the interest of the research community (Boonstra et al., 2014; Carvalho et al., 2016; Crameri et al., 2020; Fernández-Alemán et al., 2013a; Ho et al., 2019; Lluch, 2011; Miah et al., 2019; Strudwick and Eyasu, 2015; Tovanich et al., 2020). The potential of EHRs is also evidenced by the recent 2019 novel coronavirus (also referred to as 2019-nCoV and COVID-2019) pandemic, where remote patient monitoring and other healthcare deliveries are increasingly used in order to contain the situation.

As with any maturing consumer technologies, there are a number of research and operational challenges. For example, many existing EHR systems use a centralized server model, and hence such deployments inherit security and privacy limitations associated with the centralized server model (e.g. single point of failure and performance bottleneck). In addition, as EHR systems become more commonplace and the increasing understanding of the importance of data (particularly healthcare data), honest but curious servers may surreptitiously collect personal information of users while carrying out their normal activities.

In recent times, there is an increasing trend in deploying blockchain in a broad range of applications, including healthcare (e.g. public healthcare management, counterfeit drug prevention, and clinical trial) (Esposito et al., 2018; McGhin et al., 2019; Peterson et al., 2016). This is not surprising, since blockchain is an immutable, transparent and decentralized distributed database (Ahram et al., 2017) that can be leveraged to provide a secure and trusty value chain.

An architecture of blockchain-based healthcare systems is shown in Fig. 1. Blockchain is a distributed ledger database on a peer-to-peer (P2P) network that comprises a list of ordered blocks

* Corresponding author at: Computer School Luo Jia Shan, Wuhan 430072, China.
E-mail address: hedebiao@163.com (D. He).

https://doi.org/10.1016/j.cose.2020.101966
0167-4048/

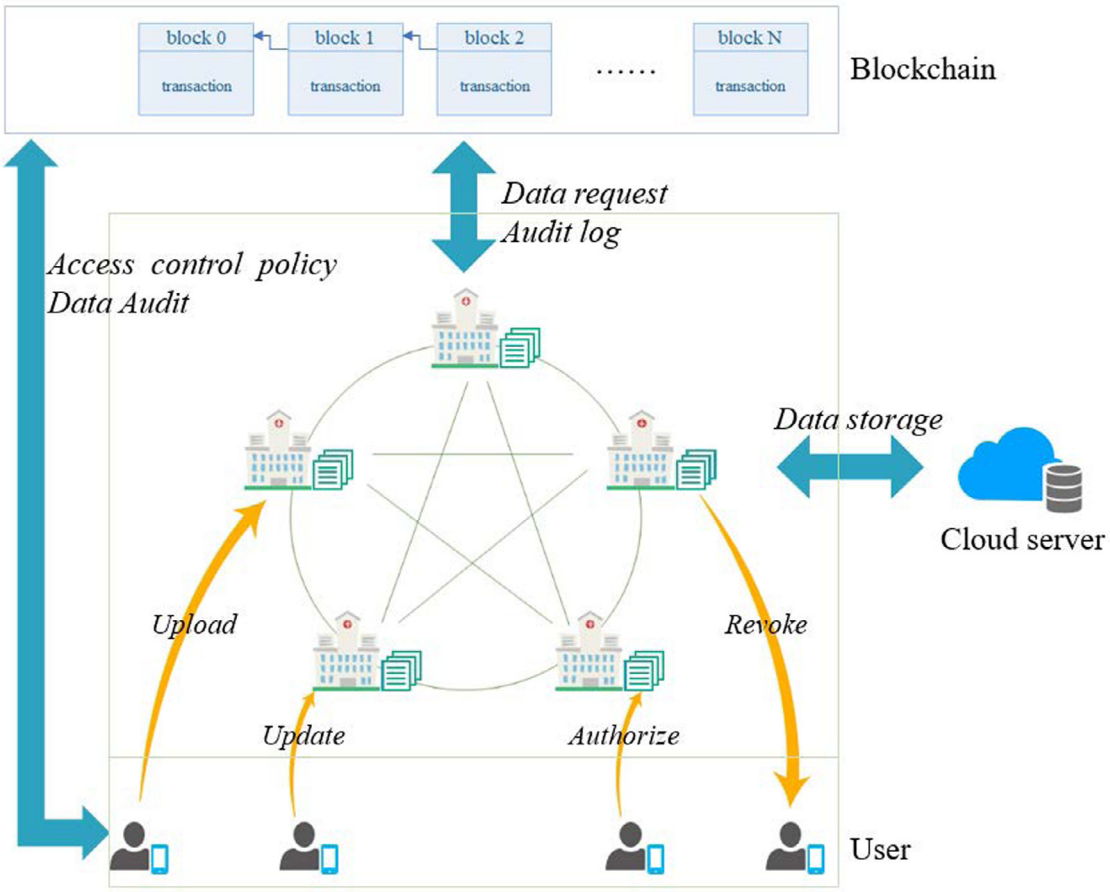

Fig. 1. Blockchain-based healthcare system: An example architecture.

chronologically. In other words, this is a decentralized and trustworthy distributed system (without relying on any third party). Trust relation among distributed nodes is established by mathematical methods and cryptography technologies instead of semi-trusted central institutions. Blockchain-based systems can mitigate the limitation of the single point of failure. Besides, since data is recorded in the public ledger, and all of nodes in the blockchain network have ledger backups and can access these data anytime and anywhere, such a system ensures data transparency and helps to build trust among distributed nodes. It also facilitates data audit and accountability by having the capability to trace tamper-resistant historical record in the ledger. Depending on the actual deployment, data in the ledger can be stored in the encrypted form using different cryptographic techniques; hence, preserving data privacy. Users can also protect their real identities in the sense of pseudo-anonymity. To enhance robustness, we can introduce smart contracts (i.e. a kind of self-executing program deployed on the distributed blockchain network) to support diverse functions for different application scenarios. Specifically, the terms of smart contract can be preset by users and the smart contract will only be executed if the terms are fulfilled. Hence, this hands over control to the owner of the data. There are a (small) number of real-world blockchain-based healthcare systems, such as *Gem, Guardtime* and *healthbank* (Mettler, 2016).

Hence, in this paper we focus on blockchain-based healthcare systems. Specifically, we will comprehensively review some existing work, and identify existing and emerging challenges and potential research opportunities. Prior to presenting the results of our review, we will first introduce EHR system and blockchain architecture in the next section. Then, in Section 3, we will review the extant literature and provide a comparative summary of some existing systems. In Section 4, we identify a number of potential research opportunities. Finally, we conclude the paper in the last section.

2. Background

In a centralized architecture, such as those that underpin a conventional EHR system, a central institution is tasked with managing, coordinating and controlling of the entire network. However, in a distributed architecture, all nodes are maintained without relying on a central authority. Now, we will briefly explain the EHR system and blockchain technology.

2.1. EHR Systems

The electronic health record (EHR) is generally defined to be the collection of patients' electronic health information (e.g. in the form of electronic medical records – EMRs). EMRs can serve as a data source for EHR mainly from healthcare providers in the medical institutions. The personal health record (PHR) contains personal healthcare information, such as those obtained from wearable devices owned and controlled by patients. Information collected as part of PHRs can be available to healthcare providers, by users (patients).

In theory, EHR systems should ensure the confidentiality, integrity and availability of the stored data, and data can be shared securely among authorized users (e.g. medical practitioners with the right need to access particular patient's data to facilitate diagnosis). In addition, such a system if implemented well, can reduce

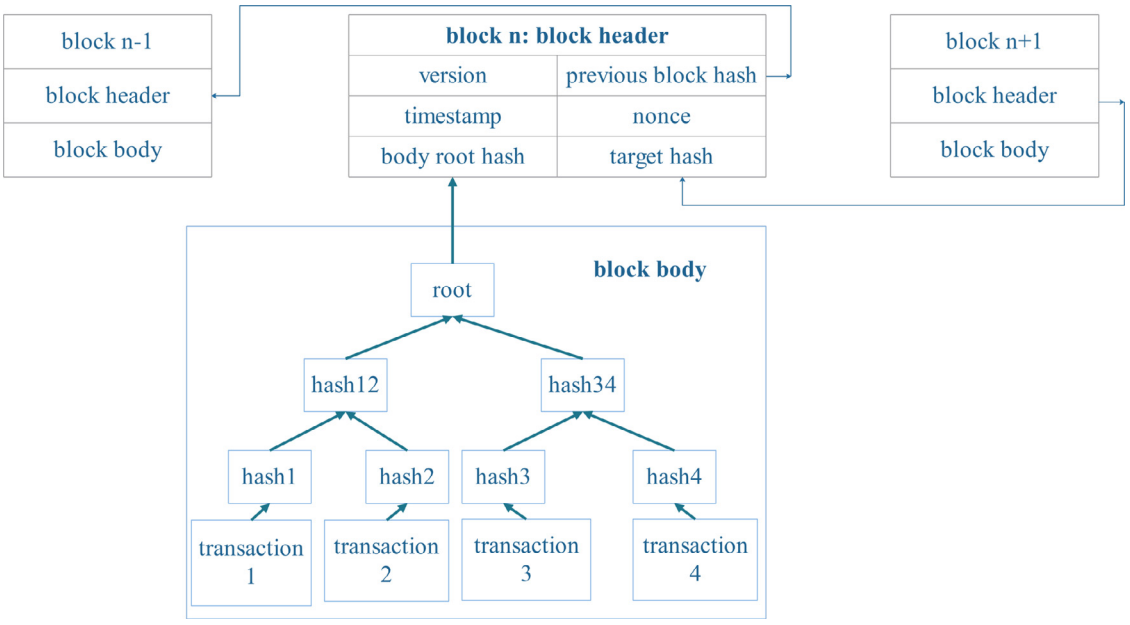

Fig. 2. Block structure.

data replication and the risk of lost record, and so on. However, the challenge of securing data in such systems, whether in-transit or at-rest, is compounded by the increasing connectivity to these systems (e.g. more potential attack vectors). For example, mobile devices that can sync with the EHR system is a potential attack vector that can be targeted (e.g. an attacker can seek to exploit a known vulnerability in the hospital-issued mobile devices and install malware to facilitate covert exfiltration of sensitive data (e.g. PHRs)).

One of the key benefits of EHR systems is the availability of large volumes of data, which can be used to facilitate data analysis and machine learning, for example to inform other medical research efforts such as disease forecasting (e.g. the 2019 Novel Coronavirus). Furthermore, wearable and other Internet of Things (IoT) devices can collect and upload relevant information, including those relating to PHRs, to the EHR systems, which can facilitate healthcare monitoring and personalized health services.

2.2. Blockchain

Blockchain is made popular by the success of Bitcoin (Nakamoto et al., 2008), and can be used to facilitate trustworthy and secure transactions across an untrusted network without relying on any centralized third party. We will now introduce the fundamental building blocks in the blockchain (Feng et al., 2019; Lin et al., 2020; Ma et al., 2020).

Blockchain is a chronological sequence of blocks including a list of complete and valid transaction record. Blocks are linked to the previous block by a reference (hash value), and thus forming a chain. The block preceding a given block is called its *parent block*, and the first block is known as the *genesis block*.

A block (Nakamoto et al., 2008) consists of the block header and the block body, as shown in Fig. 2.

The block header contains:

- *Block version*: block validation rules;
- *Previous block hash*: hash value of the previous block;
- *Timestamp*: the creation time of the current block;
- *Nonce*: a 4-byte random field that miners adjust for every hash calculation to solve a PoW mining puzzle (see also Section 2.2.2);
- *Body root hash*: hash value of the Merkle tree root built by transactions in the block body;
- *Target hash*: target threshold of hash value of a new valid block. The target hash is used to determine the difficulty of the PoW puzzle (see also Section 2.2.2).

The block body consists of validated transactions within a specific time period. The *Merkle tree* is used to store all the valid transactions, in which every leaf node is a transaction and every non-leaf node is the hash value of its two concatenated child nodes. Such a tree structure is efficient for the verification of the transaction's existence and integrity, since any node can confirm the validation of any transaction by the hash value of the corresponding branches rather than entire Merkle tree. Meanwhile, any modification on the transaction will generate a new hash value in the upper layer and this will result in a falsified root hash. Besides, the maximum number of transactions that a block can contain depends on the size of each transaction and the block size.

These blocks are then chained together using cryptographic hash function in an append-only structure. That means new data is only appended in the form of additional blocks chained with previous blocks since altering and deleting previously confirmed data is impossible. As previously discussed, any modification of one of the blocks will generate a different hash value and different link relation. Hence, achieving immutability and security.

2.2.1. Digital signature

Digital signature based on asymmetric cryptography is generally used for transaction authentication in an untrustworthy environment (Feng et al., 2020; He et al., 2018). Blockchain uses asymmetric cryptography mechanism to send transactions and verify the authentication of transactions. The transaction is signed using the sender's private key, prior to being sent over the P2P network. The elliptic curve digital signature algorithm (ECDSA) is typically used in the existing blockchain (Johnson et al., 2001).

Once any transaction is sent, it is broadcasted to all neighboring nodes through the P2P network, where peers are equally privileged participants. Once other nodes receive the transaction, the sender's public key is used to verify the authenticity of this received transaction according to predefined block validation rules. If the transaction is valid, it will be forwarded to other nodes until

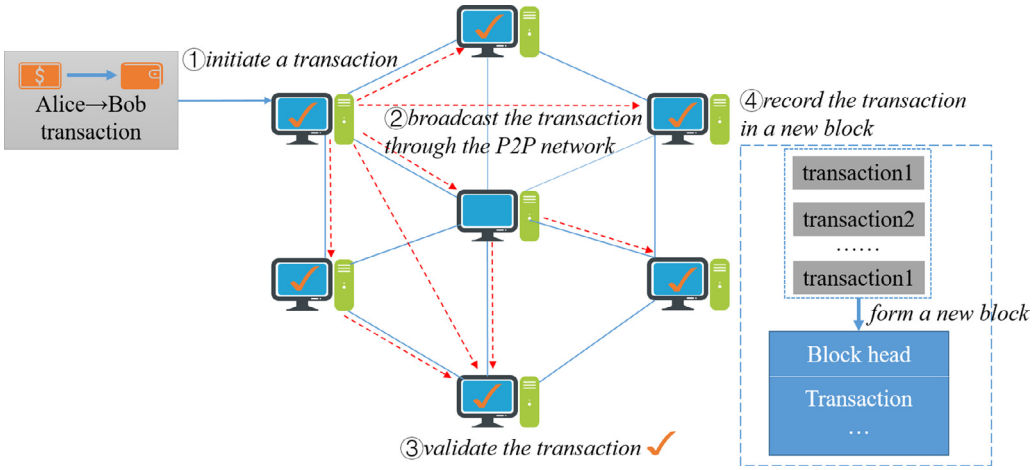

Fig. 3. working flow of transaction in the blockchain.

all the nodes receive and verify the transaction. Otherwise, it will be discarded in this process. Only valid transactions can be stored in the new block of blockchain network.

We will take the coin transfer as an example (see Fig. 3). Alice transfers a certain amount of coins to Bob. In step 1, she initiates a transaction signed by her private key. The transaction can be easily verified by others using Alice's public key. In step 2, the transaction is broadcasted to other nodes through the P2P network. In step 3, each node will verify the transaction by predefined rules. In step 4, each validated transaction will be packed chronologically and appended to a new block once a miner solves the puzzle. Finally, every node will update and back up the new block.

2.2.2. Consensus algorithms

In the blockchain network, there is no trusted central authority. Thus, reaching a consensus for these transactions among untrustworthy nodes in a distributed network is an important issue, which is a transformation of the Byzantine Generals (BG) Problem proposed in Lamport et al. (1982). The BG problem is that a group of generals command the Byzantine army to circle the city, and they have no chance of winning the war unless all of them attack at the same time. However, they are not sure whether there are traitors who might retreat in a distributed environment. Thus, they have to reach an agreement to attack or retreat. It is the same challenge for the blockchain network.

A number of protocols have been designed to reach consensus among all the distributed nodes before a new block is linked into blockchain (Wang et al., 2019), such as the following:

- PoW (Proof of Work) is the consensus mechanism used in Bitcoin. If the *miner* node who has certain computing (hashing) power wishes to obtain some rewards, the miner must perform the laborious task of *mining* to prove that he is not malicious. The task requires that the node repeatedly performs hash computations to find an eligible *nonce* value that satisfies the requirement that a hashed block head must be less than (or equal to) the *target hash* value. The nonce is difficult to generate but easy for other nodes to validate. The task is costly (in terms of computing resources) due to the number of difficult calculations. A 51% attack is a potential attack in the blockchain network, where if a miner or a group of miners can control more than 51% of the computing power, they could interfere with the generation of new blocks and create fraudulent transaction records beneficial for the attackers.
- PoS (Proof of Stake) is an improved and energy-saving mechanism of PoW. It is believed that nodes with the largest number of stakes (e.g. currency) would be less likely to attack the network. However, the selection based on account balance is unfair because the richest node is more likely to be dominant in the network, which would be similar to a centralized system gradually.
- DPoS (Delegated Proof of Stake) is similar to PoS. The major difference between DPoS and PoS is that the selection of PoS is based on all of the nodes while DPoS is representative democratic. Stake-holders can elect their delegates to generate and validate new blocks. As fewer nodes validate the block, the more quickly the transactions could be confirmed by other nodes. Besides, the dishonest delegates could be voted out easily, which eases the maintenance of the whole network.
- PBFT (Practical Byzantine Fault Tolerance) is a replication algorithm to tolerate byzantine faults (Castro and Liskov, 1999), which comprises a three-phase protocol. These three phases are pre-prepared, prepared, and commit. A new block could be generated if it has received valid replies from over 2/3 of all the nodes in each phase. The correctness of the whole network could be guaranteed in the case of less than 1/3 malicious byzantine replicas nodes. Permissioned Hyperledger Fabric utilizes PBFT as its consensus algorithm to validate the transaction.
- Raft is a consensus algorithm to manage replicated logs across a cluster of computing nodes. In each term, only the elected leader is responsible for accepting new transactions and replicating these transactions for other followers. After the leader receives feedback from a certain amount of followers who have written the transactions, the transactions will be committed. Raft is appropriate for private/consortium blockchain, which can tolerate up to 50% nodes of crash fault.
- PoA (Proof of Authority) is an efficient consensus algorithm. Only nodes who are granted a right can generate new blocks. Before that, each node must pass a preliminary authentication. However, this approach tends towards a centralized pattern.
- PoC (Proof of Capacity) is a consensus mechanism that uses available hard disks space instead of computing resources. The more storage capacity you have, the more solutions you can store, and the higher the probability of creating a new block is.
- PoET (Proof of Elapsed Time) seeks to randomly and fairly choose who can produce a block based on the time that each participant has waited within a reliable execution environment.

Instead of relying only on a single consensus algorithm, there is a trend of integrating several consensus algorithms to improve the performance in different applications.

2.2.3. Smart contract

Smart contracts can be regarded as a self-executing program deployed on the blockchain, which have been utilized in various fields, such as financial services, healthcare and government. Such a mechanism can achieve complex programmable functions by sending a contract-invoking transaction to the relevant contract address. Then, smart contract will execute the predefined terms in the secure container automatically.

Ethereum is the first open-source blockchain platform that offers Turing-complete smart contract languages for developers to deploy arbitrary decentralized applications (DApps).

2.2.4. Taxonomy of blockchain systems

Blockchain systems are divided into three types based on permissions given to network nodes:

- *Public blockchain.* The public blockchain is open to anyone who wants to join anytime and acts as a simple node or as a miner for economic rewards. Bitcoin (Nakamoto et al., 2008) and Ethereum (Eth, 2015) are two well-known public blockchain platforms.
- *Private blockchain.* The private blockchain network works based on access control, in which participants must obtain an invitation or permissions to join. GemOS (Gem, 2020) and MultiChain (MultiChain, 2020) are both typical private blockchain platforms.
- *Consortium blockchain.* The consortium blockchain is "semi-private" sitting on the fence between public and private blockchains. It is granted to a group of approved organizations commonly associated with enterprise use to improve business. Hyperledger fabric (Hyperledger, 2020) is a business consortium blockchain framework. Ethereum also supports for building consortium blockchains.

2.3. Motivations for blockchain-based EHR systems

Generally, EHRs mainly contain patient medical history, personal statistics (e.g. age and weight), laboratory test results and so on. Hence, it is crucial to ensure the security and privacy of these data. In addition, hospitals in countries such as U.S. are subject to exacting regulatory oversight. There are also a number of challenges in deploying and implementing healthcare systems in practice. For example, centralized server models are vulnerable to the single-point attack limitations and malicious insider attacks, as previously discussed. Users (e.g. patients) whose data is outsourced or stored in these EHR systems generally lose control of their data, and have no way of knowing who is accessing their data and for what kind of purposes (i.e. violation of personal privacy). Such information may also be at risk of being leaked by malicious insiders to another organization, for example an insurance company may deny insurance coverage to the particular patient based on leaked medical history.

Meanwhile, data sharing is increasingly crucial particularly as our society and population become more mobile. By leveraging the interconnectivity between different healthcare entities, shared data can improve medical service delivery, and so on. Overcoming the "Information and Resource Island" (information silo) will be challenging, for example due to privacy concerns and regulations. The information silo also contributes to unnecessary data redundancy and red-tape.

In this case, the Health Insurance Portability and Accountability Act (HIPAA) was enacted by the United States Congress and signed in 1996. It established policies for maintaining the privacy and security of individual health information and created several programs to control fraud and abuse within the healthcare systems, including five rules:

- *Privacy Rule*. Regulations for the use and disclosure of patient health information in healthcare treatment and operations.
- *Transactions and Code Sets Rule*. Requirements for all health plans to engage in the healthcare transactions in a standardized way to simplify healthcare transactions.
- *Security Rule*. The security rule complements the privacy rule, including controlling access to computer systems and securing the communications over open networks from being intercepted.
- *Unique Identifiers Rule*. Only the National Provider Identifier (NPI) identifies covered entities in the standard transactions to protect the patient identity information.
- *Enforcement Rule*. Investigation and penalties for violating HIPAA rules.

There is another common framework for audit trails for EHRs, called ISO 27789, to keep personal health information auditable across systems and domains. Secure audit record must be created each time any operation is triggered via the system complying with ISO 27789. Hence, we posit the importance of a collaborative and transparent data sharing system, which also facilitates audit and post-incident investigation or forensics in the event of an alleged misconduct (e.g. data leakage). Such a notion (forensic-by-design) is also emphasized by forensic researchers (Grispos et al., 2017; Rahman et al., 2016).

As a regulatory response to security concerns about managing the distribution, storage and retrieval of health record by medical industry, Title 21 CFR Part 11 places requirements on medical systems, including measures such as document encryption and the use of digital signature standards to ensure the authenticity, integrity and confidentiality of record.

We summarize the following requirements that should be met based on these relevant standards above when implementing the next generation secure EHR systems:

- Accuracy and integrity of data (e.g. any unauthorized modification of data is not allowed, and can be detected);
- Security and privacy of data;
- Efficient data sharing mechanism (e.g. Dai et al. (2020));
- Mechanism to return the control of EHRs back to the patients (e.g. patients can monitor their record and receive notification for loss or unauthorized acquisition);
- Audit and accountability of data (e.g. forensic-by-design (Grispos et al., 2017; Rahman et al., 2016)).

The above properties can be achieved using blockchain, as explained below:

- *Decentralization*. Compared with the centralized mode, blockchain no longer needs to rely on the semi-trusted third party.
- *Security*. It is resilient to single point of failure and insider attacks in the blockchain-based decentralized system.
- *Pseudonymity*. Each node is bound with a public pseudonymous address to protect its real identity.
- *Immutability*. It is computationally hard to delete or modify any record of any block included in the blockchain by one-way cryptographic hash function.
- *Autonomy*. Patients hold the rights of their own data and share their data flexibly by the settings of special items in the smart contract.
- *Incentive mechanism*. Incentive mechanism of blockchain can stimulate the cooperation and sharing of competitive institutions to promote the development of medical services and research.
- *Auditability*. It is easy to keep trace of any operation since any historical transaction is recorded in the blockchain.

Hence, if blockchain is applied correctly in the EHR systems, it can help to ensure the security of EHR systems, enhance the integrity and privacy of data, encourage organizations and individuals to share data, and facilitate both audit and accountability.

3. Blockchain-based EHR systems

Based on the requirements of a new version of secure EHR systems and the characteristics of blockchain discussed in the preceding Section 2.3, we will now describe the key goals in the implementation of secure blockchain-based EHR systems as follows:

- *Privacy*: individual data will be used privately and only authorized parties can access the requested data.
- *Security*: in the sense of confidentiality, integrity and availability (CIA):
  1. *Confidentiality*: only authorized users can access the data.
  2. *Integrity*: data must be accurate in transit and not be altered by unauthorized entity(ies).
  3. *Availability*: legitimate user's access to information and resources is not improperly denied.
- *Auditability*: an important component of security. For example, audit logs mainly include information on who access which the EHR (or a specific PHR), with what aim, and the time-stamping of any operation in the entire life cycle (Ahsan et al., 2020).
- *Accountability*: an individual or an organization will be audited and be responsible for misbehavior.
- *Authenticity*: capability to validate the identities of requestors before allowing access to sensitive data.
- *Anonymity*: entities have no visible identifier for privacy. Complete anonymity is challenging, and pseudo-anonymity is more common (i.e. users are identified by something other than their actual identities).

In order to satisfy the above goals, existing blockchain-based research in the healthcare domain includes the following main aspects:

- *Data storage*. Blockchain serves as a trusted ledger database to store a broad range of private healthcare data. Data privacy should be guaranteed when secure storage is achieved. However, healthcare data volume tends to be large and complex in practice. Hence, a corresponding challenge is how to deal with big data storage without having an adverse impact on the performance of blockchain network.
- *Data sharing*. In most existing healthcare systems, service providers usually maintain primary stewardship of data. With the notion of self-sovereignty, it is a trend to return the ownership of healthcare data back to the user who is capable of sharing (or not sharing) his personal data at will. It is also necessary to achieve secure data sharing across different organizations and domains.
- *Data audit*. Audit logs can serve as proofs to hold requestors accountable for their interactions with EHRs when disputes arise. Some systems utilize blockchain and smart contract to keep trace for auditability purpose. Any operation or request will be recorded in the blockchain ledger, and can be retrieved at any time.
- *Identity manager*. The legitimacy of each user's identity needs to be guaranteed in the system. In other words, only legitimate users can make the relevant requests to ensure system security and avoid malicious attacks.

In the remaining of this section, we will review existing approaches to achieve data storage, data sharing, data audit, and identity manager (see Sections 3.1 to 3.4).

3.1. Data storage

3.1.1. How to achieve secure data storage

According to Section 2.3, one of the solutions to ensure greater security in the EHR system is the use of blockchain technology. However, there are potential privacy problems for all of raw/encrypted data in the public ledger, since blockchain as a public database has the risk of sensitive data being exposed under the statistical attack.

Some measures should be taken to enhance the privacy protection of sensitive health record in the blockchain-based EHR systems. In generally, privacy preserving approaches can be classified into cryptographic and non-cryptographic approaches, including encryption, anonymisation and access control mechanism respectively.

Encryption scheme is a relatively common method, such as public key encryption (PKE), symmetric key encryption (SKE), secure multi-party computation (MPC) (Zyskind et al., 2015) and so on.

Al Omar et al. (2017) proposed a healthcare platform based on blockchain, called MediBchain, in which public key encryption technique (i.e. Elliptic Curve Cryptography (ECC)) is used to encrypt private data through a secured channel. Similarly, Lee and Yang (2018) proposed that sensors data will be uploaded using a pair of unique private and public keys in the blockchain network to protect the privacy and security of biometric information.

Zheng et al. (2018) proposed that data will be encrypted before being uploaded to cloud servers by symmetric key scheme (i.e. Rijndael AES (Daemen and Rijmen, 2002)) with threshold encryption scheme. The symmetric key will be split into multiple shares distributed among different key keepers by Shamir's secret sharing scheme (Vanstone et al., 1997). Only if data requestor gets enough key shares, he can decrypt the ciphertext. Compromising of some key keepers(less than threshold) would not lead to data leakage.

Yue et al. (2016) designed an App on smartphones based on blockchain with MPC technique, called Healthcare Data Gateway (HDG). The system allows to run computations of encrypted data directly on the private blockchain cloud and obtain the final results without revealing the raw data.

Besides, Guo et al. (2018) proposed an attribute-based signature scheme with multiple authorities (MA-ABS) in the healthcare blockchain. The signature of this scheme attests not to the identity of the patient who endorses a message, instead to a claim (like access policy) regarding the attributes delegated from some authorities he possesses. Meanwhile, the system has the ability to resist collusion attack by sharing the secret pseudorandom function (PRF) seeds among authorities.

In order to resist malicious attacks (e.g. statistical attack), healthcare systems have to change the encryption keys frequently of general methods. It will bring the cost for storage and management of a large amount of historical keys since these historical keys must be stored well to decrypt some historical data in future, then the storage cost will be greater, especially for limited computational resource and storage devices.

To address this problem, Zhao et al. (2017) designed a lightweight backup and efficient recovery key management scheme for body senor networks (BSNs) to protect the privacy of sensor data from human body and greatly reduce the storage cost of secret keys. Fuzzy vault technology is applied for the generation, backup and recovery of keys without storing any encryption key, and the recovery of the key is executed by BSNs. The adversary hardly decrypts sensor data without symmetric key since sensor data is encrypted by symmetric encryption technology (i.e. AES or 3DES).

We compare and analyse some systems above, shown in Table 1 and 2. Most systems use cryptographic technology to en-

Table 1
main contributions and limitations of blockchain-based EHR systems for secure data storage.

paper	main technologies	main contributions	limitations
Al Omar et al. (2017)	PKE(ECC)	1. keep sensitive healthcare data accountability and integrity 2. cryptographic functions can protect patient's data 3. return the control right of private data back to patients 4. use the pseudonymity can protect the real identity of the patient	1. high-cost PKE computation 2. complex key management 3. the risk of ID/PWD(password of users) and data leakage
Lee and Yang (2018)	PKE	1. the information of nail images can be used for identity management and help do further research of health and disease 2. use SVM and random forest tree algorithm for fast and accurate biometric authentication 3. protect the privacy and integrity of sensitive data using blockchain	1. bottlenecks may appear in the resource-limited IoT devices 2. the risk of nail image data leakage in the public blockchain ledger
Zheng et al. (2018)	SKE(AES)	1. the quality of data from wearable devices can be improved using machine learning techniques 2. an off-chain storage database is used for large size datasets 3. the Shamir's secret sharing technique is used to enhance the security and privacy of data 4. users hold the control right of their personal health data and can share it securely	1. data leakage on purpose or accidentally by customers who have decrypted the requested data
Yue et al. (2016)	MPC	1. healthcare data is stored in the private blockchain cloud against confidentiality and integrity attacks 2. it is flexible and easy to integrate healthcare data using simple Indicator-centric schema as storage model 3. MPC can be used to conduct computation on encrypted data among untrusted entities without data leakage 4. it enables patients to manage their own data securely through their data gateways	1. high-cost MPC computation 2. replicas of data to requestors may cause the tamper or leakage of data without the owner's permission
Guo et al. (2018)	MA-ABS	1. no identity or attributes of the patient for explicit claim of the signature for privacy preserving 2. make the verifier unforgeability 3. resist collusion attack	1. high-cost computation 2. not support general nonmonotone predicates
Liu et al. (2018)	SKE&CES	1. allow patients to selectively share the signed medical data by their willings 2. use different public keys for different transactions to protect user's real identity 3. anonymous and voluntary patients' transaction 4. malicious requestors can be tracked	1. have a direct effect on transaction processing since it takes a long time to create a new block
Zhao et al. (2017)	SKE (AES/3DES)	1. greatly reduce the storage cost for encryption keys in the blockchain 2. greatly enhance the privacy of physiological data in the block using distinguished keys 3. the adversary has little chance to decrypt ciphertexts without corresponding symmetric keys	1. the risk of data leakage in the public ledger 2. all of data will be exposed once the corresponding symmetric key is lost

Table 2
systems requirements that have been met in Table 1.

paper	security	privacy	anonymity	integrity	authentication	controllability	auditability	accountability
Al Omar et al. (2017)	✓	✓	✓	✓	✓	✓	✓	✓
Lee and Yang (2018)	✓	✓	✓	✓	✓		✓	
Zheng et al. (2018)	✓	✓	✓	✓	✓	✓		
Yue et al. (2016)	✓	✓	✓	✓		✓	✓	
Guo et al. (2018)	✓	✓	✓	✓	✓		✓	✓
Liu et al. (2018)	✓	✓	✓	✓	✓	✓	✓	✓
Zhao et al. (2017)	✓	✓	✓	✓		✓		

hance the security and privacy of healthcare data in the blockchain. However, encryption technique is not absolutely secure. The computational cost of encryption is high for some limited devices. Transaction record may also reveal user behaviors and identity because of the fixed account address. Malicious attackers may break the ciphertext stored in the public ledger by some means.

Meanwhile, another important issue is key management. It is the foundation of entire data field safety that private keys do not reveal. The loss of private key means that the holder would have no ability to control the corresponding data. Once the private/symmetric key is compromised, all of data may be exposed by attackers. So, both encryption technique and key management

should be considered when developers design a secure EHR system.

Additionally, it must guarantee that only authorized legitimate users can access private data to enhance security. Non-cryptographic approaches mainly use access control mechanism for security and preserving privacy. With regard to the security goals, access control mechanism is a kind of security technique that performs identification authentication and authorization for entities. It is a tool widely used in the secure data sharing with minimal risk of data leakage. We will discuss this mechanism in details in the next Section 3.2.2.

3.1.2. How to store large healthcare data

The EHR systems can upload medical record and other information in the blockchain. If these data is stored directly in the blockchain network, it will increase computational overhead and storage burden due to the fixed and limited block size. What's more, these data would also suffer from privacy leakage.

To solve these problems, most relevant research and applications (Azaria et al., 2016a; Juneja and Marefat, 2018; Liu et al., 2018; Zheng et al., 2018) apply the architecture in which off-chain storage is mainly to store large volumes of encrypted original data using trusted third parties (e.g. cloud computing), and blockchain for on-chain verification only stores some metadata and pointers/indexes (i.e. off-chain database location) of the corresponding raw data. It can reduce the storage burden of blockchain and ensure the integrity and privacy of private data. Moreover, users can leave and rejoin the system at any time, then get access to their historical record according to the index downloaded from the latest block in the blockchain.

Zheng et al. (2018) applied cloud storage for encrypted continuous-dynamic data from wearable devices for a specific period time with high frequency. Health data can be purchased for machine learning by sending transaction to the blockchain. Only if data buyer is authorized and gets enough key shares, data can be decrypted from cloud storages.

Juneja and Marefat (2018) proposed an architecture that uses an external storage to eliminate the storage constraint of blockchain and provides accurate rollbacks when false alarm rate raises. Similarly, Azaria et al. (2016a) utilized off-line databases as cache storage of medical data with database gatekeeper. Gatekeeper can return the query result if the request is granted permissions.

Liu et al. (2018) designed a system in which healthcare data is stored in the cloud using CP-ABE-based access control (CCAC) for secure storage. Data requestors can retrieve the data containing related extraction signature in the cloud to verify the validity and integrity of requested data.

Sun et al. (2018) designed a system in which the raw SignedEHR is signed using healthcare providers' attribute-based signature and stored in a trusted third-party database to protect the security and privacy of data. The ProposalRecord request mainly including the corresponding address of the SignedEHR must be signed by doctors using decentralizing attribute-based signature (DABS) and sent to the blockchain network. When any user wants to get access to the data, the signature of his request needs to be verified first and can be valid only if the signature matches specific attributes.

Healthcare data has many kinds of forms, such as records, text, images, etc. Since blockchain is not appropriate to provide high capacity data storage due to its limited block size, it is necessary to consider how to store large volumes of data in the healthcare systems.

Kamauu et al. (2009) proposed that each imaging study is identified by its unique digital imaging and communication in medicine (DICOM) UIDs using improved JAVA UID class. These DICOM UIDs can be applied to blockchain with continued use of existing imaging infrastructures for off-chain raw image data storage to prevent the leakage of protected health information (PHI).

Patel (2018) developed a framework for cross-domain medical image sharing system, in which patients delegate electronic access to their medical imaging data in a secure manner. There is a list of the requestors who are permitted to access authorized study referenced by its unique DICOM UID, and any raw medical image is not stored in the blockchain.

Yue et al. (2016) proposed that a simple unified Indicator Centric Schema (ICS) could organize all kinds of personal healthcare data easily in one simple "table". In this system, data is uploaded once and retrieved many times. They designed multi-level index and multi-dimensional (LD-Index), as illustrated in Fig. 4.

Data can be indexed by hash-index of category and time. For each category generated by B+ tree, data can be traversed until the leaf node. ICS achieves cell granularity of data storage to integrate shared healthcare data easily.

Most systems in the previous sections are adopted third-party database architecture. The third-party services (such as cloud computing) in the far-end assist the users to improve Quality of Service (QoS) of the applications by providing data storage and computation power, but with a transmission latency.

Such a storage system has gained common acceptance depending on a trusted third party with strong storage capacity and high-performance computing. However, it has the risk of single point of failure relying on third-party services. Meanwhile, some curious cloud servers may collect sensitive patient data without consent.

A decentralized peer-to-peer file system InterPlanetary File System (IPFS) can be an improved solution with advantages, such as no single point of failure, high storage throughput and faster data retrieval, while data hash values produced by file content are recorded in the Distributed Hash Table (DHT).

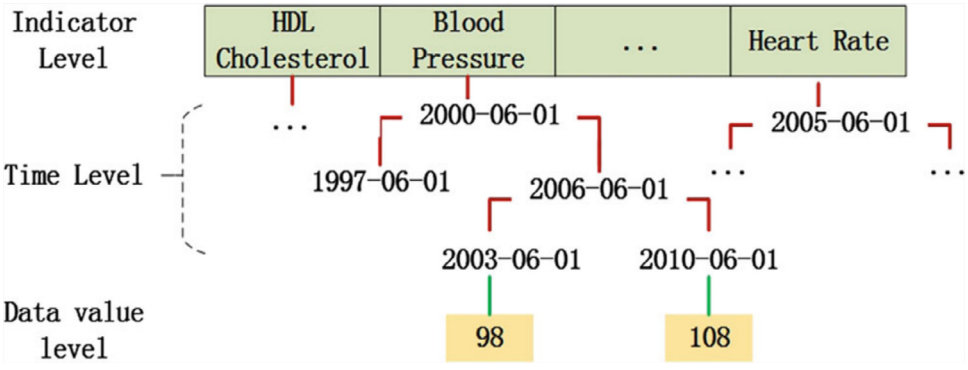

Fig. 4. Illustration of LD-index (Yue et al., 2016).

Table 3
main contributions and limitations of blockchain-based EHR systems for data storage.

paper	main technologies	main contributions	limitations
Sun et al. (2018)	off-chain database	1. secure data sharing across different Care Delivery Organizations (CDOs) 2. make it easier for users to locate EHR data 3. avoid the storage limitation of the blocks 4. secure large-scale distributed EHR data sharing using on-chain and off-chain storage model	1. it is hard to build fully-trusted third parties to store EHR data 2. the owner of data has no control right
Patel (2018)	off-chain database	1. only a list of authorized requestors in the block for better privacy protection 2. data access is valid with patient's consent 3. unique DICOM UIDs can identify image studies	1. rely on the existing imaging centers that may be curious with the risk of malicious attacks
Zheng et al. (2018)	cloud storage	1. reduce storage burden of blockchain for gigabytes continuous-dynamic data with high frequency	1. it is hard to establish fully-trusted third cloud storage platforms 2. it can not protect data privacy since data buyers will get sensitive data in the plaintext forms
Liu et al. (2018)	cloud storage	1. greatly reduce storage burden of blockchain and the risk of data leakage 2. data access is restricted on the cloud 3. cloud storages perform access data action only if the request signature is valid	1. it is not easy to build fully-trusted third parties 2. it may not resist collusion attack from cloud servers and requestors
Juneja and Marefat (2018)	cloud storage	1. patients hold the control right of their data 2. securely store rollback data to increase the accuracy for arrhythmia classfication 3. make the process of retraining SDA faster using blockchain for data location	1. have the risk of malicious attacks and data tamper
Azaria et al. (2016a)	off-chain databases	1. facilitate both continued use and interoperablility of existing healthcare infrastructures through generic interfaces 2. off-chain access action is governed and recorded by smart contact 3. missing data can be retrieved from distributed replica nodes	1. it can not stop existing databases from collecting private data without consent 2. it does not solve the security problem of single database
Nguyen et al. (2019)	IPFS	1. no single point of failure 2. high storage throughput 3. data retrieval improvement with distributed hash table(DTH)	1. the risk of personal information leakage due to curious miners
Rifi et al. (2017)	IPFS	1. IPFS as off-chain databases can store large amounts of sensor personal data 2. healthcare providers can access sensor data in the IPFS only with the permissions granted by patients	1. lack of privacy protection for personal health data
Wang et al. (2018)	IPFS	1. no longer rely on the third centralized servers 2. no single point of failure 3. higher data throughput and lower prices than traditional cloud storages 4. it cannot obtain any information of files 5. download the encrypted file honestly by smart contract	1. IPFS does not provide a strong privacy cryptographic algorithm interface for user-uploaded files

Nguyen et al. (2019) designed a system that integrates smart contract with IPFS to improve decentralized cloud storage and controlled data sharing for better user access management. Rifi et al. (2017) also adopted IPFS as the candidate for off-chain database to store large amounts of sensor personal data.

Wang et al. (2018) designed a system that utilizes IPFS to store the encrypted file. The encryption key of the file is first encrypted using ABE algorithm, then encrypted with other information (file location hash ciphertext) using AES algorithm. Only when the attributes set of the requestor meets the access policy predefined by data owner, the requestor can obtain the clue from blockchain, then download and decrypt the files from IPFS.

According to Table 3 and 4, the common architecture for data storage in the EHR system is shown in Fig. 5. The advantages of integrating off-line storage into blockchain systems are as follows. First, detailed medical record is not allowed to access directly for patient's data privacy preserving. Second, it helps to reduce the throughput requirement significantly, since only transaction record and a few metadata are stored in the blockchain. Besides, data pointers stored in the block can be linked to the location of raw data in the off-chain database for data integrity.

However, it is difficult to fully trust the third parties to store these sensitive data. Meanwhile, it may also contradict the idea of decentralization. Further research is needed to accelerate the acceptance of distributed storage systems in practice, like IPFS. Also, the next step should be to improve the storage architecture of blockchain for high storage capacity.

3.2. Data sharing

Healthcare industry relies on multiple sources of information recorded in different systems, such as hospitals, clinics, laboratories and so on. Healthcare data should be stored, retrieved and manipulated by different healthcare providers for medical purposes. However, such a sharing approach of medical data is challenging due to heterogeneous data structures among different organiza-

Table 4
systems requirements that have been met in Table 3.

paper	security	privacy	anonymity	integrity	authentication	controllability	auditability	accountability
Azaria et al. (2016a)	✓	✓	✓	✓	✓	✓	✓	✓
Patel (2018)	✓	✓	✓	✓	✓	✓	✓	✓
Liu et al. (2018)	✓	✓	✓	✓	✓	✓	✓	✓
Sun et al. (2018)	✓	✓	✓	✓	✓			
Zheng et al. (2018)	✓	✓	✓	✓	✓	✓	✓	✓
Juneja and Marefat (2018)	✓	✓	✓	✓	✓	✓		
Nguyen et al. (2019)	✓	✓	✓	✓	✓	✓	✓	✓
Rifi et al. (2017)	✓	✓	✓	✓		✓		
Wang et al. (2018)	✓	✓	✓	✓	✓	✓		

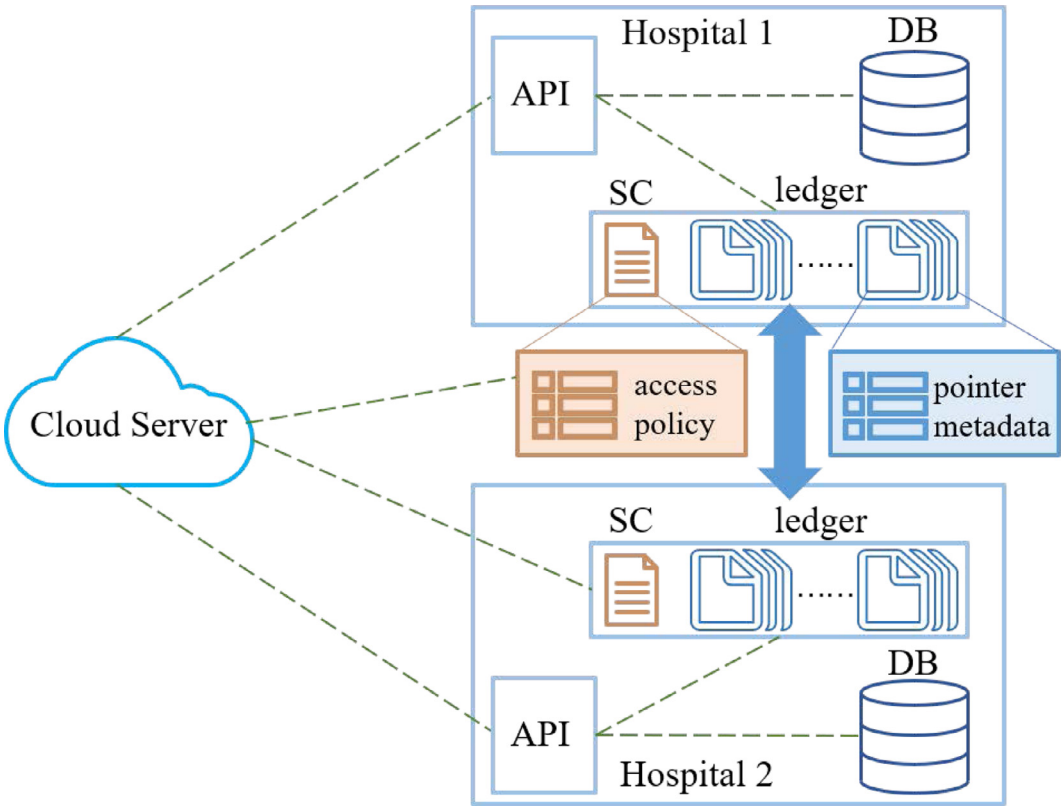

Fig. 5. common architecture for data storage in the EHR system.

tions. It is necessary to consider interoperability of data among different organizations before sharing data. We will introduce interoperability first.

3.2.1. Interoperability

Interoperability of EHR is the degree to which EHR is understood and used by multiple different providers as they read each other's data. Interoperability can be used to standardize and optimize the quality of health care. Interoperability can mainly be classified into three levels:

- *Syntactic interoperability*: One EHR system can communicate with another system through compatible formats.
- *Semantic interoperability*: Data can be exchanged and accurately interpreted at the data field level between different systems.
- *Cross-domain interoperability*: Multiple organizations work together to facilitate secure and timely communication and efficient use of data between organizations and individuals.

The lack of unified interoperability standards has been a major barrier in the high-performance data sharing between different entities. According to the study (Begoyan (2007)), there are different EHR standards adopted by different institutions and countries, such as the Health Level Seven International (HL7), European Committee for Standardisation (CEN) and Digital Imaging and Communications in Medicine (DICOM).

In some studies (Azaria et al., 2016b; Kim et al., 2018; Peterson et al., 2016), they adopted the Health Level Seven International (FHIR) as data specification and standard formats for data exchange between different organizations. The criterion was created by HL7 healthcare standards organization.

The system in Peterson et al. (2016) references FHIR resources via Uniform Resource Locators (URLs) stored in the blockchain, which keeps sensitive data out of the blockchain at the same time. Besides, they proposed Proof of Interoperability (POI) based on conformance to the FHIR protocol. Miners must verify incoming messages to ensure that these messages meet the known structural and semantic standards. This mechanism avoids some disadvantages of Proof of Work (PoW) and enhances the interoperability.

Kim et al. (2018) introduced medical questionnaire management system, in which data can be interoperable with other systems based on HL7 FHIR. First, patient data is generated into the

FHIR questionnaire resource format. After the parse and the validation of data format, hospital information system stores personal information in the internal databases. Only the questionnaire result data is stored in the blockchain for next questionnaire result data sharing.

Peng et al. (2018) designed a blockchain-based healthcare architecture called FHIRChain to meet Office of the National Coordinator (ONC) for health information technology requirements by encapsulating the HL7 FHIR for clinical data sharing, which can be compatible with many software libraries and some existing blockchain systems.

Despite much interest in using blockchain for healthcare interoperability, a little information is available on the concrete architectural patterns for applying blockchain to healthcare Apps. Zhang et al. (2017) filled this gap and showed how modularized software patterns are applied to address the interoperability challenges of blockchain-based healthcare Apps.

Bahga and Madisetti (2013) proposed that cloud health information systems technology architecture (CHISTAR) achieves semantic interoperability, defines a general purpose set of data structures and attributes and allows to aggregate healthcare data from disparate data sources. Besides, it can support security features and address the key requirements of HIPAA.

Hsieh and Chen (2012) designed a secure interoperable cloud-based EHR service with Continuity of Care Document (CCD). They provided self-protecting security for health documents with support for embedding and user-friendly control.

In a word, interoperability is the basic ability for different information systems to communicate, exchange and use data in the healthcare context. EHR systems following international standards can achieve interoperability and support for data sharing between multiple healthcare providers and organizations. We will discuss data sharing in detail next.

3.2.2. Access control mechanism with smart contract for data sharing

It is obviously inconvenient and inefficient to transfer paper medical record between different hospitals by patients themselves.Sharing healthcare data is considered to be a critical approach to improve the quality of healthcare service and reduce medical costs.

Though current EHR systems bring much convenience, many obstacles still exist in the healthcare information systems in practice, hinder secure and scalable data sharing across multiple organizations and thus limit the development of medical decision-making and research.

As mentioned above, there are risks of the single-point attack and data leakage in a centralized system. Besides, patients cannot preserve the ownership of their own private data to share with someone who they trust. It may result in unauthorized use of private data by curious organizations. Furthermore, different competing organizations lacking of trust partnerships are not willing to share data, which would also hinder the development of data sharing.

In this case, it is necessary to ensure security and privacy-protection and return the control right of data back to users in order to encourage data sharing. It is relatively simply to deal with security and privacy issues when data resides in a single organisation, but it will be challenging in the case of secure health information exchange across different domains. Meanwhile, it also needs to consider further how to encourage efficient collaboration in the medical industry.

Secure access control mechanism as one of common approaches requires that only authorized entities can access sharing data. This mechanism includes access policy commonly consisting of access control list (ACL) associated with data owner. ACL is a list of requestors who can access data, and related permissions (read, write, update) to specific data.

Authorization is a function of granting permission to authenticated users in order to access the protected resources following predefined access policies. The authentication process always comes before the authorization process.

Access policies of this mechanism mainly focus on who is performing which action on what data object for which purposes. Traditional access control approaches for EHRs sharing are deployed, managed and run by third parties. Users always assume that third parties (e.g. cloud servers) perform authentication and access requests on data usage honestly. However, in fact, the server is honest but curious.

It is promising that combining blockchain with access control mechanism is to build a trustworthy system. Users can realize secure self-management of their own data and keep shared data private. In this new model, patients can predefine access permissions (authorize, refuse, revoke), operation (read, write, update, delete) and duration to share their data by smart contracts on the blockchain without the loss of control right.

Smart contracts can be triggered on the blockchain once all of preconditions are met and can provide audit mechanism for any request recorded in the ledger as well. There are many existing studies and applications applying smart contract for secure healthcare data sharing.

Peterson et al. (2016) proposed that patients can authorize access to their record only under predefined conditions (research of a certain type, and for a given time range). Smart contract placed directly on the blockchain verifies whether data requestors meet these conditions to access the specified data. If the requestor does not have the access rights, the system will abort the session. Similarly, smart contracts in Dan et al., (2016) can be used for granting and revocation of access right and notifying the updated information as providers move in and out of networks.

Azaria et al. (2016a) designed a decentralized record management system based on blockchain, called MedRec. In this system, Patient-Provider Relationship Contract is deployed between any two nodes in which patients manage and share medical records with healthcare providers. Providers can add or modify these record in the case of patient's permissions. Data access record is preserved in the block to track the malicious entities when violated access activities happen. They also designed a simple graphical interface tool that allows patients to share off-chain data with fine-grained access control. The similar design is proposed in Rifi et al. (2017).

Nguyen et al. (2019) developed an access protocol based on smart contract through admin component when mobile users send the request. Smart contract will verify any transaction by predefined policies of access protocol to prevent malicious attack and achieve reliable EHRs sharing. But curious miners may infer personal information during the mining process due to the processing transactions including Area ID, mobile gateway ID and patient ID.

Liang et al. (2017) creatively adopted the channel scheme of Hyperledger Fabric, which separates different types of activities for users in the different channels to share different grained data. Chaincode (smart contract) can be launched in the channel with different access type, permissioned operations and selective shared data specified in the certificate by data owners. In addition to data sharing, such a channel scheme make good use of Fabric to enhance data privacy.

Most policies of access control above are set for who can perform which authorized operations on which part of data. The diverse forms of policies are used in different scenarios, such as based on roles, purposes, attributes and so on. Most systems mentioned above belong to role-based access control (RBAC) schemes.

Yue et al. (2016) designed a blockchain-based App architecture on smart-phone or PC called Healthcare Data Gateway (HDG). They proposed a purpose-centric access control model, which is divided into two types based on access purposes: raw data (healthcare service) and statistical data (medical research). In the whole workflow, any transaction is processed with different sharing strategies for different purposes. This scheme allows patients to manage and monitor their sharing healthcare data easily.

Smart contract in most systems includes predefined access policies depending on requestors' role/purposes and based-role/based-purpose privileges. However, it is inflexible to handle unplanned or dynamic events and may lead to potential security threats (Fernández-Alemán et al., 2013b). Another mechanism, Attribute-Based Access Control (ABAC), has been applied in the secure systems to handle remaining issues in the extensions of RBAC and enhance the security in some specific cases.

The system based on ABAC extends role-based features to attributes and defines different policies for different attributes sets of access requests. These attributes mainly describe the properties of subjects, resources, environment and so on. Only if the attributes set of the requestor meets predefined access policies, he can get access to sharing data (Dias et al., 2018).

Maesa et al., (2018) proposed a blockchain-based attribute-based access control scheme according to the XACML standard for the compatibility of smart contracts. They describes how to create and translate access policies in details. Their solution makes sure that legitimate requestors can be correctly evaluated while malicious or faulty entities would be refused to access any resource.

Pussewalage and Oleshchuk, (2018) proposed a delegable attribute-based access control based on blockchain to manage the operations of permission and reduce key management overhead by attribute revocation mechanism. They designed a maximum permissible length chain of delegations that consists of delegatee and his further delegation to provide flexible relegatable access with lower computational overhead of revocation operation.

In addition to ACL, access control matrix is another structure, of which each row represents a subject, each column an object and each corresponding entry is access rights set.

Dias et al., (2018) adopted a similar access control matrix integrated with consortium blockchain to solve access control management among different entities. In the case of multiple entities owned healthcare data, blockchain is used to store transaction about access policies to overcome the complexity.

The systems based on access control mechanism record any operation about access policies by logging. However, it is vulnerable to malicious tampering without the assurance of integrity of these logs in the traditional systems. Blockchain and smart contract can perform access authorization automatically in a secure container and make sure the integrity of policies and operations. Thus, access control mechanism integrated with blockchain can provide secure data sharing.

The diversified forms of access control can be applied into different situations depending on the demands for system security. Audit-based access control aims to enhance the reliability of posteriori verification (Morelli et al., 2019). Organization-based access control (OrBAC) (Kalam et al., 2003) can be expressed dynamically based on hierarchical structure, including organization, role, activity, view and context.

Based on the information in the Table 5 and 6, most policies are static in the healthcare systems, in which the owner or the security officer writes access control rules in a static manner. It may have the potential risk of conflicts. In the context of IoT, it is difficult to manage the security policies for large amounts of smart devices. Hence, it is necessary to propose one dynamic and self-adjusted access control policy to face complex and unpredicted environment using machine learning Outchakoucht et al. (2017).

3.2.3. Cryptography technology for data sharing

We can also use cryptography technology to enhance secure data sharing and the security of access control mechanism in most EHR systems.

Dubovitskaya et al. (2017) proposed a framework to manage and share EMRs for cancer patient care based on symmetric encryption. Patients can generate symmetric encryption keys to encrypt/decrypt the sharing data with doctors. If the symmetric key is compromised, proxy re-encryption algorithm on the data stored in the trusty cloud can be performed and then a new key will be shared with clinicians according to predefined access policies. Only the patients can share symmetric keys and set up the access policies by smart contract to enhance the security of sharing data.

Xia et al. (2017) designed a system that allows users to get access to requested data from a shared sensitive data repository after both their identities and issuing keys are verified. In this system, User-Issuer Protocol is designed to create membership verification key and transaction key. User-Verifier Protocol is used for membership verification, then only valid users can send data request to the system.

Ramani et al. (2018) utilized lightweight public key cryptographic operations to enhance the security of permissioned requests (append, retrieve). Nobody can change the patients' data without sending a notification to patients, since the requested transaction will be checked whether it has signed by the patient before being stored on a private blockchain.

Wang et al. (2018) designed a system that combines Ethereum with attribute-based encryption (ABE) technology to achieve fine-grained access control over data in the decentralized storage system without trusted private key generator (PKG). The encryption key of the file is stored on the blockchain in the encrypted format using AES algorithm. Requestors whose attributes meet the access policies can decrypt the file encryption key and then download the encrypted file from IPFS. Besides, the keyword search implemented by smart contract can avoid dishonest behavior of cloud servers.

Zhang et al. (2016) designed a protocol to share healthcare data among pervasive social network (PSN) nodes. The healthcare data is generated by the wireless body area network (WBAN). Through the addresses of sensors and mobile devices stored in the blockchain, PSN nodes can establish secure links for the WBAN by improved version of the IEEE 802.15.6 display authenticated association and then get access to sharing data from other nodes if the verification succeeds, which does not bring heavy storage load to PSN nodes or high computational load on the sensors. In addition, it avoids data leakage from illegal behavior since all of data is stored in the smart devices and body sensors.

Liu et al. (2018) proposed blockchain-based privacy-preserving data sharing scheme for EMR called BPDS. The system adopted content extraction signature (CES) Steinfeld et al. (2001) which can remove sensitive information of EMRs, support for selective sharing data and generate valid extraction signatures to reduce the risk of data privacy leakage and help enhance the security of access control policies. Besides, users can use different public keys for different transactions to keep anonymous.

Hui et al. (0000) designed a blockchain-based data sharing scheme in the cloud computing environment to solve the trust issue among different groups using group signature and ensure the reliability of the data from other organizations. Requestors can verify the integrity of shared data from the immutable ledger record. When a dispute emerges, the real identity of the data owner can be traced by the agencies who manage all the group members in the group signature. It is provable that data sharing with traceability can enhance the trust relationship among different organizations.

Table 5
Main contributions and limitations of blockchain-based EHR systems for data sharing.

paper	main technologies	main contributions	limitations
Peterson et al. (2016)	smart contract RBAC	1. design a new consensus algorithm Proof of Interoperability to facilitate data interoperability 2. effective data sharing networks require consensus on data syntax, meaning, and security	1. this consensus may not be reached programmatically
Dan et al. (2016)	smart contract RBAC	1. smart contract is used to automatically verify access permissions to minimize manual operation 2. efficient dissemination of any operation on record	1. potential real identity and personal information leakage
Azaria et al. (2016a)	smart contract RBAC	1. patients have fine-grained access control right of their medical record 2. provide auditable history of any request 3. incentivizing model drives the emergence of data economics	1. the security of individual databases has not addressed yet 2. the pseudonymous property of transactions may cause data leakage from frequency analysis
Rifi et al. (2017)	smart contract RBAC	1. combine the flexibility of smart contract with the security of blockchain for healthcare data access 2. the gateway is used to overcome the limited computational power of sensors 3. patients can completely hold the control right of their own data by smart contract	1. lack of privacy protection for healthcare data
Nguyen et al. (2019)	smart contract RBAC	1. flexible data exchanges on mobile clouds 2. lightweight access control design with minimum network latency 3. employ an asymmetric encryption algorithm to enhance the security	1. curious miners may infer private information during the mining process
Liang et al. (2017)	smart contract RBAC	1. user-centric health data sharing solution can make patients control their own information 2. make good use of channel formation scheme to preserver the privacy	1. it may not be good for keeping track with these record in the subledgers of different channels
Yue et al. (2016)	purpose-centric access control mechanism	1. purpose-centric access control model can process transactions with different sharing strategies 2. patients know who is accessing specified data with which authorized actions 3. secure multi-party computation is applied to conduct the process on encrypted data without the risk of patient privacy	1. high-cost MPC computation 2. replica of data to requestor may cause the tamper and leakage of data without the owner's permission
Maesa et al. (2018)	ABAC	1. design ABAC policies following XACML standard 2. map XACML architecture to smart contracts executed on the blockchain 3. guarantee the correctness and completeness of the system	1. auditability may bring some potential privacy problems
Pussewalage and Oleshchuk (2018)	relegatable ABAC	1. flexible access grant can be achieved across the domains 2. resistance against attribute forgery and attribute collusion 3. chain of delegations has lower overhead of revocation operation	1. pseudo-identities included in the public blocks may have the risk of personal information leakage 2. delegatee may be in collusion with his delegatee to obtain more information beyond the permission
Dias et al. (2018)	access control matrix	1. ensure the integrity of access policies lifecycle 2. define fine-grained permission at the user level and the resource level	1. potential data leakage of access policies stored in the blockchain
Dubovitskaya et al. (2017)	SKE smart contract	1. fine-grained access control policy 2. ensure privacy, security and integrity of encrypted data in the cloud	1. potential risk of earlier data leakage in case that the symmetric key is compromised
Xia et al. (2017)	cryptographic techniques	1. identity-based authentication can guarantee user anonymity 2. membership verification can achieve secure data sharing by issuing key 3. accountability is guaranteed since immutable logs of their operations are kept in the blockchain	1. communication and authentication protocols and algorithms between entities need further study 2. potential risk of personal identity leakage 3. it is difficult to fully trust the verification component
Ramani et al. (2018)	lightweight public key cryptography Schnorr signature scheme	1. the signature of patients including timestamp resist against reply attack 2. Schnorr signature scheme can resist against man-in-the-middle attack and impersonation attack 3. patients have access control right of their own data	1. public key encryption may have high computing cost
Wang et al. (2018)	ABE AES smart contract	1. data owners have the ability to distribute file keys for requestors and predefine access policies 2. avoid the problem of the key abuse without trusted PKG 3. search operations honestly by smart contract can avoid dishonest or wrong results of cloud servers	1. the scheme does not implement the functions of attribute revocation and access policy update

(*continued on next page*)

Table 5 (*continued*)

paper	main technologies	main contributions	limitations
Zhang et al. (2016)	improved IEEE 802.15.6 display authenticated association protocol	1. secure links for mobile devices and resource-limited sensor nodes are established to ensure secure data sharing 2. reduce computational load on the sensors 3. reduce the storage load of PSN nodes 4. avoid the dishonest behaviors of third parties 5. this protocol can be extended to other PSN-based applications	1. not fully utilize the benefits of the blockchain for this protocol
Liu et al. (2018)	smart contract ABE CES	1. achieve selective sharing data by content extraction signature scheme with low computational overhead 2. trace the malicious behaviours by immutable record in the blockchain 3. different public keys for different transactions can protect personal identity	1. users need to store and manage multiple key pairs
Hui et al. (0000)	group signature smart contract	1. group signature achieves anonymous information exchange to enhance the security and privacy of data among different groups 2. trace the real identity of malicious nodes in the process of solving a dispute	1. the complete privilege of tracking held by agencies may be abused
Seol et al. (2018)	partial encryption	1. flexible and fine-grained attributes-based access contol 2. XML encryption can provide selective encrypted data	1. user's identity may be exposed without de-identification mechanism

Table 6
systems requirements that have been met in Table 5.

paper	security	privacy	anonymity	integrity	authentication	controllability	auditability	accountability
Peterson et al. (2016)	✓	✓	✓	✓	✓		✓	✓
Dan et al. (2016)	✓	✓	✓	✓	✓	✓	✓	✓
Azaria et al. (2016a)	✓	✓	✓	✓	✓	✓	✓	✓
Rifi et al. (2017)	✓	✓	✓	✓		✓		
Nguyen et al. (2019)	✓	✓	✓	✓	✓	✓	✓	✓
Liang et al. (2017)	✓	✓	✓	✓	✓	✓	✓	✓
Yue et al. (2016)	✓	✓	✓	✓	✓	✓	✓	✓
Maesa et al. (2018)	✓	✓	✓	✓	✓	✓	✓	✓
Dias et al. (2018)	✓	✓	✓	✓	✓	✓	✓	✓
Dubovitskaya et al. (2017)	✓	✓	✓	✓	✓	✓		
Xia et al. (2017)	✓	✓	✓	✓	✓	✓	✓	✓
Ramani et al. (2018)	✓	✓	✓	✓	✓	✓		
Wang et al. (2018)	✓	✓	✓	✓	✓	✓		
Zhang et al. (2016)	✓	✓	✓	✓	✓		✓	✓
Liu et al. (2018)	✓	✓	✓	✓	✓	✓	✓	✓
Hui et al. (0000)	✓	✓	✓	✓	✓		✓	✓
Seol et al. (2018)	✓	✓	✓	✓	✓		✓	✓

Seol et al. (2018) proposed an EHR model that performs attribute-based access control built upon extensible access control markup language(XACML) that has the capability to define different policies for different contexts. Partial encryption is performed using XML encryption and digital signature is added using XML digital signature as auxiliary security measures in order to avoid the leakage of sensitive information after the access control step has been performed.

As shown in Table 5 and 6, cryptography technology can protect sensitive data directly and improve the traditional access control mechanism to meet the demand for security and privacy. However, public key encryption has high computational overhead and trusted PKI is necessary for authentication. The similar problem exists in a trusted PKG as one of important components of ABE. Besides, how to transmit the shared key securely should be addressed in the symmetric encryption. As mentioned before, MPC may not be suitable for wearable devices in the IoT context due to high computational cost. It is necessary to improve these algorithms to adapt devices/sensors with limited resource.

Above all, blockchain as a secure, immutable and decentralized framework makes the control right of data return to patients themselves in the healthcare industry. As shown in Fig. 6, The combination of access control mechanism by smart contract with cryptography technology on sensitive data can be achieved secure data sharing among different individuals and institutions. Meanwhile, all of record is included in the immutable public ledger to ensure the integrity and reliability of data and minimize the risk of raw data leakage.

Concerning potential dishonest behavior or wrong results of third parties (cloud servers) holding large amounts of raw/encrypted data, blockchain offers immutable historical record for traceability and accountability, sometimes with cryptography technique (such as group signature). Next we discuss about secure audit to enhance the security of EHR systems further.

3.3. Data audit

Healthcare systems also rely on audit log management as security mechanism since some exceptions may have resulted from the misuse of access privileges or dishonest behavior by third parties or data requestors. Audit log can serve as proofs when disputes arise to hold users accountable for their interactions with patient record. Immutable public ledger and smart contract in the

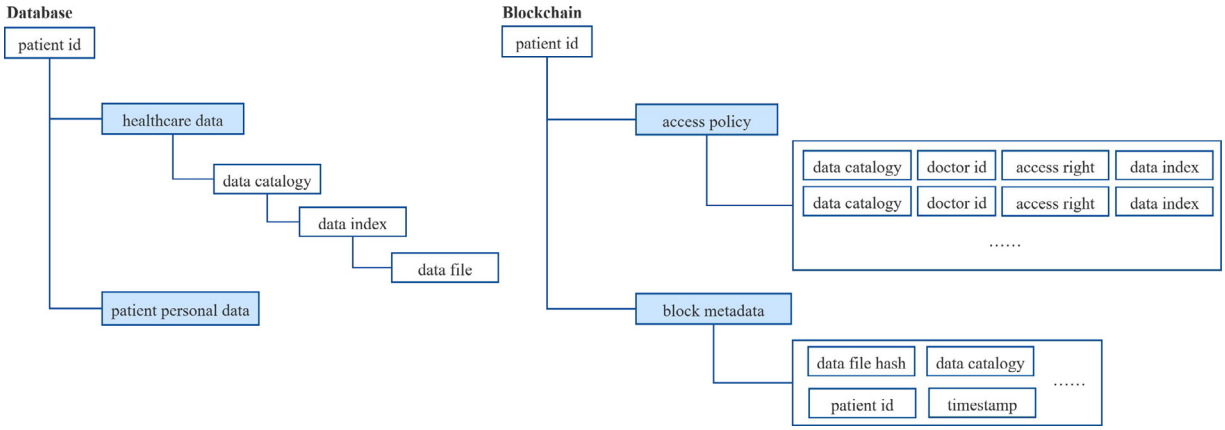

Fig. 6. patients' data stored in the database; access control policies in the smart contract and healthcare metadata in the block.

blockchain can provide immutable record for all of access requests to achieve traceability and accountability.

Audit log mainly contains vital and understandable information:

- timestamp of logged event
- user ID which requests the data
- data owner ID whose data is accessed
- action type (create, delete, query, update)
- the validation result of the request

Qi et al. (2017) designed a data sharing model with the ability to effectively track the dishonest behaviour of sharing data as well as revoke access right to violated permissions and malicious access. The system provides provenance, audit and medical data sharing among cloud service providers with minimal risk of data privacy.

The similar system in Xia et al. (2017) provides auditable and accountable access control for shared cloud repositories among big data entities in a trust-less environment. Azaria et al. (2016b) also provided auditability via comprehensive log. They mentioned that obfuscation for privacy needs further exploration while preserving auditability in the public ledger.

Fernández-Alemán et al. (2013c) designed a blockchain-based system called AuditChain to manage the logs generated by all of access operations. Smart contract in the AuditChain handles the creation, updating and querying of audit log data. It also facilitates the interoperability of audit log among different healthcare organizations by exposing the same data structure for each audit transaction.

When clinical trials, medical research and pharmaceutical data are error-prone, missing or manipulated, trust issue is intensive between patients and healthcare providers. The transparency and tamper-resistant of blockchain can keep trace of historical trial log and avoid storing selective good outcomes of clinical trials.

Smart contract in Nugent et al. (2016) acts as a trusted administrator to solve the data manipulation problem by immutable record of trial history in the blockchain, which can improve the transparency of trail reports and address trust issue of clinical trials.

To improve quality of research by better reproducibility, the timestamped statistical analysis on clinical trials ensures traceability and integrity of each sample's metadata in Benchoufi and Ravaud (2017) based on blockchain which allows to store proofs of existence of data. The related analytical code to process the data must be timestamped in order that data is checked and analysis is reproducible. Timestamp in the blockchain will provide for better version control than git.

The above-mentioned studies indicate that blockchain plays an important role in auditing and accountability. Users can not only hold the control right of their own data, but also monitor all request operations for data audit and accountability when disputes occur.

Above all, audit log provides reliable evidence for anomalous and potentially malicious behavior to improve the security of access control models. Meanwhile, it brings benefits to the adjustment of healthcare service by gaining insight into personnel interactions and workflows in hospitals.

Full patient metadata as audit log data would be expensive and time-consuming to store and process. Currently, audit log data does not contain required and representative information reliably, which would be difficult to interpret or hardly access. It would get worse in the collaboration of multiple EHR organizations. In this case, it is necessary to consider how to achieve interoperable and well-formatted audit log standard for the support of secure data exchange among different healthcare institutions.

3.4. Identity manager

Membership verification is the first step to ensure the security of any system before getting access to any resource. In the access control mechanism mentioned before, identity authentication is always first performed to make sure that specific rights are granted to data requestors with legal identity before sharing data.

Common types of user authentication have pass-through authentication, biometric authentication and identity verification based on public key cryptography algorithms. Public Key Infrastructure (PKI) is commonly used, which relies on trusted third parties to provide membership management services.

In the traditional EHR system, centralized master patient index (MPI) serves as the foundation of managing individual data to ensure identity integrity and accurately link the individual information.

Users mainly participate in the blockchain network by creating an account including a private key to sign any transaction and a public key for user identification. Then all of these entities are represented by the public portion of this asymmetric key pair. Data on the blockchain is associated with the address instead of a real identity.

Liang et al. (2017) achieved identity management by Hyperledger Fabric Membership Service Provider (MSP), which is responsible to issue enrollment certificates and transaction certificates for participating nodes. MSP is a powerful tool to support the identity authentication and authorization verification in Fabric using X.509 certifications based on traditional Public Key Infrastructure (PKI) model.

Al Omar et al. (2017) designed a registration module for identity management. When any party requests to the system at the first time, it will have to register for once before and need to preserve its ID and PWD for logging in and accessing through secured channel after authentication.

Identity registration is performed in Azaria et al. (2016a) with registrar smart contract to map valid string form of identity information to a unique Ethereum address via public key cryptography. It can employe a DNS-like implementation to allow the mapping of regulate existing forms of ID.

Zhang et al. (2016) established secure links for wireless body area network (WBAN) area and wireless body area network (PSN) area after authentication and key establishment through an improved IEEE 802.15.6 display authenticated association protocol Kuo et al. (2017). The protocol can protect collected data through Human body channels (HBCs) and reduce computational load on the sensors.

Xia et al. (2017) designed an efficient and secure identity-based authentication and key agreement protocol for membership authentication with anonymity in a permissioned blockchain. The process of verification is a challenge-response dialog to prove whether the sender is authentic when the verifier receives a verification request from a user using shared key.

Most blockchain-based systems use pseudonyms to hide the real identity for privacy. However, there is conflict between privacy preserving and authenticity. That means how to verify the identity without exposing the information of real identity. In addition, adversaries or curious third parties can guess the real identity and relevant behavior pattern through inference attacks, such as transaction graph analysis.

Shae and Tsai (2017) designed an anonymous identity authentication mechanism based on zero-knowledge technology Blum et al. (1988), which can address two conflicting requirements: maintain the identity anonymous and verify the legitimacy of user identity as well as IoT devices.

Sun et al. (2018) proposed a decentralizing attribute-based signature (called DABS) scheme to provide effective verification of signer's attributes without his identity information leakage. Multiple authorities can issue valid signature keys according to user's attributes rather than real identity and provide privacy-preserving verification service. Other nodes can verify whether the data owner is qualified by verification key corresponding to satisfied attributes without revealing owner identity.

Hardjono, (2019) designed an anonymous but verifiable identity scheme, called ChainAchor, using the EPID zero-knowledge proof scheme. These anonymous identities can achieve unlinkable transactions using different public key in the blockchain when nodes execute zero-knowledge proof protocol successfully. They also provide optional disclosure of the real identity when disputes occur.

Biometric authentication is also widely used, such as face and voice pattern identification, retinal pattern analysis, hand characteristics and automated fingerprint analysis based on pattern recognition.

Lee and Yang (2018) proposed that human nails can be used for identity authentication since nails have the high degree of uniqueness. The system uses histogram of oriented gradients (HOG) and local binary pattern (LBP) feature to extract the biometric identification signature, then SVM and convolutional neural network are utilized for authentication with high accuracy. This identity verification technology with dynamic identity rather than regular real identity information ensures user anonymity and privacy.

The main goal of identity management is to ensure that only authenticated users can be authorized to access the specified resource. Currently, most systems rely on membership service component or similar providers for identity authentication.

Traditional authentication process mainly adopts password authentication and even transmit user account in the clear text. Anyone can eavesdrop on the external connection to intercept user account. In this case, attackers or curious third parties may impersonate compromised users to gain access to sensitive data.

It is difficult to find and rely on such a trustworthy third membership service party that validates user identity and accomplishes complex cross-heterogeneous domains authentication honestly without potential risk of real identity leakage. Besides, typical blockchain systems cannot provide privacy-preserving verification due to public transaction record including pseudonyms and related behavior. In this case, curious third servers or network nodes may collect large amounts of data to infer the real identity by statistical analysis.

From Table 7, most schemes adopt different authentication protocols, some of which bring a certain amount of cost and may be not suitable for IoT environment. Lightweight authentication protocol is a direction for improving the performance of blockchain-based EHR systems, especially in the IoT context. Attention should be paid to privacy preserving membership verification support by proper cryptographic algorithms and transaction privacy of blockchain without disclosure of identities.

4. Future trends

4.1. Big data

A big challenge for healthcare data systems to improve healthcare service quality is how to gather, process and analyze large volumes of personal healthcare data, especially from widely used mobile devices and wearable devices, with minimal privacy violations. Blockchain technology can be a solution for security issue of big data technique with immutability, security and traceability.

Otero et al. (2014) mentioned that big data can make maximal use of all of healthcare data assets to support necessary improvements: prediction in the healthcare diagnosis, analysis in the magnetic resonance imaging and other applications.

Big data analysis can be roughly categorized into two types: data management and data analysis. As for data management, blockchain can be used to store immutable healthcare information. As for data analysis, transactions and record on the blockchain can be extracted and analyzed for potential trading behavior.

4.2. Machine learning

Machine learning technique can promote the optimization of healthcare systems and provide intelligent services effectively. A big challenge for practical systems applying machine learning is how to store, share and train sensitive datasets securely. There is a growing trend of integrating machine learning with blockchain to enhance the security and privacy of datasets Zheng et al. (2018); Lee and Yang (2018).

Federated learning is an efficient machine learning technique carried out among multiple computing nodes under the precondition of the security and privacy protection of sensitive data during data exchange. Different medical institutions can collaborate to train high accurate prediction model by sharing encrypted datasets. Blockchain as a regulator can record related training transactions in an immutable and transparent manner to achieve accountability and reliable cooperation. In this case, medical organizations and researchers will be more willing to share encrypted datasets to promote the development of medical treatment and public health.

Blockchain as reliable backbone for machine learning algorithms makes sure the security of data input. Sharing large datasets across different applications and domains is the first concern

Table 7
Main techniques of identity manager in the existing EHR schemes.

paper	main techniques	analysis
Liang et al. (2017)	MSP	MSP supports the identity authentication and authorization verification based on traditional Public Key Infrastructure (PKI) model
Al Omar et al. (2017)	customized registration module	the preservation of PWD and the establishment of secured channel for authentication are vulnerable using pass-through authentication
Azaria et al. (2016a)	registrar smart contract	the mapping of identity information is like a DNS-like implementation secured ID-based identification scheme can be employed to enhance the security
Zhang et al. (2016)	improved IEEE 802.15.6 display authenticated association protocol	the performance of this improved protocol under large scale devices needs to be studied
Xia et al. (2017)	identity-based authentication and key agreement protocol	authentication protocols and algorithms between entities are not fully investigated, such as computational cost, performance and security analysis
Shae and Tsai (2017)	anonymous identities authentication mechanism	this mechanism based on zero-knowledge technology may have high computational cost among resource-limited IoT devices
Sun et al. (2018)	decentralizing attribute-based signature scheme	the performance of this scheme under large scale requests needs to be studied
Hardjono (2019)	anonymous but verifiable identification scheme	this scheme based on zero-knowledge technology may have high computational cost in the blockchain
Lee and Yang (2018)	biometric recognition	it is difficult to avoid the data manager from leaking nail data

Yaji et al. (2018). There is active research into homomorphic encryption Gentry (2009) to perform machine learning on encrypted data. However, the computational overhead of homomorphic encryption is high in practice. Perhaps in the future sensitive data can be encrypted without impacting the machine learning for intelligent services.

Blockchain can also allow rollback models storage if false predication rate is high. Blockchain stores the pointers of relevant data of retrained models in a secure and immutable manner. Juneja and Marefat (2018) proposed that retraining models indexed by pointers in the blockchain can increase the accuracies for continuous remote systems in the context of irregular arrhythmia alarm rate.

Additionally, artificial intelligence can be applied to design automatic generation of smart contact to enhance secure and flexible operations.

4.3. Internet of things (IoT)

In the context of IoT, the locations of products can be tracked at each step with radio-frequency identification (RFID), sensors or GPS tags. Individual healthy situation can be monitored at home via sensor devices and shared on the cloud environment where physical providers can access to provide on-time medical supports.

However, as the use of sensors is experiencing exponential growth in various environments, the security level of sensitive data of these sensors has to be improved. Currently most of IoT data is transmitted among computationally limited devices in the trustless wireless environments where malicious attackers may intercept the communication link and alter the data.

Blockchain can contribute to ensuring the security of these devices and the privacy of personal information. The relevant systems based on blockchain in the previous sections provide secure data access control framework and decentralized key management to build secure communication among IoT devices.

Additionally, 5G would be the next generation communication network with high speed, large capacity and scalability. IoT with 5G is expected to become an important driver of next-generation smart healthcare with greater throughput, lower latency and high reliability. Lloret et al. (2017) proposed a next-generation wireless smartphone 5G network for continuous monitoring of chronic patients. Similarly, Min et al. (2018) provided constant assessment and monitoring of diabetes patients.

Blockchain could be also deployed in this framework to enhance the security of network slice broker and 5G network management layer.

4.4. Edge computing

The far placement of cloud services makes network communication inefficient for time-critical applications. Edge computing is proposed in Gai et al. (2019) to extend cloud services to the edge of network, provide computation power and improve Quality of Service of the applications. Edge computing consists of a group of servers/sensors for data collections, some of which can offer computation capabilities. Multiple edge servers have so sufficient resources to perform the blockchain computation such as encryption algorithms and consensus operations.

However, there are big challenges for decentralized management and data security across edge nodes since data is stored across different storage locations. Blockchain could enhance the capability of edge computing from privacy preserving, tamper-resistant verification as well as transparent auditability aspects Yang et al. (2019). Besides, smart contracts can facilitate edge resources allocation and reduce operational costs.

Such integrated framework is aimed at computational resources reduction on devices and secure distributed management, which covers the core layers of blockchain and the capability of edge computing.

Moreover, edge computing integrated with outsourcing computation is a direction worthy of further study to realize secure and private computation.

4.5. Improvement of blockchain performance

Blockchain suffering from expensive computing, large storage and high bandwidth overhead may be not suitable for practical application development. When many organizations participate in the network, large data volume, frequent requests and the stability of blockchain can not be ignored.

Currently, a few studies focus on solving the above mentioned problems. Related research mainly focuses on the improvement of consensus algorithm, block size design Xia et al. (2017) and so on.

Croman et al. (2016) mainly improved the scalability of blockchain on latency, throughput and other parameters. The experiments showed that block size and generation interval in Bitcoin are the first step toward throughput improvements and latency reduction without threat to system decentralization.

Consensus protocols are necessary structures for transactions verification to reach an agreement in the blockchain network. Liu et al. (2018) improved election method of DPoS according to the rank of medical institutions credit scores to enhance the trust between a certain number of selected medical organizations nodes and guarantee the reliability of consortium blockchain.

Brooks et al. (2018) designed a novel Lightweight Mining (LWM) algorithm that requires fewer resources in terms of both storage and computation. The core idea, "sharing-hash-first", ensures the fairness for every miner in the whole network. LMW can tolerate up to N-1 colluded miners, which indicates its robustness to malicious miners and Distributed Denial of Service (DDoS) attack.

Jiang et al. (2018) proposed two loosely-coupled blockchain based on two kinds of healthcare data, electronic medical records (EMR) and personal healthcare data(PHD). New challenges for two data types in the blockchain-based system are throughput and fairness. Two fairness-based packing algorithms are designed to improve the throughput and fairness of system among users.

In the practical application scenario, how to encourage miners to participate in the network is important for the maintenance of trustworthy and stable blockchain. Azaria et al. (2016a) proposed an incentive mechanism to encourage medical researchers and healthcare authorities as miners and create data economics by awarding for big data on hospital records to researchers.

Yang and Li (2018) proposed a selection method in the incentive mechanism. Providers have less significance (means the efforts that providers have been made on network maintenance and new blocks generation) with higher probabilities of being selected to carry out the task of new block generation and will be granted significance as bonus to reduce the selected probability in future.

Pham et al. (2018) made further improvements on gas prices of blockchain, which can boost the priority in the processing transaction queue by automatically adjusting the gas price and then trigger an emergency contact to providers for on-time treatment immediately.

Meanwhile, it should be noted that all transactions can be "seen" by any node in the blockchain network. Homomorphic encryption and zero knowledge proofs could be utilized to prevent data forensics by inference, maintain the privacy of individual information and allow computations to be performed without the leakage of input and output of computations.

As the above statement, blockchain still has many limitations and more aggressive extensions will require fundamental protocol redesign. So it is urgent to be towards to the improvement of underlying architecture of blockchain for better service.

In the context of IoT, personal healthcare data streams collected from wearable devices are high in volume and at fast rate. Large amounts of data can support for big data and machine learning to increase the quality of data and provide more intelligent health service.

However, it may lead to high network latency due to the physical distance to mobile devices and traffic congestion on the cloud servers. Besides, the mining process and some encryption algorithms may cost high computational power on resource-limited devices and restrict the use of blockchain.

A new trend is increasingly moving from the function of clouds towards network edge with low network latency. It is mainly required by time-sensitive applications, like healthcare monitor applications. Combining with edge computing, blockchain is broadened to a wide range of services from pure data storage, such as device configuration and governance, sensor data storage and management, and multi-access payments.

4.6. Standards and regulations

If new technologies enter the market without some form of vetting, they should be adopted with care for example based on a cost-benefit-analysis. Hence, to improve compliance, security, interoperability and other factors, we need to develop uniform standards, policies and regulations (e.g. those relating to data security and privacy, and blockchain ecosystem). For example, we would likely need different independent and trusted mechanisms to evaluate different blockchain solutions for different applications and context, in terms of privacy, security, throughput, latency, capacity, etc. We would also need to be able to police and enforce penalty for misbehavior and/or violations (e.g. non-compliance or not delivering as agreed in the contract).

5. Conclusion

Blockchain has shown great potential in transforming the conventional healthcare industry, as demonstrated in this paper. There, however, remain a number of research and operational challenges, when attempting to fully integrate blockchain technology with existing EHR systems. In this paper, we reviewed and discussed some of these challenges. Then, we identified a number of potential research opportunities, for example relating to IoT, big data, machine learning and edge computing. We hope this review will contribute to further insight into the development and implementation of the next generation EHR systems, which will benefit our (ageing) society.

Declaration of Competing Interest

The authors declare that they have no conflicts of interest.

Acknowledgements

We thank the anonymous reviewers for their valuable comments and suggestions which helped us to improve the content and presentation of this paper. The work was supported by the National Key Research and Development Program of China (No. 2018YFC1315404), the National Natural Science Foundation of China (Nos. 61972294, 61932016), Researchers Supporting Project number (RSP-2020/12), King Saud University, Riyadh, Saudi Arabia and the Opening Project of Guangxi Key Laboratory of Trusted Software (No. kx202001). The last author is supported only by the Cloud Technology Endowed Professorship of USA.

References

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., Amaba, B., 2017. Blockchain technology innovations. In: 2017 IEEE Technology & Engineering Management Conference (TEMSCON). IEEE, pp. 137–141.

Ahsan, M.M., Wahab, A.W.A., Idris, M.Y.I., Khan, S., Bachura, E., Choo, K.-K.R., 2020. Class: cloud log assuring soundness and secrecy scheme for cloud forensics. IEEE Trans. Sustain. Comput..

Al Omar, A., Rahman, M.S., Basu, A., Kiyomoto, S., 2017. Medibchain: a blockchain based privacy preserving platform for healthcare data. In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, pp. 534–543.

Azaria, A., Ekblaw, A., Vieira, T., Lippman, A., 2016. Medrec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD). IEEE, pp. 25–30.

Azaria, A., Ekblaw, A., Vieira, T., Lippman, A., 2016. Medrec:using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD). IEEE, pp. 25–30.

Bahga, A., Madisetti, V.K., 2013. A cloud-based approach for interoperable electronic health records (ehrs). IEEE J. Biomed. Health Inform. 17 (5), 894–906.

Begoyan, A., 2007. An overview of interoperability standards for electronic health records. USA: society for design and process science.

Benchoufi, M., Ravaud, P., 2017. Blockchain technology for improving clinical research quality. Trials 18 (1), 335.

Blum, M., Feldman, P., Micali, S., 1988. Non-interactive zero-knowledge and its applications (extended abstract). In: Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2–4, 1988, Chicago, Illinois, USA.

Boonstra, A., Versluis, A., Vos, J.F., 2014. Implementing electronic health records in hospitals: a systematic literature review. BMC Health Serv. Res. 14 (1), 370.

Brooks, R.R., Wang, K.-H.C., Yu, L., Oakley, J., Skjellum, A., SimCenter, Obeid, J.S., Lenert, L., Worley, C.R., 2018. Scrybe : A blockchain ledger for clinical trials.

Carvalho, J.V., Rocha, Á., Abreu, A., 2016. Maturity models of healthcare information systems and technologies: a literature review. J. Med. Syst. 40 (6), 131.

Castro, M., Liskov, B., 1999. Practical byzantine fault tolerance. Symposium on Operating Systems Design & Implementation.

Crameri, K.-A., Maher, L., Van Dam, P., Prior, S., 2020. Personal electronic healthcare records: What influences consumers to engage with their clinical data online? a literature review. Health Inf. Manag. J.. 1833358319895369

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., 2016. On scaling decentralized blockchains.

Daemen, J., Rijmen, V., 2002. The design of rijndael: aes - the advanced encryption standard.

Dai, W., Dai, C., Choo, K.R., Cui, C., Zou, D., Jin, H., 2020. SDTE: a secure blockchain-based data trading ecosystem. IEEE Trans. Inf. Forens. Secur. 15, 725–737.

Dan G., Paul B., Angus Ch., Andrew B., How distributed ledgers can improve provider data management and support interoperability, 2016.

Dias, J. P., Reis, L., Ferreira, H. S., Martins, Â., 2018. Blockchain for access control in e-health scenarios. arXiv:1805.12267.

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F., 2017. Secure and trustable electronic medical records sharing using blockchain. In: AMIA Annual Symposium Proceedings, 2017. American Medical Informatics Association, p. 650.

Esposito, C., Santis, A.D., Tortora, G., Chang, H., Choo, K.R., 2018. Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 5 (1), 31–37.

Ethereum: Blockchain app platforms. (2015). [online] Available: https://www.ethereum.org/.

Feng, Q., He, D., Liu, Z., Wang, D., Choo, K.-K.R., 2020. Multi-party signing protocol for the identity-based signature scheme in ieee p1363 standard. IET Information Security 1 (99), 1–10. DOI: 10.1049/iet-ifs.2019.0559

Feng, Q., He, D., Zeadally, S., Khan, M.K., Kumar, N., 2019. A survey on privacy protection in blockchain system. J. Netw. Comput. Appl. 126, 45–58.

Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O., Toval, A., 2013. Security and privacy in electronic health records: asystematic literature review. J. Biomed. Inform. 46 (3), 541–562.

Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O., Toval, A., 2013. Security and privacy in electronic health records: asystematic literature review. J. Biomed. Inform. 46 (3), 541–562.

Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O., Toval, A., 2013. Security and privacy in electronic health records: asystematic literature review. J. Biomed. Inform. 46 (3), 541–562.

Gai, K., Wu, Y., Zhu, L., Xu, L., Zhang, Y., 2019. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. IEEE Internet Things J..

Gentry, C., 2009. A fully homomorphic encryption scheme. Stanford University. https://www.crypto.stanford.edu/craig

Grispos, G., Glisson, W.B., Choo, K.-K.R., 2017. Medical cyber-physical systems development: a forensics-driven approach. In: 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE). IEEE, pp. 108–113.

Guo, R., Shi, H., Zhao, Q., Zheng, D., 2018. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access 6, 11676–11686.

GemOS: the blockchain operating system. (2020). [online.] Available: https://enterprise.gem.co/.

He, D., Zhang, Y., Wang, D., Choo, K.-K.R., 2018. Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography. IEEE Transactions on Dependable and Secure Computing 1 (99), 1–10. DOI: 10.1109/TDSC.2018.2857775

Ho, S.Y., Guo, X., Vogel, D., 2019. Opportunities and challenges in healthcare information systems research: caring for patients with chronic conditions. Commun. Assoc. Inf. Syst. 44 (1), 39.

Hsieh, G., Chen, R.-J., 2012. Design for a secure interoperable cloud-based personal health record service. In: 4th IEEE international conference on cloud computing technology and science proceedings. IEEE, pp. 472–479.

Hardjono, Thomas, and Alex Pentland. "Verifiable anonymous identities and access control in permissioned blockchains." arXiv preprint arXiv:1903.04584 (2019).

Hui, H., XiaoFeng, C., Jianfeng, W., Blockchain-based multiple groups data sharing with anonymity and traceability. SCI. CHINA Inf. Sci.

Hyperledger Fabric, (2020). [online] Available: https://www.hyperledger.org/.

Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., He, J., 2018. Blochie: a blockchain-based platform for healthcare information exchange. In: 2018 IEEE International Conference on Smart Computing (SMARTCOMP). IEEE, pp. 49–56.

Johnson, D., Menezes, A., Vanstone, S., 2001. The elliptic curve digital signature algorithm (ecdsa). Int. J. Inf. Secur. 1 (1), 36–63.

Juneja, A., Marefat, M., 2018. Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification. In: 2018 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI). IEEE, pp. 393–397.

Kalam, A.A.E., Baida, R.E., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C., Trouessin, G., 2003. Organization based access control. In: Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks. IEEE, pp. 120–131.

Kamauu, A.W., DuVall, S.L., Avrin, D.E., 2009. Using java to generate globally unique identifiers for dicom objects. J. Digit. Imag. 22 (1), 11–14.

Kim, M.G., Lee, A.R., Kwon, H.J., Kim, J.W., Kim, I.K., 2018. Sharing medical questionnaries based on blockchain. In: 2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM). IEEE, pp. 2767–2769.

Kuo, T.-T., Kim, H.-E., Ohno-Machado, L., 2017. Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inf. Assoc. 24 (6), 1211–1220.

Lamport, L., Shostak, R., Pease, M., 1982. The byzantine generals problem. Acm Trans. Programm. Lang. Syst. 4 (3), 382–401.

Lee, S.H., Yang, C.S., 2018. Fingernail analysis management system using microscopy sensor and blockchain technology. International Journal of Distributed Sensor Networks 14 (3). 1550147718767044

Liang, X., Zhao, J., Shetty, S., Liu, J., Li, D., 2017. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, pp. 1–5.

Lin, C., He, D., Huang, X., Khan, M.K., Choo, K.-K.R., 2020. Dcap: a secure and efficient decentralized conditional anonymous payment system based on blockchain. IEEE Trans. Inf. Forensics Secur. 15, 2440–2452.

Liu, J., Li, X., Ye, L., Zhang, H., Du, X., Guizani, M., 2018. Bpds: A blockchain based privacy-preserving data sharing for electronic medical records. In: 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, pp. 1–6.

Lloret, J., Parra, L., Taha, M., Toms, J., 2017. An architecture and protocol for smart continuous ehealth monitoring using 5g. Computer Networks. S1389128617302189

Lluch, M., 2011. Healthcare professionals organisational barriers to health information technologies a literature review. Int. J. Med. Inform. 80 (12), 849–862.

Ma, S., Deng, Y., He, D., Zhang, J., Xie, X., 2020. An efficient nizk scheme for privacy-preserving transactions over account-model blockchain. IEEE Transactions on Dependable and Secure Computing. DOI: 10.1109/TDSC.2020.2969418

Maesa, D., Mori, P., Ricci, L., 2018. Blockchain based access control services. 10.1109/Cybermatics_2018.2018.00237.

McGhin, T., Choo, K.R., Liu, C.Z., He, D., 2019. Blockchain in healthcare applications: research challenges and opportunities. J. Netw. Comput. Appl. 135, 62–75.

Mettler, M., 2016. Blockchain technology in healthcare: The revolution starts here. In: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE, pp. 1–3.

Miah, S.J., Gammack, J., Hasan, N., 2019. Methodologies for designing healthcare analytics solutions: A literature analysis. Health Informatics Journal. 1460458219895386

Min, C., Yang, J., Zhou, J., Hao, Y., Youn, C.H., 2018. 5g-smart diabetes: toward personalized diabetes diagnosis with healthcare big data clouds. IEEE Commun. Mag. 56 (4), 16–23.

Morelli, U., Ranise, S., Sartori, D., Sciarretta, G., Tomasi, A., 2019. Audit-based access control with a distributed ledger: applications to healthcare organizations. In: International Workshop on Security and Trust Management. Springer, pp. 19–35.

MultiChain: Open platform for building blockchains. (2020). [online] Available: https://www.multichain.com/.

Nakamoto, S., et al., 2008. Bitcoin: A peer-to-peer electronic cash system.

Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A., 2019. Blockchain for secure ehrs sharing of mobile cloud based e-health systems. IEEE Access.

Nugent, T., Upton, D., Cimpoesu, M., 2016. Improving data transparency in clinical trials using blockchain smart contracts. F1000Res 5.

Otero, P., Hersh, W., Ganesh, A.J., 2014. Big data: are biomedical and health informatics training programs ready? Yearb Med. Inform. 23 (01), 177–181.

Outchakoucht, A., Hamza, E., Leroy, J.P., 2017. Dynamic access control policy based on blockchain and machine learning for the internet of things. Int. J. Adv. Comput. Sci. Appl. 8 (7), 417–424.

Patel, V., 2018. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health informatics journal. 1460458218769699

Peng, Z., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T., 2018. Fhirchain: applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J. 16, 267–278.

Peterson, K., Deeduvanu, R., Kanjamala, P., Boles, K., 2016. A blockchain-based approach to health information exchange networks. In: Proc. NIST Workshop Blockchain Healthcare, 1, pp. 1–10.

Pham, H.L., Tran, T.H., Nakashima, Y., 2018. A secure remote healthcare system for hospital using blockchain smart contract. In: 2018 IEEE Globecom Workshops (GC Wkshps). IEEE, pp. 1–6.

Pussewalage, H.S.G., Oleshchuk, V.A., 2018. Blockchain based delegatable access control scheme for a collaborative e-health environment. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, pp. 1204–1211.

Qi, X., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., Guizani, M., 2017. Medshare: trust–less medical data sharing among cloud service providers via blockchain. IEEE Access 5 (99), 14757–14767.

Rahman, N.H.A., Glisson, W.B., Yang, Y., Choo, K.R., 2016. Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Comput. 3 (1), 50–59.
Ramani, V., Kumar, T., Bracken, A., Liyanage, M., Ylianttila, M., 2018. Secure and efficient data accessibility in blockchain based healthcare systems. In: 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, pp. 206–212.
Rifi, N., Rachkidi, E., Agoulmine, N., Taher, N.C., 2017. Towards using blockchain technology for ehealth data access management. In: 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME). IEEE, pp. 1–4.
Seol, K., Kim, Y.-G., Lee, E., Seo, Y.-D., Baik, D.-K., 2018. Privacy-preserving attribute-based access control model for xml-based electronic health record system. IEEE Access 6, 9114–9128.
Shae, Z., Tsai, J.J., 2017. On the design of a blockchain platform for clinical trial and precision medicine. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). IEEE, pp. 1972–1980.
Steinfeld, R., Bull, L., Zheng, Y., 2001. Content extraction signatures.. Icisc 2002, 285–304.
Strudwick, G., Eyasu, T., 2015. Electronic health record use by nurses in mental health settings: a literature review. Arch. Psychiatr. Nurs. 29 (4), 238–241.
Sun, Y., Zhang, R., Wang, X., Gao, K., Liu, L., 2018. A decentralizing attribute-based signature for healthcare blockchain. In: 2018 27th International Conference on Computer Communication and Networks (ICCCN). IEEE, pp. 1–9.
Tovanich, N., Heulot, N., Fekete, J.-D., Isenberg, P., 2020. Visualization of blockchain data: a systematic review. IEEE Trans. Vis. Comput. Graph..
Vanstone, S., Menezes, A., Oorschot, P.V., 1997. Handbook of applied cryptography.
Wang, S., Zhang, Y., Zhang, Y., 2018. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access 6, 38437–38450.
Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., Kim, D.I., 2019. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access 7, 22328–22370.
Xia, Q., Sifah, E., Smahi, A., Amofa, S., Zhang, X., 2017. Bbds: blockchain-based data sharing for electronic medical records in cloud environments. Information 8 (2), 44.
Yaji, S., Bangera, K., Neelima, B., 2018. Privacy preserving in blockchain based on partial homomorphic encryption system for ai applications. In: 2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW). IEEE, pp. 81–85.
Yang, G., Li, C., 2018. A design of blockchain-based architecture for the security of electronic health record (ehr) systems. In: 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, pp. 261–265.
Yang, R., Yu, F.R., Si, P., Yang, Z., Zhang, Y., 2019. Integrated blockchain and edge computing systems: asurvey, some research issues and challenges. IEEE Commun. Surv. Tutor. 21 (2), 1508–1532.
Yue, X., Wang, H., Jin, D., Li, M., Jiang, W., 2016. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. 40 (10), 218.
Zhang, J., Xue, N., Huang, X., 2016. A secure system for pervasive social network-based healthcare. IEEE Access 4, 9239–9250.
Zhang, P., White, J., Schmidt, D. C., Lenz, G., 2017. Applying software patterns to address interoperability in blockchain-based healthcare apps. arXiv:1706.03700.
Zhao, H., Zhang, Y., Peng, Y., Xu, R., 2017. Lightweight backup and efficient recovery scheme for health blockchain keys. In: 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS). IEEE, pp. 229–234.
Zheng, X., Mukkamala, R.R., Vatrapu, R., Ordieres-Mere, J., 2018. Blockchain-based personal health data sharing system using cloud storage. In: 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE, pp. 1–6.
Zyskind, G., Nathan, O., Pentland, A., 2015. Enigma: Decentralized computation platform with guaranteed privacy. arXiv:1506.03471.

Shuyun Shi received the Bachelor degree in 2019, from the School of Computer Science, SUN YAT-SEN University, Guangzhou, China. She is currently working toward a Master degree at the Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China. Her research interests include blockchain and cryptographic protocols.

Debiao He received his Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University, Wuhan, China in 2009. He is currently a professor of the Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China. His main research interests include cryptography and information security, in particular, cryptographic protocols.

Li Li received her Ph.D degree in computer science from Computer School, Wuhan University. She is currently an associate professor at School of Software, Wuhan University. Her research interests include data security and privacy, applied cryptography and security protocols.

Neeraj Kumar received his Ph.D. in CSE from Shri Mata Vaishno Devi University, Katra, India. He is now an Associate Professor in the Department of Computer Science and Engineering, Thapar University, Patiala, Punjab (India). He is with Department of Computer Science and Information Engineering, Asia University, Taiwan and King Abdul Aziz University, Jeddah, Saudi Arabia. He is a member of IEEE. His research is focused on mobile computing, parallel/distributed computing, multiagent systems, service oriented computing, routing and security issues in mobile ad hoc, sensor and mesh networks. He has more than 100 technical research papers in leading journals such as-IEEE TII, IEEE TIE, IEEE TDSC, IEEE ITS, IEEE TWPS, IEEE SJ, IEEE ComMag, IEEE WCMag, IEEE NetMag and conferences. His research is supported from DST, TCS and UGC. He has guided many students leading to M.E. and Ph.D.

Muhammad Khurram Khan is currently working as a Professor of Cybersecurity at the Center of Excellence in Information Assurance (CoEIA), King Saud University, Kingdom of Saudi Arabia. He is founder and CEO of the 'Global Foundation for Cyber Studies and Research' (http://www.gfcyber.org). He is the Editor-in-Chief of a well-reputed International journal 'Telecommunication Systems' published by Springer for over 26 years with its recent impact factor of 1.707 (JCR 2019). Furthermore, he is on the editorial board of several international journals, including, IEEE Communications Surveys & Tutorials, IEEE Communications Magazine, IEEE Internet of Things Journal, IEEE Transactions on Consumer Electronics, etc. He has published more than 350 research papers in the journals and conferences of international repute. In addition, he is an inventor of 10 US/PCT patents. He has edited 7 books/proceedings published by Springer-Verlag and IEEE. He has secured several national and international competitive research grants in the domain of Cybersecurity. He has played a leading role in developing 'BS Cybersecurity Degree Program' and 'Higher Diploma in Cybersecurity' at King Saud University. His research areas of interest are Cybersecurity, digital authentication, IoT security, cyber policy, and technological innovation management. He is a fellow of the IET (UK), fellow of the BCS (UK), fellow of the FTRA (Korea), senior member of the IEEE (USA), senior member of the IACSIT (Singapore), member of the IEEE Consumer Electronics Society, member of the IEEE Communications Society, member of the IEEE Technical Committee on Security & Privacy, member of the IEEE IoT Community, member of the IEEE Smart Cities Community, and member of the IEEE Cybersecurity Community. He is also the Vice Chair of IEEE Communications Society Saudi Chapter. He is a distinguished Lecturer of the IEEE (CESoC).

Kim-Kwang Raymond Choo holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). He is the recipient of the 2019 IEEE TCSC Award for Excellence in Scalable Computing (Middle Career Researcher), 2018 UTSA College of Business Endowed Research Award for Tenured Faculty, IEEE Access Outstanding Associate Editor of 2018, British Computer Society's 2019 Wilkes Award Runner-up, 2019 EURASIP JWCN Best Paper Award, Korea Information Processing Society's JIPS Survey Paper Award (Gold) 2019, IEEE Blockchain 2019 Outstanding Paper Award, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a Fellow of the Australian Computer Society, an IEEE Senior Member, and Co-Chair of IEEE MTCT's Digital Rights Management for Multimedia Interest Group.