Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-021-03448-7

ORIGINAL RESEARCH

Blockchain-based medical data sharing schedule guaranteeing security of individual entities

Chien-Ming Chen[1] · Xiaoting Deng[2] · Sachin Kumar[3] · Saru Kumari[4] · SK Hafizul Islam[5]

Received: 25 February 2021 / Accepted: 17 August 2021

Abstract

In a modern electronic medical system, data sharing between medical institutions must have a more comprehensive understanding of the patient's condition. However, different hospitals typically use other databases, even if the data belong to the same person. Each hospital manages its database in a centralized and closed manner. This approach makes the databases vulnerable to single-point attacks by malicious attackers and undermines medical care continuity. In this paper, we use a blockchain concept that provides a secure distributed environment to avoid single-point attacks. We develop a novel medical data sharing schedule that uses the blockchain to integrate each hospital's resources. Compared with other blockchain-based schemes, we categorize and manage different requests for medical data sharing: (i) sharing between hospitals of the same level; (ii) sharing between hospitals of different levels. Additionally, our schedule ensures the security of individual entities in the process of data sharing. We conduct a security analysis and a comparative validation to show that the proposed systems are secure. In the subsequent analysis of the system, the feasibility of the proposed system was examined.

Keywords Blockchain · Medical data sharing · Individual security · Privacy

1 Introduction

With the rapid development of science and technology, modern medical data have been recorded electronically. However, to ensure patient data security and specific business interests, various hospitals commonly save the data in their private databases to manage it in a centralized manner (Kuo and Ohno-Machado 2018; Axelsson 2000; Zhang et al. 2017; Shamshad et al. 2020). This data management approach has become a major stumbling block for the rapid development of the medical industry.

First, the data storage approach easily causes data fragmentation, limiting the access to medical data and impeding the big data analysis for complex diseases (Azaria et al. 2016). Besides, centralized organizational structures are vulnerable to single-point attacks that may compromise patient data. Furthermore, medical data belong to hospitals, and patients do not own their medical data (Kish and Topol 2015). The patients cannot access their data at any time: the access is restricted. Thus, it is difficult for patients to provide relevant information on their medical history when seeing a doctor in another hospital because they cannot describe their illness accurately and professionally (as a skilled medical staff member would explain). Consequently, doctors from

✉ Chien-Ming Chen
chienmingchen@ieee.org

Xiaoting Deng
1553968578@qq.com

Sachin Kumar
imsachingupta@rediffmail.com

Saru Kumari
saryusiirohi@gmail.com

SK Hafizul Islam
hafi786@gmail.com

[1] College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao, China

[2] School of Computer Science and Technology, Harbin Institute of Technology (Shenzhen), Shenzhen, China

[3] Department of Computer Science and Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, India

[4] Department of Mathematics, Ch. Charan Singh University, Meerut, Utter Paradesh, India

[5] Department of Computer Science and Engineering, Indian Institute of Information Technology Kalyani, West Bengal, India

Published online: 22 August 2021

another hospital may be unable to give a comprehensive treatment plan for complex diseases because of a lack of detailed understanding of patients' previous visits, thus delaying the treatment or misdiagnosing the condition.

Therefore, more experts and scholars start to research the problem of secure sharing of medical data. In previous years, with the development of cloud service technology (Lin et al. 2019; Huang et al. 2016), most medical institutions have chosen a third-party cloud server as a platform for data sharing (Yang et al. 2015; Thilakanathan et al. 2014; Koufi et al. 2010). However, these cloud-based applications are often subject to a range of attacks, including identity theft, eavesdropping, and data modification. Although several services provide unsupervised cloud servers to protect the privacy of data sharing, this centralized storage mode is obviously vulnerable to single-point attacks.

Blockchain is a distributed ledger technology: a series of data records organized in a specific order. The distributed nature of blockchain makes it perfectly able to avoid the single point of attack in the cloud storage environment. Besides, the irreversibility of its embedded hash makes it resistant to both phishing attacks and tampering attacks. Many papers have demonstrated that blockchain has specific features to address everyday life's security requirements, such as distributed storage, verified authentication, and anonymity. After more than ten years of development, Bitcoin network has verified the security of blockchain technology. In Chen et al. (2018) describes some of the current blockchain applications for education. Griggs et al. (2018) proposed a blockchain system for secure automated remote patient monitoring. In Tseng et al. (2019) proposed a mechanism for food traceability based on blockchain. Security features of blockchain are gradually being applied in other fields, such as digital cash (Wörner and Bomhard 2014; Yeh et al. 2018), Internet of things (Yavari et al. 2020; Chen et al. 2021a; Wang et al. 2020; Sharma et al. 2018), and smart cities (Chen et al. 2021b; Zhu et al. 2020; Hsiao et al. 2017).

Our analysis and comparison found that the globally distributed property of blockchain is perfectly matched with the cross-domain demand for medical data sharing. Thus, in this paper, we utilize the blockchain to manage data sharing for medical industries. We use hierarchical thinking to stratify the existing medical institutions. More specifically, medical data sharing may happen in various national hospitals or between national hospitals and community hospitals. Thus, we provide two feasible data sharing solutions for each situation, respectively. The proposed schemes are used to ensure the privacy of data sharing parties. Finally, we conduct a security analysis and a comparative validation to show that the proposed systems are secure and efficient.

The remainder of the paper is organized as follows. Section 2 overviews the recent literature on blockchain applications in medical data sharing. Additionally, we formulate the security requirements for our solution. Section 3 presents the network model of our proposed data sharing schedule and describes the data sharing process for national hospitals and community hospitals. In Sect. 4, we systematically analyze the security of our design and compare it with blockchain-based systems mentioned in Sect. 2. Finally, our conclusion is presented in Sect. 5.

2 Related work

2.1 Drawbacks of existing approaches

Characteristics of blockchain technology correspond to the architectural characteristics and security requirements of typical medical data sharing applications. Several approaches to the use of blockchain for medical data sharing have been proposed.

Gem Health Network (Mettler 2016) is a shared network infrastructure proposed to ensure real-time access of healthcare professionals to the same information. In this design, any certified medical professional can view the data on the shared platform. This approach not only removes the centralized architecture, but also ensures the privacy and security of data sharing. However, uniform resource allocation increases the storage pressure on the entire blockchain sharing platform, and data requests of different levels are mixed together, which makes it very difficult to update the data.

A system called *Medrec* (Azaria et al. 2016) is another data sharing system for medical industry. It has a strict identity authentication mechanism with smart contracts, clever to achieve the recovery and release of authority. Using this system, patients can access their medical information in real time across multiple medical providers and different treatment locations. The biggest weakness of this design is that it is difficult to ensure the data security of individual hospital databases in the process of sharing.

To ensure the security of patient data, Xia et al. (2017) proposed a method of protecting data security among different medical institutions in an untrusted environment. Their design uses smart contracts and access control to track the data flow and revoke the access rights when malicious attacks are detected, increasing the confidence. However, as the number of requests for adding or retrieving the data increases, the system's latency also increases (Xia et al. 2017; McGhin et al. 2019).

2.2 Security requirements

In the process of medical data sharing, the most basic requirement is to ensure the accessibility of medical data. The second requirement is to ensure the security of medical data transmission and avoid various attacks. The third

requirement is to ensure individual security of data-sharing entities. Only when the privacy of individual parties is protected, the medical entities will be willing to share their resources, and the level of medical services will improve faster. In this section, we discuss the security requirements for the medical data sharing and explain how to address them.

- **Decentralization**: We need to eliminate the single point of attack (the problem that appears in the traditional cloud storage). In our model, we use the distributed nature of blockchain to form a point-to-point distributed network architecture among national hospitals. (A national hospital is owned by the state, which means that it has more medical resources and a higher medical level than private hospitals.)
- **Ownership of data**: In the traditional cloud storage model, patients' medical data are stored on the cloud server and owned by the cloud service provider. This involves a risk of leakage and malicious tampering of patient data. Most importantly, patients have no access to their own medical data, even if they can prove their ownership. Thus, we need to ensure that patients at one hospital can authorize the doctors to access their previous medical records from another hospital. In this system, we assign a unique attribute to the data by storing the patient's biological information.
- **Protect individual safety**: Medical data of a patient include not only details of their medical condition, but also key information about the hospital such as the prices of services (which the hospital may not be willing to disclose). Thus, for the security of medical entities, we will preprocess the patient records and obtain a summary of the case for data sharing.

3 Our system

In this section, we introduce the proposed design. First, we describe a blockchain-based model for medical data sharing. Next, we initialize a secure link between each entity and the addresses assigned for communication. Next, we mention how patient information is stored. Finally, we provide an ideal solution when sharing management happens in various national hospitals or happens between national hospital and community hospital, respectively. Notations used in this paper are listed in Table 1.

3.1 Network model

A complete data sharing system for medical industries, as shown in Fig. 1, involves three layers: patient, hospital, and a processing layer. Next, we describe the attributes of these three layers.

Table 1 Notations

Notations	Descriptions
P	Patient
Id_P	Identity of P
Bio_P	Fingerprint information of P
N	National hospital
C	Community hospital
D	Doctor
M	Database manager
B	Blockchain-based sharing platform manger
T	Transaction
t	Timestamps
$\|\|$	Concatenation
$\oplus$	Bitwise XOR operation
$Sig()$	Signature operation
$H()$	One-way hash function
$E()$	Encryption operation
$D()$	Description operation

- **Patient**: We consider a medical system where the data sharing request is initiated by the patient. In our design, patients are the owners of their medical data. The patient can allow authorized medical staff to access their medical data by the PKI mechanism. When a patient visits a hospital that can interact with the sharing system, he/she can check all personal medical details at that hospital, as well as his/her medical profiles at other hospitals.
- **Hospital layer**: In China, national and community hospitals are available. The patient can choose to treat their illness in any legal hospital. As shown in Fig. 1, there is an obvious superior-subordinate relationship between national hospitals and community hospitals. Unlike previous approaches, we fully use the hierarchical structure of the existing medical mechanisms. Different levels of medical institutions can undertake different medical tasks. A national hospital with the most experienced doctors is the main point of reference for the patient treatment. A community hospital (affiliated with a national hospital) is mostly responsible for basic checks and follow-up: this saves resources for the national hospital but also saves the patient's travel time required to see a doctor. In the system architecture diagram (Fig. 1), we listed the role of a database manager in charge of data storage in various hospitals. To ensure the security of the data sharing parties, as mentioned above, we need this role to summarize sensitive data before sharing.

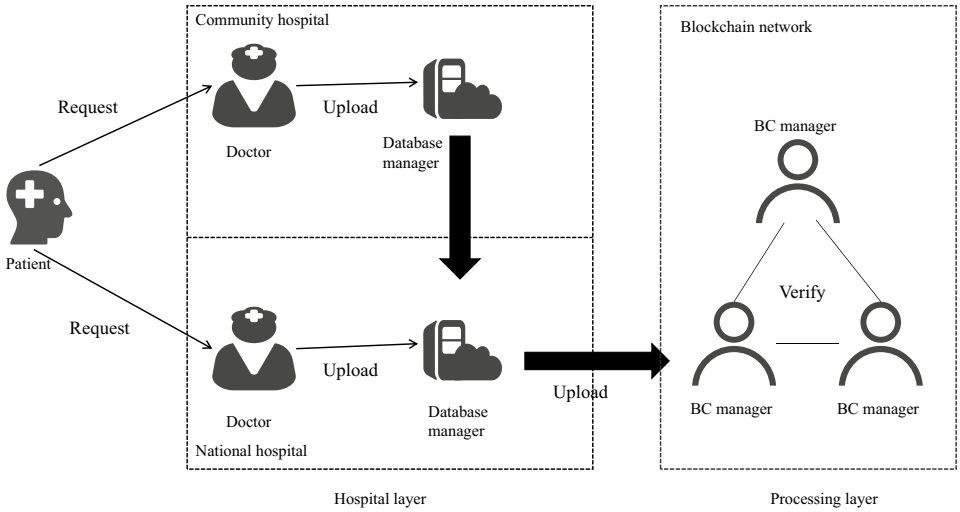

Fig. 1 Architecture of the proposed system

– **Processing layer**: The overlay design is a peer-to-peer network that is based on the blockchain architecture. In such a distributed architecture, each node represents a national hospital's sharing platform manager, and the communication between hospitals is completed through the transaction mechanism of blockchain (Le and Mutka 2018). As a globally interconnected public platform, the role of the blockchain network in this design is to integrate the interfaces of major national hospitals. This solution was chosen because a blockchain-based platform requires a certain energy consumption when running. As described in Fan et al. (2018), national hospitals with more resources should bear the sharing costs of the whole medical system. On the one hand, compared with community hospitals, the information given by national hospitals is more professional and authoritative. On the other hand, it is because the national hospitals have abundant resources and China has a large amount of financial support for them, they are more credible and enforceable in maintaining the consensus of blockchain and protecting data security. Platform representatives from major national hospitals have the same rights to constitute the blockchain platform and complete the information processing of the entire sharing platform together. Considering the security of data, we stipulate that only national hospitals with a high access level have the right to update data to the sharing platform, while community hospitals at a lower level can only perform conditional query operations on patients' medical data. As for the specific processes of data interaction between entities, we discuss them in the following section.

3.2 Platform initialization

Establishing a secure data sharing platform is the basis for our subsequent data sharing. As mentioned above, we divide the economic cost of establishing a shared platform among national hospitals. Thus, in this part, our main task is establishing a safe data sharing platform by the authoritative national hospitals. Some basic security rules have been agreed in advance, to ensure that only entities conforming to the rules can enter the blockchain sharing platform and act as the maintainer of the shared platform. Any entity access that does not conform to the rule definition is denied. The specific procedures for this approval are described as follows:

1. Each national hospital implements an identity registration to further become the primary responsible entity of the information sharing platform. Once the registration information of the state-owned hospital meets the requirements for the application defined by the state, the national hospital will become a node on the blockchain sharing platform through verification.
2. The first node has the right and obligation to verify the next node. Thus, once the information of the national hospital is registered, the platform manager will be treated as a strong authentication node, and activities such as "read," "modify," and "access" can be performed as in the previous node.
3. After a series of tests, various institutions and organizations form an alliance of stakeholders to jointly maintain the reliable operation of blockchain. To protect the privacy of information sharing, we assume that once the sharing platform is formed, the identity of the platform manager responsible for verifying information inside the platform cannot be changed. That is, we have a list of hospital members who have agreed to maintain the platform from the very beginning.

After the establishment of the sharing platform, we distribute platform tokens (address accounts) to every communications entity. Referring to the membership structure

of the medical system in Fig. 1, doctors of national hospitals and community hospitals are responsible for treating patients. Database managers of national hospitals and previously set platform managers, as entities that interact with the blockchain sharing platform, should be assigned transaction addresses for subsequent data sharing. Here, we do not assign a fixed address to the patient, because the patient is mobile and does not provide the energy resources required to maintain the shared platform. Patient access data must pass through the admitted hospital. Once the access token is allocated, it becomes the identity of the entity, and subsequent data sharing and storage need to be performed using the token. Each entity is assigned a list of tokens that contains all entities with a legal access. Meanwhile, each entity is assigned a pair of public and private keys to send and receive information. Based on the above facts, identity control can be effectively implemented to ensure the security of communication.

3.3 Storage authentication mechanism for the model

Medical data is very sensitive, because its security is related to the patient's economic situation and even life. Therefore, it is necessary to establish an access control mechanism to prevent illicit users from accessing the data. In the system, the patient who produces the case data is the sole owner of the medical data. When a patient is admitted to any hospital (national or community), registration is the first step. In this process, the system requires patients to provide their identity information Id_P and fingerprint information Bio_P. Identity information Id_P is the unique identification of every legal citizen, and fingerprint information Bio_P is unique for every citizen. Id_P information may be lost, but fingerprint information Bio_P will not. Therefore, in this system, we use the unique token $< Id_P, H(Bio_P) >$ to identify patients' ownership of their own medical data. The patient's data can be accessed only if the two types of identification are provided at the same time.

To successfully share the data, we first need to write the data to be shared to the blockchain-based data sharing platform. Here, we assume that the patient is first admitted to a national hospital N_i. The business process requires the collaboration of four roles: patient P, doctor D_{N_i}, database manager M_{N_i}, and blockchain-based sharing platform manager B_{N_i}. The processing is described as follows:

1. To register, patient P provides personal information (such as patient name, ID number, phone number, and fingerprint). This personal information will be uploaded to the national hospital database.
2. Doctor D_{N_i} generates identity token $X_P =< Id_P, H(Bio_P) >$ for patient P. Next, according to the patient's condition, doctor D_{N_i} also gives reasonable treatment suggestions D_P to the patient. Additionally, the patient's initial diagnosis will be recorded in the database as a log-on message.
3. After receiving information from the client, database manager M_{N_i} will integrate medical data $X_P \parallel D_P$ as usual. Afterwards, he/she extracts key diagnostic information (such as etiological diagnosis and treatment methods), following which he/she generates a diagnostic summary of the extracted information De_P for local platform manager B_{N_i}.
4. Platform manager B_{N_i} generates a transaction T_s for himself/herself and invokes the call-function to the local storage. The transaction is as follows:

$$Tx_1 =< X_P, De_P, address_{D_{N_i}}, sig_{B_{N_i}} >,$$

where

$$sig_{B_{N_i}} = SIG(SK_{B_{N_i}}, X_P, De_P, address_{D_{N_i}}).$$

3.4 Medical data sharing requirements for different scenarios

There are two kinds of situations when a patient will go to another hospital. One situation is when the patient's condition did not improve after he/she was hospitalized in N_i, so he/she should go to another equally authoritative national hospital N_{i+1} for an additional treatment. In this case, a second hospital N_{i+1} always needs to check the previous records in N_i. Importantly, previous medical records of the patient need to be consulted to make a more accurate diagnosis. Especially for complex diseases, previous treatment programs play a significant role in the ultimate cure of patients.

Another case is when the patient has recovered shortly after visiting a national hospital N_i and only needs to do basic checks in a community hospital C_{N_i}. As mentioned above, C_{N_i} is the affiliated hospital of N_i. By doing so, the coordination and cooperation between the upper- and lower-level hospitals (the national hospitals and their community hospitals) can greatly facilitate the timely treatment of patients. Additionally, it can greatly alleviate the serious shortage of medical resources in the national hospitals.

For both cases, details of data sharing are covered in the next two subsections.

3.4.1 Sharing requests come from peers

In this subsection, we illustrate how a national hospital N_i shares the requested data that belong to patient P with another national hospital N_{i+1}. As described in the previous section, when patient P visits the first national hospital, his/her medical data $X_P \parallel De_P$ have been stored on the

blockchain sharing platform according to the business process. Based on the above steps, the workflow of sharing the data between two hospitals of the same type is described in Fig. 2. Details are provided as follows:

1. As in the case of an initial visit to the first national hospital N_i, personal information needs to be updated when patient P is referred to the second hospital N_{i+1}. After an oral examination, $D_{N_{i+1}}$ in hospital N_{i+1} was informed that patient P had received an initial treatment in another national hospital N_i.
2. To further understand the patient's medical history, doctor $D_{N_{i+1}}$ needs to get the patient's previous medical records from the public information sharing platform. Therefore, the doctor asks patient P to provide the fingerprint information Bio_P as he/she entered in previous hospital N_i, to generate the same identity token $X =< Id_P, H(Bio_P) >$ as an index for information retrieval.
3. Doctor $D_{N_{i+1}}$ of the second national hospital using his/her own address token A_D generates a transaction $T_{D_{i+1}}$ for the local blockchain-based platform manager $B_{N_{i+1}}$. The message format is as follows:

$$T_{D_{i+1}} = E_{P_B}(X) \parallel Sig_{S_D}(h(X)) \parallel t_{i+1},$$

where P_B is the public key of platform manager $B_{N_{i+1}}$ for national hospital N_{i+1}, and S_D is the private key of doctor $D_{N_{i+1}}$.

4. After receiving $T_{D_{i+1}}$, platform manager $B_{N_{i+1}}$ will verify the validity of the data request $T_{D_{i+1}}$ by calculating $D_{S_B}(E_{P_B}(X))$ and $D_{P_D}(Sig_{S_D}(h(X)))$, getting X,$h(X)$ and recalculating $X^* = X \parallel A_D$. If request $T_{D_{i+1}}$ is from the local doctor, platform manager $B_{N_{i+1}}$ will generate a new transaction $T_{B_{i+1}}$ for platform manager B_{N_i} of national hospital N_i. Transmitted information $T_{B_{i+1}}$ not only contains the ownership identification for patient P, but also includes address A_D of the requesting doctor $D_{N_{i+1}}$. The message format is as follows:

$$T_{B_{i+1}} = E_{P_B}(X^*) \parallel Sig_{S_D}(h(X^*)) \parallel t_{i+1}.$$

5. When receiving data request $T_{B_{i+1}}$ from adjacent nodes $B_{N_{i+1}}$, information owner B_{N_i} will search for the records of patient P as follows: if

$$< Id_P, H(Bio_P) >_{T_{B_{i+1}}} ==< Id_P, H(Bio_P) >_{Tx_1}$$

then platform manager B_{N_i} will regard $T_{B_{i+1}}$ as a legal request and will generate a response for address A_D:

$$T_{B_i} = E_{A_D}(De_P) \parallel Sig_{S_B}(h(De_P)) \parallel t_i,$$

where De_P contains a summary of the patient's previous visits.

After checking the patient's treatment records, doctor $D_{N_{i+1}}$ in national hospital N_{i+1} will give the patient a reasonable therapeutic schedule based on the comprehensive analysis of this history. To ensure the reusability of the information, as mentioned above, doctor $D_{N_{i+1}}$ will perform the same operation as the previous national hospital N_i.

3.4.2 Share requests come from subordinates

Here, we discuss the second case of data sharing: patient P has already received a proper treatment in the national hospital N_i and, to save time, follow-up basic examinations need to be conducted in community hospital C_{N_i} of national hospital N_i. To have a comprehensive understanding of the patient's situation, community hospital C_{N_i} needs to make a data sharing request to their superior national hospital

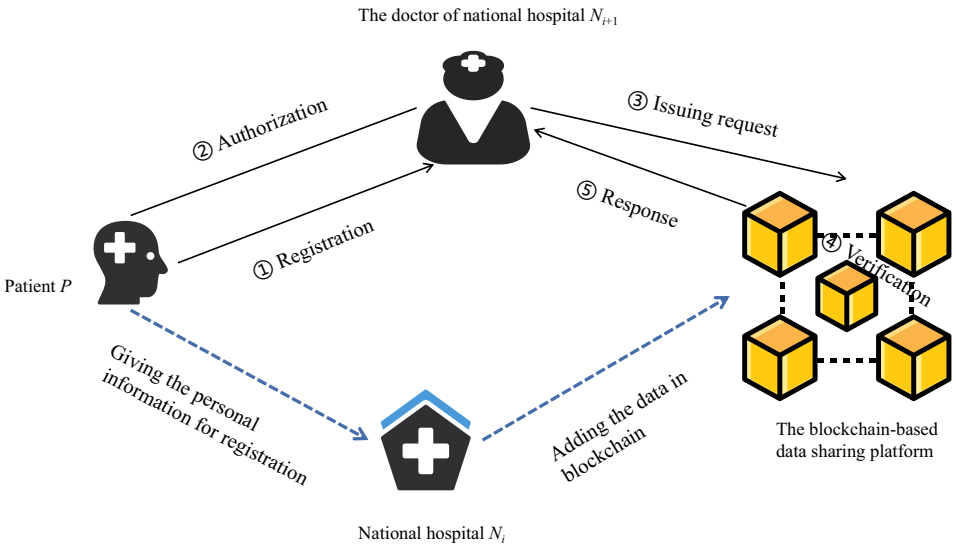

Fig. 2 Data exchange among national hospitals at the same level

N_i. Unlike for the data sharing process between national hospitals (which are of the same level), considering the limitations of the resources and qualifications of subordinate hospitals, we only discuss the data sharing between superior and subordinate hospitals, without considering the data sharing between different affiliated hospitals. The data sharing workflow is described as follows:

1. After an interview, doctor D_{C_i} in the community hospital has learned that patient P has received treatment in superior hospital N_i and only requires basic tests during this visit. To understand better what kind of follow-up examination the patient needs, it is necessary to know the patient's previous medical records in hospital N_i. As discussed in the last section, identity token $X_P =< Id_P, H(Bio_P) >$ of patient P is the key information. Patient P provides the identity information Id_P and fingerprint information Bio_P to the doctor at community hospital C_{N_i}, making it easier for the doctor to see their previous visits.
2. When granted access, doctor D_{C_i} at affiliated hospital C_{N_i} will calculate new transaction information $Q = X \parallel R_i$ and generate transaction information to the superior node N_i as follows:

$$T_{C_i} = E_{P_{B_{N_i}}}(Q) \parallel Sig_{S_C}(h(Q)) \parallel t_i,$$

where R_i is the code number of community hospital C_{N_i} at national hospital N_i and $P_{B_{N_i}}$ is the public key of platform manager B_{N_i} for parent national hospital N_i.
3. When a data sharing request T_{C_i} is received from a lower authority, platform manager B_{N_i} in national hospital N_i does two things to validate the request. First, he/she will calculate $D_{S_B}(E_{P_{B_{N_i}}}(Q))$ and get the called data token X for the patient and R_i for the community hospital. Then, B_{N_i} will check the code number list U of local subset hospitals to confirm the authenticity of the request. Importantly, the platform manager also checks signature information $Sig_{S_C}(h(Q))$ to prevent someone from making a request to an affiliated hospital in a malicious way. If both verifications pass, manager B_{N_i} of national hospital N_i will pass medical record De_P to doctor D_{C_i} in the community hospital.

After consulting the patient's history De_P obtained from the superior hospital, doctors in community hospitals can understand the condition of patient P better.

4 Performance evaluation

In this section, we will discuss the security and efficiency of our schedule.

4.1 Security analysis

Here, we discuss how our system meets the security requirements listed above through a counter-proof. As for the basic security requirements (such as confidentiality and integrity), we list them in Table 2.

Theorem 1 *Assume the integrity of the blockchain architecture mechanism and the uniqueness of the input and output of the hash function. Our system can guarantee the security of data sharing in the distributed system.*

Proof In our system, we use the transaction mechanism inherent to blockchain as a carrier of medical data sharing. Generally, an effective transaction consists of addresses of two communicating parties, shared content, unique signature, and hash value. If the addresses or content are modified, the original signature will become invalid because of the existence of a digital signature. If the hash value is changed by anyone, the miner in the blockchain-based sharing platform will find the change, because the blocks responsible for storing the data are connected by hash functions one by one. Thus, any modification will be discovered, and our blockchain-based distributed architecture ensures that medical data of patients is shared without modification attacks. □

Theorem 2 *Assume that the patient's fingerprint information Bio_P cannot be easily obtained by illegal users and hash operations $h(.)$ are unique and irreversible. Our system can*

Table 2 Basic security requirement evaluation

Requirement	Model solution	Reference
Confidentiality	Unique blockchain-based address mechanism	Section 3.2
Integrity	Hashing of data blocks	Section 3.1
Availability	Thanks to the cross-domain features of blockchain	Section 3.2
Authorization	Use of the PKI encryption mechanism	Sections 3.4 and 3.5
User control	Uniqueness of user's biological information	Section 3.3
Anonymity	Unique blockchain-based address mechanism	Section 3.2

ensure that patients own their personal data during the whole process of medical data sharing and can achieve a necessary access at any time.

Proof In our system, patient P controls the access to their medical data by unique token $< Id_P, H(Bio_P) >$. If any attacker wants to impersonate patient P on the data sharing platform to obtain the patient's personal medical information or authorize other illegal users to access the patient's data, he/she needs to have both patient identity information and fingerprint information. However, we know from Theorem 1 that the individual patient's biological characteristics are unique and almost impossible to obtain illegally. Therefore, it is impossible for an attacker to impersonate a patient to access the patient's data or authorize other illegal users to access it. In other words, patient P has the highest level of ownership of their own personal data. □

Theorem 3 *Assume that each entity (doctor D_{N_i}, database manager M_{N_i}, and platform manager B_{N_i}) in hospital N_i has an access to the shared platform and locally holds the address communication information and public key information of other participants. Our system can provide a convenient data sharing platform whilst protecting the safety of individual data sharers.*

Proof As described above, for a doctor from a national hospital (at the same level) or for a doctor from a community hospital (that is affiliated to a superior hospital), data sharing relies on the P2P network based on the blockchain for transmission, and the use of the address mechanism ensures a direct access to information and will not be counterfeited. Thus, if an attacker wants to impersonate a hospital doctor to access data from a blockchain platform, he/she needs to generate a transaction locally to transmit his/her information. The format of the transaction is shown below:

$$Tn = (addressfrom, siganature, content, hash),$$

where

$$signature = (SK_{sender}, addressfrom, content, hash).$$

However, private key SK_{sender} is securely stored locally by the sender. Thus, it cannot be stolen by any intermediary. Therefore, the attacker cannot generate a legal transaction on behalf of a certified doctor to issue a request to sharing medical data. Moreover, unlike in previous approaches, in our system, we did not authorize distributors to directly access each other's databases, but preprocessed abstracts of data locally. Hence, only the patient's copy of information can be shared in the blockchain-based platform, thus ensuring the individual safety of the medical institutions at all levels. □

4.2 Feasibility analysis

caption For a medical data sharing platform proposed in our scheme, scalability is important to measure when estimating the feasibility of the system.

As mentioned above, each block consists of a block header and a block body. Among them, the block header size is approximately 75 bytes, and the block body contains the transaction information. According to the statistical results of the simulation experiment, the size of a valid transaction is approximately 250 bytes. In the blockchain system, the number of transactions that can be accommodated in a block can be set by oneself. In our system, we assume that 30 transactions can be accommodated in a block. On this basis, we can calculate the size of a block: $250 \times 30 + 75 = 7535$ bytes = 7.36 KB.

Consider a data-sharing platform with 1,000 users and the transaction threshold of 100 users per second. Then, the size of the blockchain network is 735.8 KB/s, 43.1 MB/min, 2.5 GB/h, and 0.15 TB/day. Calculations are shown below:

- $100 \times (7535 \times 1) = 753500$ bytes/s = 735.8 KB/s
- $100 \times (7535 \times 60) = 45210000$ bytes/s = 43.1 MB/min
- $100 \times (7535 \times 60 \times 60) = 2712600000$ bytes/s = 2.5 GB/hour
- $100 \times (7535 \times 60 \times 60 \times 60) = 162756000000$ bytes/s = 0.15 TB/day

For a given period of time, we can infer the total amount of data in the system as in the example above. Table 3 shows the data growth of the system over ten years. According to our results, the storage capacity required by our system is completely within the range of medical storage, which further explains the feasibility of our system.

Table 4 compares the performance of our system and other existing blockchain-based systems for medical data sharing. For our system, we designed the architecture for scenarios of the data sharing between the-same-level hospitals and the data sharing between the upper- and lower-level hospitals, to make the patient identity management more

Table 3 Total amount of system data in a fixed time

Transaction	Per second	Per hour	Per day	Per year	Per 10 years
1000	7.19 MB	25.28 GB	606.72 GB	216.26 TB	2.11 PB
5000	35.95 MB	126.4 GB	2.96 TB	1081.3 TB	10.56 PB
10000	71.9 MB	252.8 GB	5.92 TB	2.11 PB	21.12 PB
50000	359.5 MB	1264 GB	29.6 TB	10.56 PB	105.6 PB
100000	719 MB	2528 GB	59.2 TB	21.12 PB	211.19 PB

Table 4 Comparison of the proposed system and existing systems

References	Block-chain-based	Cat-egorizing requests	Privacy for data sharers	Scalability
Zyskind et al. (2015)	Y	N	Y	N
Yue et al. (2016)	Y	N	Y	N
Mettler (2016)	Y	N	N	Y
Azaria et al. (2016)	Y	N	N	Y
Xia et al. (2017)	Y	Y	N	Y
Fan et al. (2018)	Y	Y	N	Y
The proposed system	Y	Y	Y	Y

simple and clear. In addition, to ensure the safety of individual hospital data, we conducted a secondary processing on the data. This will not only ensure the security of the individual database, but also greatly reduce the storage burden of the blockchain sharing platform. The table shows that we consider the security of individual hospital databases while resisting various attacks. In addition, we also consider the identity management of patients. After a comprehensive analysis, we conclude that our scheme is more advantageous than other schemes.

5 Conclusion

Data sharing and data access are constant requirements of modern electronic medicine. However, different hospitals protect the security of their own data and use different encryption methods to encrypt their medical data. It is a problem that the medical records of the same patient are fragmentally stored in different locations. This approach seriously limits the interoperability of medical data. In this paper, we proposed a blockchain-based schedule in two scenarios (for national hospitals of the same level and between a national hospital and a community hospital) to share data of the same patient in a novel sharing platform. Unlike previous systems, we extract and preprocess the source data before sharing (thus, we share a copy of the data instead of the source data itself). Compared with other blockchain-based systems, our system satisfies the security requirements of data sharing itself and alleviates the concerns of medical institutions, as data sharing may affect their privacy and security. In the subsequent analysis of the system, the feasibility of the proposed system was examined.

Given the unique security and cross-domain nature of blockchain technology, it is considered an important tool to change human labor relations. At present, the research on the applicability of blockchain technology to traditional business is still ongoing. With the development of computer communication technology and people's attention to security and privacy, it is believed that more application scenarios will be implemented in the future blockchain.

Funding Not applicable.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

Axelsson R (2000) The organizational pendulum: healthcare management in Sweden 1865–1998. Scand J Public Health 28(1):47–53

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

Chen G, Bing X, Manli L, Chen N-S (2018) Exploring blockchain technology and its potential applications for education. Smart Learn Environ 5(1):1–10

Chen C-M, Deng X, Gan W, Chen J, Islam SKH (2021a) A secure blockchain-based group key agreement protocol for iot. TJ Supercomputi: 1–23

Chen J, Gan W, Muchuang H, Chen C-M (2021b) On the construction of a post-quantum blockchain for smart city. J Inform Secur Appl 58:102780

Fan K, Wang S, Ren Y, Li H, Yang Y (2018) Medblock: efficient and secure medical data sharing via blockchain. J Med Syst 42(8):136

Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst 42(7):1–7

Hsiao J-H , Tso R, Chen C-M, Wu M-E (2017) Decentralized e-voting systems based on the blockchain technology. In: Advances in Computer Science and Ubiquitous Computing, pages 305–309. Springer,

Huang G, Liu X, Ma Y, Xuan L, Zhang Y, Xiong Y (2016) Programming situational mobile web applications with cloud-mobile convergence: an internetware-oriented approach. IEEE Trans Serv Comput 12(1):6–19

Kish LJ, Topol EJ (2015) Unpatients-why patients should own their medical data. Nat Biotechnol 33(9):921

Koufi V, Malamateniou F, Vassilacopoulos G (2010) Ubiquitous access to cloud emergency medical services. In: Proceedings of the 10th IEEE International Conference on Information Technology and Applications in Biomedicine, pages 1–4. IEEE

Kuo T-T, Ohno-Machado L (2018) Modelchain: decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. arXiv preprint arXiv:1802.01746

Le T, Mutka MW (2018) Capchain: a privacy preserving access control framework based on blockchain for pervasive environments. In: 2018 IEEE International Conference on Smart Computing (SMARTCOMP), pages 57–64. IEEE

Lin B, Huang Y, Zhang J, Junqin H, Chen X, Li J (2019) Cost-driven off-loading for dnn-based applications over cloud, edge, and end devices. IEEE Trans Ind Inform 16(8):5456–5466

McGhin T, Kim-Kwang RC, Charles ZL, Debiao H (2019) Blockchain in healthcare applications: research challenges and opportunities. J Netw Comput Appl 135:67–75

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), pages 1–3. IEEE

Shamshad S, Mahmood K, Kumari S, Chen C-M et al (2020) A secure blockchain-based e-health records storage and sharing scheme. J Inform Secur Appl 55:102590

Sharma PK, Mu-Yen C, Jong HP (2018) A software defined fog node based distributed blockchain cloud architecture for iot. IEEE Access 6:115–124

Thilakanathan D, Chen S, Nepal S, Calvo R, Alem L (2014) A platform for secure monitoring and sharing of generic health data in the cloud. Fut Gen Comput Syst 35:102–113

Tsang YP, Choy KL, Chun HW, Ho GTS, Lam HY (2019) Blockchain-driven iot for food traceability with an integrated consensus mechanism. IEEE Access 7:129000–129017

Wang E, RuiPei S, Chien-Ming C, Zuodong L, Saru K, Muhammad KK (2020) Proof of x-repute blockchain consensus protocol for iot systems. Comput Secur 95:101871

Wörner D, von Bomhard T (2014) When your sensor earns money: exchanging data for cash with bitcoin. In: Proceedings of the 2014 ACM International Joint Con- ference on Pervasive and Ubiquitous Computing: Adjunct Publication, pages 295–298. ACM, 2014

Xia Q, Boateng SE, Omono AK, Gao JD, Xiaojiang GM (2017) Medshare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 5:14757–14767

Yang J-J, Li J-Q, Niu Y (2015) A hybrid solution for privacy preserving medical data sharing in the cloud environment. Fut Gen Comput Syst 43:74–86

Yavari M, Safkhani M, Kumari S, Kumar S, Chen C-M (2020) An improved blockchain-based authentication protocol for iot network management. Secur Commun Netw. https://doi.org/10.1155/2020/8836214

Yeh K-H, Chunhua S, Hou J-L, Chiu W, Chen C-M (2018) A robust mobile payment scheme with smart contract-based transaction repository. IEEE Access 6:59394–59404

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 P, White J, Schmidt DC , Lenz G (2017) Applying software patterns to address interoperability in blockchain-based healthcare apps. arXiv preprint arXiv:1706.03700

Zhu H, Wang X, Chen C-M, Kumari S (2020) Two novel semi-quantum-reflection protocols applied in connected vehicle systems with blockchain. Comput Elect Eng 86:106714

Zyskind G, Nathan O, et al. (2015) Decentralizing privacy: Using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops, pages 180–184. IEEE