Journal of Medical Systems (2019) 43: 5
https://doi.org/10.1007/s10916-018-1121-4

PATIENT FACING SYSTEMS

Blockchain-Based Medical Records Secure Storage and Medical Service Framework

Yi Chen [1,2] · Shuai Ding [1,2] · Zheng Xu [3] · Handong Zheng [1,2] · Shanlin Yang [1,2]

Received: 13 June 2018 / Accepted: 8 November 2018 / Published online: 22 November 2018

Abstract

Accurate and complete medical data are one valuable asset for patients. Privacy protection and the secure storage of medical data are crucial issues during medical services. Secure storage and making full use of personal medical records has always been a concern for the general population. The emergence of blockchain technology brings a new idea to solve this problem. As a hash chain with the characteristics of decentralization, verifiability and immutability, blockchain technology can be used to securely store personal medical data. In this paper, we design a storage scheme to manage personal medical data based on blockchain and cloud storage. Furthermore, a service framework for sharing medical records is described. In addition, the characteristics of the medical blockchain are presented and analyzed through a comparison with traditional systems. The proposed storage and sharing scheme does not depend on any third-party and no single party has absolute power to affect the processing.

Keywords Medical data · Blockchain technology · Medical data sharing · Medical data storage · Medical service

Introduction

Those who have ever visited more than one hospital have likely experienced undergoing a medical examination that was previously performed at another hospital [1]. This phenomenon is caused by the fact that medical data are mainly managed by medical institutions, and there are strict restrictions and regulations on policies and for the transfer and sharing of important personal information, such as medical records. Medical data is scattered throughout various medical institutions, and the data standards of different medical institutions are not uniform, resulting in a low level of interoperability of medical information systems among agencies. In addition, the subjects that can handle medical data are limited. In addition to the patient's request to transfer and view his or her personal medical record, in principle, medical data transfer and sharing outside the medical institution are not allowed. All of these cause the exchange and sharing of medical data to be very difficult, which seriously hinders its effective.

Under the current medical data management system oriented by medical institutions, there is no guarantee of the integrity and reliability of patient data. The risks of medical data loss or hacking is inevitable, and these data are always facing data security, personal privacy leaks and other issues. Most medical data are stored in medical institutions in a centralized manner, which is vulnerable to different threats, such as malicious tampering, hacking and natural disasters, which can lead to the leakage and loss of medical data. In June 2017, according to a British "Daily Telegraph" report, the Cosmetic Institute in Bondi Junction posted information on patient names, addresses, medical insurance numbers and medical

This article is part of the Topical Collection on *Patient Facing Systems*

✉ Shuai Ding
dingshuai@hfut.edu.cn

✉ Zheng Xu
juven_xz@163.com

Yi Chen
chenyihfut@163.com

Handong Zheng
zhdhfut@163.com

Shanlin Yang
yangsl@hfut.edu.cn

[1] Present address: School of Management, Hefei University of Technology, Hefei 23009, Anhui, China

[2] Key Laboratory of Process Optimization and Intelligent Decision-Making (Ministry of Education), Hefei University of Technology, Hefei 23009, Anhui, China

[3] Present address: The Third Research Institute of the Ministry of Public Security, Shanghai 201142, China

records online, resulting in exposure of patient data and privacy. In October 2017, approximately 47GB of medical data stored by a medical institution on the Amazon database was accidentally opened to the public, with an initial estimate of at least 150,000 patients affected.

With the increased demand for personal health management, various health service institutions hope to gather health information through medical data exchange and sharing. Examples of these efforts include the Blue Button Connector [2], a US government led project, Apple's Mobile Healthcare Application [3], and Google Health (https://health.google.com/health/). However, these solutions have not yet satisfied the requirements for an ideal healthcare information system, such as security, reliability, and transparency [1]. Hence, a management scheme with decentralization, verifiability, and immutability characteristics is need for personal medical data.

Blockchain offers a promising new distributed framework to amplify and support integration of health care information across a range of uses and stakeholders [4]. The unique advantages of real-time recordings and tamper-resistance of the blockchain can be reflected in the field of healthcare. Data captured on the blockchain can be shared in real time across a group of people and organizations. Each event or transaction is time stamped and becomes part of a long chain or permanent record that cannot be tampered with afterwards. On the nonpermissive blockchain, all parties can view all records. On a permissive blockchain, privacy can be protected by agreeing on where and by whom to look for deals and hiding the identities of all parties. Thus, the blockchain turns the different information held by a single owner into the entire history of the asset.

Blockchain technology presents numerous opportunities for health care; however, it is not a fully mature technology today nor a panacea that can be immediately applied [4]. The management of personal medical data and service patients based on blockchain technology is an issue to still to be solved. In this study, we designed a storage scheme to manage personal medical data on a blockchain storage system. The key contributions of this work are as follows. 1) We propose a storage scheme for medical data based on blockchain technology to achieve the safe storage and sharing of personal medical data. In the scheme, we describe the permissions of three types of transaction bodies and design the block structure and the main function of the medical blockchain. 2) We introduce a service framework for sharing medical records to describe the process of personal medical data management in some applications. A blockchain-based personal medical data application can provide a patient medical information service without violating privacy policies. 3) The characteristics of the medical blockchain are described, and a comparison to traditional systems from different aspects is analyzed. The medical blockchain does not depend on a trusted third party, it is the establishment of a system in which patients have their own complete personal medical data, and it can achieve secure storage, privacy protection and tamper-proofing.

The structure of the paper is as follows. The "Related work" section of this paper discusses the existing literature related to this topic. The "Blockchain-based medical data storage and service" section presents the storage scheme of medical data and a service framework based on blockchain technology. The "System analysis" section contains the characteristics of a medical blockchain and a comparison to traditional systems. The "Conclusion" section summarizes the paper and discusses future work.

Related work

Health information technology is widely considered to be a part of the solution to improving the productivity and safety of healthcare [5–7]. Health information technology has increased accessibility of health and medical data and benefited medical research and healthcare management [8–12]. Currently, many medical institutions are outsourcing their repositories to the cloud. To provide a more convenient service and environment for medical services, various solutions regarding cloud service technology and management have been proposed [13–19]. However, security and privacy are rising concerns in the storage and sharing of medical data in a cloud service environment. To ensure the security and privacy of patients' medical data, proposed data storage solutions include a privacy-preserving smart IoT-based healthcare big data storage system [20], a solution for sharing sensitive data based on a nonstandard diagonal data aggregation method [21], a cloud-based data sharing model [22], a hybrid solution [23, 24], a scalable privacy-enabled architecture and a context-aware privacy-preserving scheme [25], a security model using a fog computing facility [26], and a distributed architecture with double-phase microaggregation [27]. However, most of these solutions rely on a fully trusted third party. Users usually do not believe that the third party is doing a good job of keeping their data confidential.

Blockchain technology acts as a shared decentralized ledger to record transactions. It can be used to record events as products or subject experiences from its origin to the current state in an unalterable log [28–30]. Blockchain has the characteristics of decentralization, verifiability and immutability, which are essential in the medical and healthcare industry, especially in managing of medical records. Blockchain applications and research in healthcare have attracted much attention; many research institutions around the world are involved in the push towards blockchain solutions. Healthbank is a global innovator in digital health, it is actively exploring

options to tap into blockchain such as smart contracts [31]. Gem Health is a provider of enterprise blockchain solutions, it partnered with Philips Blockchain Lab to leverage blockchain technology to address the trade-off between patient centric care and operational efficiency by creating a healthcare ecosystem connected to universal data infrastructure [32]. The potential uses of blockchain technology in healthcare are multiple, and the exponential growth of blockchain technology applications can benefit population health and medical records.

In addition, relevant studies about blockchain in healthcare have appeared in succession. Existing research in the blockchain for the healthcare field mainly includes medical information protection, medical data storage and sharing, medical data application, forecast analysis, etc. Mettler [33] illustrated possible influences, goals and potentials connected to blockchain technologies in healthcare. Yue et al. [34] proposed an App (Healthcare Data Gateway) based on the blockchain. The architecture not only enabled the patient to own, control and share their own data easily and securely but also enabled untrusted third parties to process medical and health data while ensuring patient privacy through introducing secure multifactor computing. Shrier et al. [35] proposed using the Massachusetts Institute of Technology's OPAL/Enigma encryption platform that works with blockchain technology to create a secure environment for storing and analyzing medical data. Some methods [36, 37] and systems [38, 39] based on the blockchain are proposed for storing and managing patient medical records. Xia et al. [40] proposed a blockchain-based data sharing framework that sufficiently addresses the access control challenges associated with sensitive data stored in the cloud using immutability and built-in autonomy properties of the blockchain. Peterson et al. [41] presented a blockchain-based approach to sharing patient data. Kuo et al. [42] used blockchain network technology to create an interinstitutional medical health prediction model.

Blockchain-based medical data storage and service

The storage scheme of medical data

The storage scheme of medical data uses blockchain technology and cloud storage technology to achieve safe storage and sharing. The architecture of the medical blockchain is shown in Fig. 1. Medical institutions, patients and third-party agencies (such as medical information service platform, medical insurance company, etc.) are three main types of transaction bodies in the medical blockchain. Medical institutions are responsible for the diagnosis and treatment of patients and generating their medical records. Patients can visit a doctor in different medical institutions and have

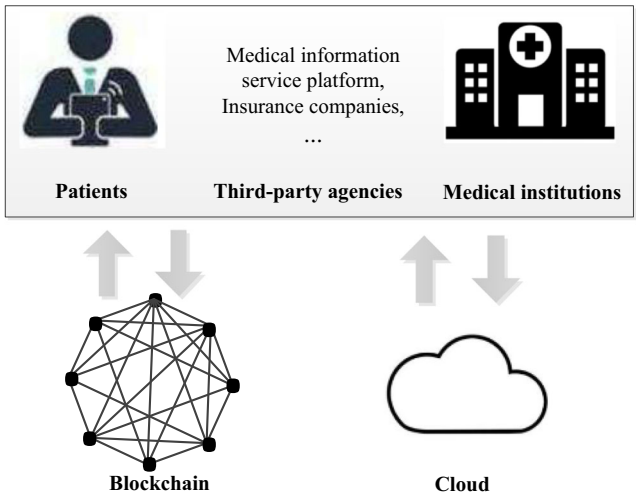

Fig. 1 The architecture of the medical blockchain

ownership and control over their personal medical data. The third-party agencies can provide some services, such as medical institution recommendation and appointment registration. Different types of transaction body have different permissions. The permissions for the three types of transaction bodies are shown in Table 1.

Data storage and access control are the main transactions in the medical blockchain. It would be optimal to be able to hold all medical data on the blockchain, but due to practical constraints such as cost, storage capacity, only index information of medical data and transaction records are recorded onto the blockchain. Large medical data should be encrypted and saved outside of the blockchain. In our scheme, these medical data are stored in cloud storage under the chain. Access control is determined by permission, and different transaction entities have different access control permissions. In the medical blockchain, the right to use personal medical data is entirely controlled by the patient, the patient may grant a subject access to the relevant data. The patient can also withdraw their authorization in time.

The medical blockchain is responsible for generating creation blocks. The newly generated blocks by network nodes are first validated and then added to the main chain to form a permanent preservation of the transaction data. The timestamp is used to ensure the blocks follow the timing link in the medical blockchain. The data in the blockchain have not been tampered through the hash function, and identity authentication can be achieved with a public key encryption. The combinations of these technologies ensure the medical blockchain safety and security. The block structure of the medical blockchain is a Merkle Tree-based structure and is designed as shown in Fig. 2.

In the medical blockchain, the main functions are the release, preservation and sharing of medical data.

Table 1 The permissions of the three types of transaction bodies

	Patients	Medical institutions	Third-party agencies
Read/write access to itself medical data	Have permission	Have permission	Have permission
Read access to others medical data	Default does not have permission, you can get permission with the consent of the account owner.	In special circumstances such as an emergency, medical data can be read without authorization. In general, the default is only allowed if the account owner agrees.	Default does not have permission, you can get permission with the consent of the account owner
Write access to others medical data	Default does not have permission, you can get permission with the consent of the account owner.	Default does not have permission, you can get permission with the consent of the account owner.	Default does not have permission, you can get permission with the consent of the account owner.

- *Medical data release*. When a patient visits a medical institution, the doctor generates medical records or examination reports for the patient. When the medical data are generated, the physician generates the digest and hash of the medical data and posts them to the blockchain after signing in with the issuer's private key. At the same time, the medical data are encrypted with a symmetric key and encryption key of the medical data encrypted with the patient's public key. Both of them are sent to the patient together.
- *Medical data storage*. After receiving the data from the medical institution, the patient verifies the signature of the institution, then uses its own private key to decrypt the medical data encryption key, the original medical data and the signature, and then generates a new encryption key to store the medical data and its signature in the cloud storage.
- *Medical data sharing*. The usage rights of the medical data are completely controlled by the user himself, and the patient can authorize the third-party agency to access some of his or her medical data through the access control mechanism and can withdraw his or her authorization at any time. The location, usage rights and expiration date of the shared records in the cloud storage and the decryption key of the third-party agency write into the medical blockchain, and cloud storage management will set the access control policy.

A service framework for sharing medical records

Traditionally, medical institutions keep the records of patients [43]. The sharing of medical data is one essential step to make the medical system smarter and improve the quality of medical services [34]. It can help patients become active participants [44, 45], improve service quality [46] and give better recommendations for patients and physicians [47].

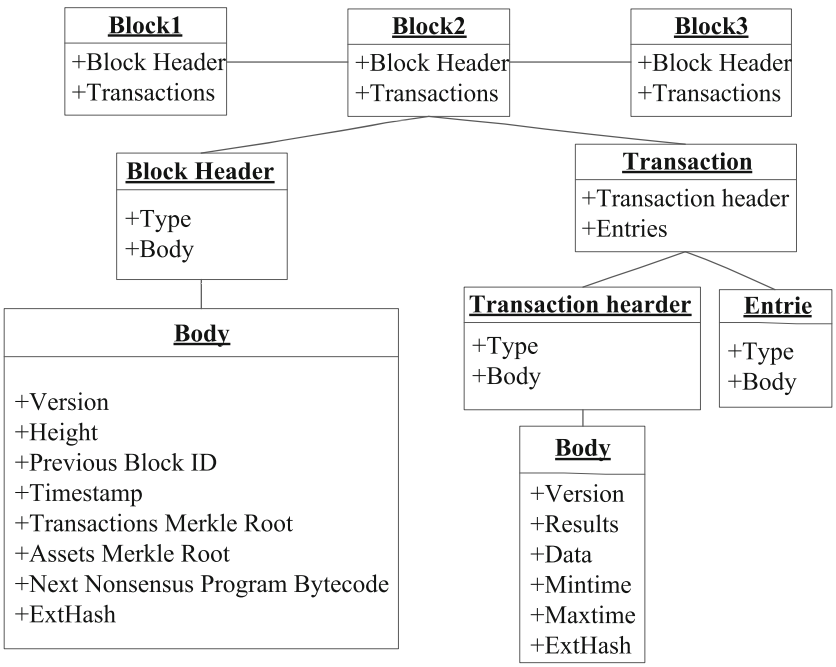

Fig. 2 The block structure of the medical blockchain

Blockchain technology helps medical institutions, patients, and service providers quickly and securely authenticate permissions for free data access and sharing. Based on blockchain technology, personal medical data can be obtained quickly and accurately, and patients will receive better service. Therefore, we design a service framework for personal medical data sharing and access control based on the blockchain technology. Figure 3 outlines the process of our service framework.

(1) Personal medical data management

First, each person has a digital archive that contains personal medical data. The storage and access of the digital archive are realized through blockchain technology, and each person has access control rights of their own information. Accessible and safety electronic information can be more conveniently and rapidly integrated into the routine diagnosis and treatment work of medical institutions. The standardization and digitization of various records enable the sharing of information among medical institutions, patients and service providers.

Second, personal medical data management rights are completely controlled by the user. A service provider makes a request to the patient to access and collect personal medical data when the service provider has a need. The individual may authorize the service provider to access part of his or her medical records and can withdraw the service provider's right at any time.

(2) Personal medical data application

Personal medical data is very valuable. There are many applications for these data; the data are not only used for diagnosis but also to provide a better choice of doctor. For example, the number of Chinese hospital visits reached 7 billion in 2017. The bigger the medical institution, the more crowded it is. Because of the lack of information, people do not know how to choose a medical institution to seek medical treatment in China. They often choose to go to the largest hospital around them for medical treatment. It is a common phenomenon for a patient to face issues of long waiting times for registration, treatment and receiving medicine after arrival at the hospital. It is very important to guide patients to seek treatment in different grade medical institutions according to their conditions.

Blockchain-based personal medical data applications can provide a patient medical information service without violating privacy concerns. Currently, there are many medical service platforms in China that help patients make an appointment before going to a medical institution. Due to the lack of medical data sharing, they cannot effectively guide different patients to different medical institutions. However, blockchain-based personal medical data sharing and access control can play an important role in the field of medical services. For example, if someone feels sick and wants to go to a medical institution, he or she authorizes his or her medical data (such as age, gender, home address, individual symptoms, medical records, treatment preferences, etc.) to a medical service provider for a better recommendation of medical institution without risking patient privacy.

System analysis

The characteristics of the medical blockchain

The medical blockchain is the establishment of a system in which patients have their own complete personal medical data, the storage and sharing of medical data between patients, medical institutions and third-party agencies in the system are safe and reliable. The ideal characteristics of the medical blockchain include patient ownership, storage security, privacy protection, tamper-proof and convenient interoperability.

The medical blockchain provides a distributed and decentralized way to store and manage medical data. This approach breaks the information island of traditional medical information systems, enabling patients to concentrate on their own medical data scattered in different medical institutions. Patient gives full control of his or her personal medical data. Others have to make a request and get the appropriate permission before they access the patient's relevant medical data. The patient can also withdraw their authorization at any time.

Data storage security is an important characteristic of the medical blockchain. The secure storage of the medical data is analyzed from three aspects of public information, data generation and data reception. The public information of medical data, such as store address, the hash value and permission of medical data, are recorded onto blocks. This public information is visible but cannot be tampered with. Using hash algorithms to process data generated by medical institutions, the hash value is signed, and the patient's record and signature are used to encrypt the patient's public key. These data are stored in the cloud storage under the chain. The patient obtains the hash and signature of medical institutions' record by decrypting the ciphertext with his private key. Then, the new record is encrypted and added to the existing record. These mechanisms ensure the authenticity of medical data sources, the security of medical data transmission and storage.

Patients are currently participating in transactions on the blockchain anonymously for privacy protection. Users can generate different public and private key pairs for each transaction. Medical records are encrypted and stored in cloud storage under the chain. One cannot decrypt the plaintext information of the medical data without the patient's encryption key. Therefore, it is not possible to obtain any real data about the medical data from the public information of the medical

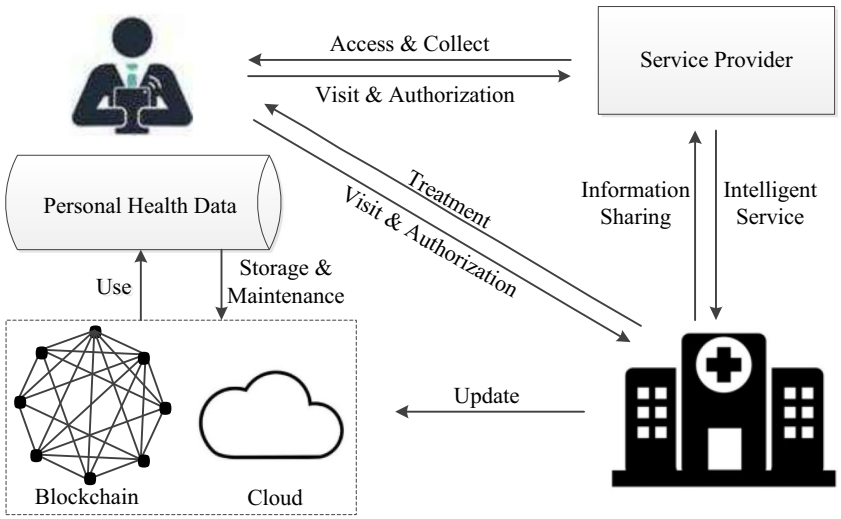

Fig. 3 A medical service framework based on blockchain technology

chain, thus protecting privacy of the patient. The control authority is in the hands of the patient. Patients can authorize certain data to an entity and can revoke their access rights at any time.

Medical data is arranged on the blockchain by time. Each block holds a hash of the previous block. and the data cannot tamper with once they are written into the blockchain. The hash of the medical data is stored in the medical blockchain. Any change to the original data will cause its hash value to change, which ensures that the medical data cannot be modified. The medical blockchain will transparently provide information on when, where and for what purpose the healthcare information was used. Access to all medical records on the medical blockchain is managed by the person, which prevents malicious access to medical information from the source.

Convenient interoperability is also an important feature of the medical blockchain. The medical blockchain not only allows for storing medical data by medical institutions but also stores data from some medical service providers. Integrated medical data can be used extensively for treatment at medical institutions and services from third-party agencies. Different users can easily access medical data in the medical blockchain anywhere through the Internet.

Comparison to traditional systems

Attribute-based encryption (ABE) and key-aggregate cryptosystem (KAC) are typical cryptographic for data sharing in cloud storage. Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes, it is recommended by the Cloud Security Alliance (CSA) as one of the possible cryptographic tools for access control in big data applications [48, 49]. In KAC, data owner encrypts a message not only by the public key but also under an identifier of ciphertext that denotes the ciphertext belong to which class [50]. All the ciphertexts are categorized into different classes, and the key owner can extract an aggregate key over different classes by using a master-secret key [51]. Compared with the ABE and KAC, the medical blockchain system is tamper-proof and has privacy protection and secure storage. The cloud-based electronic medical record system relies on a trusted third party, but the medical blockchain system will not. In addition, patients have complete control over medical data, while the cloud-based electronic medical record system cannot enable patients to have complete control. Table 2 shows the comparison between the ABE, the KAC and the proposed scheme.

More importantly, the medical blockchain system plays an important role in personal medical data management and sharing. A structured electronic medical data system is established using blockchain-based distributed recording and storage, which cannot be falsified and is unforgeable. The decentralized structure of the blockchain enables the medical data to be updated in real time at each network node participating in the data storage, securely collecting and storing data and permanently storing it on the cloud server, which reduces the risks of sensitive information loss in the medical data set, and increases the security and credibility of the medical data. The medical blockchain system uses peer-to-peer propagation methods to share resources, such as medical health data, through consensus-based, standard protocols. The doctor will decide whether to anonymously share the medical record into the public research domain according to the patient's wishes. If the patient agrees to share, a certain number of tokens will be obtained, and the doctor will make a standard match according to the patient's disease type, age, work type and other characteristics and add it to the shared center of the private network.

While blockchain technology enables faster, near-real time transactions, the costs of operating such a system are not yet known [4]. Medical institutions and governments spend a lot of time and money on the storage and management of medical

Table 2 Comparison between the ABE, the KAC and the proposed scheme

	ABE	KAC	Proposed scheme
Reliance on trusted third parties	Yes	Yes	No
Tamper resistance	Yes	Yes	Yes
Privacy protection	Yes	Yes	Yes
Secure Storage	Yes	Yes	Yes
Control of medical records	Incomplete control	Incomplete control	Complete control

data, while constantly resolving system problems, device updates, data backups, and more. Blockchain technology can reduce the cost of these operations. When a blockchain system is set up successfully, the system will automatically run, record medical data continuously, and back up the entire network without the need for disaster recovery costs. Medical data sharing can create more value and reduce the cost of medical information transmissions. To avoid future energy costs caused by the "Proof of Work" (PoW) protocol, a "Delegate Proof of Stake" (DPOS) protocol could be employed in the medical blockchain since there would be no competition over discovering the blocks. The economics of the medical blockchain also need to be tested in practice.

Conclusion

Sharing and application of personal medical data are vital for intelligent medicine. However, most medical data are stored in different medical institutions, which leads to medical data being scattered. It is difficult for patients to acquire all their medical records from different medical institutions they have visited. Breaking the information island phenomenon in medical data is an urgent problem that needs a solution. In the meantime, storing, sharing and applying medical data is essential in situations where security and privacy are guaranteed. The blockchain is viewed as a storage supply chain in which every operation may be verified, accountable and immutable. Such inherent characteristics make it a potential solution for healthcare data systems that concerns both sharing and patient privacy. Therefore, the storage scheme and service framework based on the blockchain are proposed for storing, sharing and using medical data in this study. In the future, a medical blockchain network connecting as many medical and health institutions as possible should be established. Valuable medical data can flow safely, conveniently and cost controllable in the medical blockchain network. More application scenarios based on medical blockchain networks are thus developed. Comparing some mature blockchains with traditional systems makes it easier to analyze and discover their advantages and disadvantages, and further improve the safety management scheme of medical data.

Acknowledgements This work is partly supported by the National Natural Science Foundation of China (Grant No. 71571058 and 71690235), Anhui Provincial Science and Technology Major Project (Grant No. 16030801121 and 17030801001), CCF-Venustech Open Research Fund (Grant No. CCF-VenustechRP2017006).

Funding This study was funded by the National Natural Science Foundation of China (Grant No. 71571058 and 71690235), Anhui Provincial Science and Technology Major Project (Grant No. 16030801121 and 17030801001), CCF-Venustech Open Research Fund (Grant No. CCF-VenustechRP2017006).

Compliance with Ethical Standards

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

Ethical Approval This article does not contain any studies with human participants or animals performed by any of the authors.

Informed Consent Informed consent was obtained from all individual participants included in the study.

References

1. Medibloc Team. Medibloc whitepaper, 2017. https://www.chainwhy.com/whitepaper/medxwhite paperen.html. Accessed 15 September 2018.
2. U.S. Department of Health and Human Services. Blue Button Connector | You're your Health Records, 2017. http://bluebuttonconnector.healthit.gov/. Accessed 15 September 2018.
3. Apple Inc. iOS-Health, 2018. https://www.apple.com/ios/health/. Accessed 15 September 2018.
4. Deloitte Consulting LLP. Blockchain: Opportunities for health care, 2016. https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html. Accessed 15 September 2018.
5. Hydari, M. Z., Telang, R., and Marella, W. M., Saving Patient Ryan—Can Advanced Electronic Medical Records Make Patient Care Safer? Manage Sci Articles in Advance:1–19, 2018. https://doi.org/10.1287/mnsc.2018.3042.
6. Bhargava, H. K., and Mishra, A. N., Electronic Medical Records and Physician Productivity: Evidence from Panel Data Analysis. Manag. Sci. 60:2543–2562, 2014. https://doi.org/10.1287/mnsc.2014.1934.
7. Zheng, C., Xia, C., Guo, Q., and Dehmer, M., Interplay Between SIR-based Disease Spreading and Awareness Diffusion on Multiplex Networks. J Parallel Distr Com 115:20–28, 2018. https://doi.org/10.1016/j.jpdc.2018.01.001.

8. Li, X.-B., and Qin, J., Anonymizing and Sharing Medical Text Records. Inf. Syst. Res. 28:332–352, 2017. https://doi.org/10.1287/isre.2016.0676.
9. Li, C., Wang, L., Sun, S., and Xia, C., Identification of influential spreaders based on classified neighbors in real-world complex networks. Appl. Math. Comput. 320:512–523, 2018. https://doi.org/10.1016/j.amc.2017.10.001.
10. Xu, Z., Wei, X., Luo, X., Liu, Y., Mei, L., Hu, C., and Chen, L., Knowle: a semantic link network based system for organizing large scale online news events. Future Gener Comp Sy 43-44:40–50, 2015. https://doi.org/10.1016/j.future.2014.04.002.
11. He, D., Kumar, N., Wang, H., Wang, L., Choo, K.-K. R., and Vinel, A., A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network. IEEE Trans Dependable Secur Comput 15:633–645, 2018. https://doi.org/10.1109/TDSC.2016.2596286.
12. Ma, M., He, D., Khan, M. K., and Chen, J., Certificateless searchable public key encryption scheme for mobile healthcare system. Comput. Electr. Eng. 65:413–424, 2018. https://doi.org/10.1016/J.COMPELECENG.2017.05.014.
13. Zhang, Y., Qiu, M., Tsai, C., Hassan, M., and Alamri, A., Health-CPS: Healthcare-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data. IEEE Syst. J. 11:88–95, 2017. https://doi.org/10.1109/JSYST.2015.2460747.
14. Bahga, A., and Madisetti, V., A Cloud-based Approach for Interoperable Electronic Health Records (EHRs). IEEE J Biomed Health 17:894–906, 2013. https://doi.org/10.1109/JBHI.2013.2257818.
15. Godinho, T., Viana-Ferreira, C., and Silva, L., A Routing Mechanism for Cloud Outsourcing of Medical Imaging Repositories. IEEE J Biomed Health 20:367–375, 2016. https://doi.org/10.1109/JBHI.2014.2361633.
16. He, C., Fan, X., and Li, Y., Toward Ubiquitous Healthcare Services with a Novel Efficient Cloud Platform. IEEE Bio-med Eng 60:230–234, 2013. https://doi.org/10.1109/TBME.2012.2222404.
17. Wang, H., Ding, S., Wu, D., Zhang, Y., and Yang, S., Smart connected electronic gastroscope system for gastric cancer screening using multi-column convolutional neural networks. Int. J. Prod. Res.:1–12, 2018. https://doi.org/10.1080/00207543.2018.1464232.
18. Ding, S., Li, Y., Wu, D., Zhang, Y., and Yang, S., Time-aware cloud service recommendation using similarity-enhanced collaborative filtering and ARIMA model. Decis. Support. Syst. 107:103–115, 2018. https://doi.org/10.1016/j.dss.2017.12.012.
19. Ding, S., Wang, Z., Wu, D., and Olson, D. L., Utilizing customer satisfaction in ranking prediction for personalized cloud service selection. Decis. Support. Syst. 93:1–10, 2017. https://doi.org/10.1016/j.dss.2016.09.001.
20. Yang, Y., Zheng, X., Guo, W., Liu, X., and Chang, V., Privacy-preserving Smart IoT-based Healthcare Big Data Storage and Self-adaptive Access Control System. Inf. Sci.:1–26, 2018. https://doi.org/10.1016/j.ins.2018.02.005.
21. Singh, K., and Batten, L., Aggregating Privatized Pedical Data for Secure Querying Applications. Future Gener Comp Sy 72:250–263, 2017. https://doi.org/10.1016/j.future.2016.11.028.
22. Alshagathrh, F., Khan, S., Alothmany, N., Al-Rawashdeh, N., and Househ, M., Building a Cloud-based Data Sharing Model for the Saudi National Registry for Implantable Medical Devices: Results of a Readiness Assessment. Int. J. Med. Inform. 118:113–119, 2018. https://doi.org/10.1016/j.ijmedinf.2018.08.005.
23. Yang, J., Li, J., and Niu, Y., A Hybrid Solution for Privacy Preserving Medical Data Sharing in the Coud Environment. Future Gener Comp Sy 43-44:74–86, 2015. https://doi.org/10.1016/j.future.2014.06.004.
24. Xia, C., Meloni, S., Perc, M., and Moreno, Y., Dynamic instability of cooperation due to diverse activity patterns in evolutionary social dilemmas. EPL 109:58002, 2015. https://doi.org/10.1209/0295-5075/109/58002.
25. Jabeen, F., Hamid, Z., and Abdul, W., Enhanced Architecture for Privacy Preserving Data Integration in a Medical Research Environment. IEEE Access 5:13308–13326, 2017. https://doi.org/10.1109/ACCESS.2017.2707584.
26. Al, H. H., Rahman, S., and Hossain, M., A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-based Cryptography. IEEE Access 5:22313–22328, 2017. https://doi.org/10.1109/ACCESS.2017.2757844.
27. Solanas, A., Martínez-Ballesté, A., and Mateo-Sanz, J., Distributed Architecture with Double-phase Microaggregation for the Private Sharing of Biomedical Data in Mobile Health. IEEE T Inf Foren Sec 8:901–910, 2013. https://doi.org/10.1109/TIFS.2013.2248728.
28. Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., and Hayajneh, T., Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J. Med. Syst. 42:130, 2018. https://doi.org/10.1007/s10916-018-0982-x.
29. Lin, C., He, D., Huang, X., Choo, K.-K. R., and Vasilakos, A. V., BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. J. Netw. Comput. Appl. 116:42–52, 2018. https://doi.org/10.1016/J.JNCA.2018.05.005.
30. Lin, C., He, D., Huang, X., Khan, M., and Choo, K., A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-Based Identity Management Systems. IEEE Access 6:28203–28212, 2018. https://doi.org/10.1109/ACCESS.2018.2837650.
31. Peter BN (2017) Blockchain applications for healthcare. http://www.cio.com/article/3042603/innovation/blockchain-applications-for-healthcare.html. Accessed 17 March 2017.
32. Prisco G (2016) The Blockchain for Healthcare: Gem Launches Gem Health Network With Philips Blockchain Lab. https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938/. Accessed 26 April 2018.
33. Mettler M (2016) Blockchain Technology in Healthcare: The Revolution Starts Here. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) 1–3. https://doi.org/10.1109/HealthCom.2016.7749510
34. Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W., Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J. Med. Syst. 40(10):1–8, 2016. https://doi.org/10.1007/s10916-016-0574-6.
35. Shrier AA, Chang A, Diakun-thibault N, Forni L, Landa F, Mayo J, van Riezen R (2016) Blockchain and Health IT: Algorithms, Privacy, and Data. http://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf. Accessed 19 August 2017.
36. Lvan D (2016) Moving toward a blockchain-based method for the secure storage of patient records. http://www.healthit.gov/sites/default/files/9-16-drew_ivan-20160804_blockchain_for_healthcare_final.pdf. Accessed 4 August 2016.
37. Yuan B, Lin W, McDonnell C (2016) Blockchains and electronic health records. http://mcdonnell.mit.edu/blockchain_ehr.pdf. Accessed 4 May 2016.
38. Ekblaw A, Azaria A, Halamka JD, Lippman A (2016) A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf. Accessed 4 May 2017.
39. Azaria A, Ekblaw A, Vieira T, Lippman A (2016) MedRec: Using Blockchain for Medical Data Access and Permission Management.

2016 2nd International Conference on Open and Big Data (OBD) 25–30. https://doi.org/10.1109/OBD.2016.11

40. Xia, Q., Sifah, E., Smahi, A., Amofa, S., and Zhang, X., BBDS: blockchain-based data sharing for electronic medical records in cloud environments. Information 8(2):44, 2017. https://doi.org/10.3390/info8020044.
41. Peterson K, Deeduvanu R, Kanjamala P, Clinic KBM (2016) A Blockchain-Based Approach to Health Information Exchange Networks. https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf. Accessed 26 May 2016.
42. Kuo TT, Hsu CN, Ohno-Machado L (2016) ModelChain: decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. https://www.healthit.gov/sites/default/files/10-30-ucsd-dbmi-onc-blockchain-challenge.pdf. Accessed 22 May 2016.
43. Chen, T., and Zhong, S., Emergency access authorization for personally controlled online health care data. J. Med. Syst. 36(1):291, 2012. https://doi.org/10.1007/s10916-010-9475-2.
44. Huba, N., and Zhang, Y., Designing patient-centered personal health records (PHRs): health care professionals' perspective on patient-generated data. J. Med. Syst. 36(6):3893–3905, 2012. https://doi.org/10.1007/s10916-012-9861-z.
45. Xia, C., Ding, S., Wang, C., Wang, J., and Chen, Z., Risk analysis and enhancement of cooperation yielded by the individual reputation in the spatial public goods game. IEEE Syst. J. 11(3): 1516–1525, 2017. https://doi.org/10.1109/JSYST.2016.2539364.
46. Simpao, A. F., Ahumada, L. M., Gálvez, J. A., and Rehman, M. A., A review of analytics and clinical informatics in health care. J. Med. Syst. 38(4):45, 2014. https://doi.org/10.1007/s10916-014-0045-x.
47. Wang, Y., Tian, Y., Tian, L. L., Qian, Y. M., and Li, J. S., An electronic medical record system with treatment recommendations based on patient similarity. J. Med. Syst. 39(5):1–9, 2015. https://doi.org/10.1007/s10916-015-0237-z.
48. Wang, Z., Cao, C., Yang, N., and Chang, V., ABE with improved auxiliary input for big data security. J. Comput. Syst. Sci. 89:41–50, 2017. https://doi.org/10.1016/j.jcss.2016.12.006.
49. Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM conference on Computer and communications security 89–98. https://doi.org/10.1145/1180405.1180418
50. Chu, C., Chow, S. S. M., Tzeng, W., Zhou, J., Deng, R. H., and Member, S., Supplementary Material for Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage. IEEE Trans Parallel Distrib Syst 25:1–4, 2014. https://doi.org/10.1109/TPDS.2013.112.
51. Wang, Z., Provably secure key-aggregate cryptosystems with auxiliary inputs for data sharing on the cloud. Futur. Gener. Comput. Syst., 2017. https://doi.org/10.1016/j.future.2017.09.041.