Efficient Patient-Friendly Medical Blockchain System Based on Attribute-Based Encryption

Yan Sun, Wei Song(✉), and Yuan Shen

School of Computer Science, Wuhan University, Wuhan 430072, China
songwei@whu.edu.com

Abstract. In recent years, there have been rapid advances in electronic medical record (EMR) sharing with the fast development of blockchain technology. Using blockchain technology to build the electronic medical record sharing system can effectively solve the problem that medical data is hard to share between different hospitals' databases. However, existing EMR sharing system using blockchain technology is mainly for medical institutions, and the patients as the data owner even can't easily share their own personal EMR when they need to use it. The patient's demand for management of personal EMRs is largely ignored. At the same time, the doctor's longitudinal access to personal EMRs requires a fairly large overhead, which severely causes treatment delay. This paper proposes a patient-friendly blockchain electronic medical data sharing system based on main-sub structured blockchain, which enables patients to manage their personal medical data directly and enhances the authorized users' efficiency of access to personal EMRs significantly. Experimental results demonstrate that our scheme is efficient enough to support the real medical record sharing applications.

Keywords: Electronic medical record · Main-sub blockchain · Medical data sharing · Attribute-based encryption

1 Introduction

EMR system can facilitate the medical diagnosis process, but it is limited by the traditional management mechanism. In particular, EMR data are stored and managed by the hospital which generated it. However, the real data owner, the patient, cannot conveniently manage their own medical records. When they visit other hospitals, they are not available to provide the doctor their past medical records, because their past records were stored in the hospital's private database. Interoperability challenges between different hospital systems give tough problems to data sharing. It is difficult for patients to share the medical data because of lack of personal data management and sharing. At the same time, due to the centralized management of hospitals, EMR cannot resist the threats of personal information leakage as well.

To meet the requirements on medical data sharing, some researchers [1–3] have proposed some relative schemes about cloud storage technologies to provide suitable solutions to share medical data. However, cloud service providers (CSP) still face some significant problems in persuading hospitals to use centralized cloud services due to the

G. Wang et al. (Eds.): WISA 2020, LNCS 12432, pp. 642–653, 2020.
https://doi.org/10.1007/978-3-030-60029-7_57

risks of personal privacy disclosure. After all, a whole lot of data stored in third parties is not reassuring.

Blockchain is a distributed and shared database, characterized by decentralization, non-tampering, traceability and openness. In recent years, blockchain has been proposed to be a promising solution to achieve EMR sharing with security and privacy preservation due to its advantages of non-tampering and traceability. Therefore, compared with the cloud-based electronic medical record (EMR) sharing system, blockchain has the advantages of decentralization and traceability, so it has higher security level. But most existing systems are mainly for medical institutions, which ignores the patient's requirements of personal data management and control. When the patients want to share their personal EMR to someone, they cannot provide their own medical records.

Generally speaking, there are still three major challenges that need to be over-come:

- The EMRs are distributed in different hospitals. Therefore, it can only be visited through the hospital where the patient was treated. When the patient is going to another hospital, his or her EMR can't be shared between hospitals, which can cause misdiagnosis and unnecessary repeated physical examination. How to deal with interoperability problems between different hospital systems is the first challenge.
- Besides the interoperability issue, the patient pays more attention to personal privacy as the EMR contains many sensitive information [4]. The patient needs a more personalized method to share their EMR, which means the authorized attributes of attribute set can be decided by the patient. Therefore, a fine-grained access control mechanism is highly desirable for the real EMR sharing applications.
- Furthermore, when the data user accesses to the patient's EMR which they need, the overhead of query personal EMR is quite big. As the blockchain length increases, the query overhead becomes larger.

Motivated by the above issues, we deign a medical blockchain system using attribute-based encryption which meets all the practical requirements mentioned above with strong security guarantee. The main contributions of this paper can be summarized as:

- First, we design a main-sub medical blockchain system, all the patients' medical records are stored in the blockchain, the authorized medical institutions can share these data for treatment and research. Therefore, interoperability between different hospital systems is well addressed.
- Second, we introduce the attribute-based encryption method [5]. By it, the patients are allowed to directly manage and share their own EMR with strong security guarantee. And the data users can only access to authorized personal EMR without leaking out other sensitive information, which effectively avoids personal information disclosure.
- Third, we store the patient's EMR according to unique personal ID in the sub blockchain, so that various data users can efficiently access the medical data by comparing the hash value of attribute set which reduce the overhead of query and computation greatly.

– Finally, we formally prove the security of the proposed scheme and conduct experiments which can also demonstrate that our scheme is efficient.

The rest of this paper is organized as follows. In Sect. 2, we discuss related work about medical data sharing based-on blockchain, and present the necessary background to understand the proposed scheme. In Sect. 3, we present our scheme. Our experimental analysis is outlined in Sect. 4, and the conclusion is presented in Sect. 5.

2 Related Work

Blockchain is widely used in the field of data sharing, due to its characteristics of decentralization, openness, anti-tampering and traceability.

Prior work by Zyskind et al. [6] has demonstrated the use of blockchain protocols for permission management. They implement a trusted blind escrow service, storing encrypted data in trusted third party hosting services while logging pointers on the blockchain, but the third party brings the risk of data disclosure. Kish proposed the blockchain for hypothetical key management in a medical context [7].

Ariel et al. build on these ideas and develop MedRec: a decentralized record management system to handle EMRs, using blockchain technology [8]. But the cost of querying personal EMR is relatively large.

Esposito et al. [9] detailed the drawbacks of using cloud storage technology to establish a data sharing system in the medical field. They also raised the possible challenges of using blockchain technology in medical data sharing (such as privacy protection). However, the article does not propose practical schemes to address these challenges. These studies [10] only proposed a framework, but did not implement specific security data access authorization scheme.

Kai Fan et al. [11] proposed a blockchain-based information management system, MedBlock, to handle patients' information. But it used the bread crumbs which will bring additional amount of data, leading to excessive storage consumption.

Therefore, we need an encryption scheme that provides a more efficient way to control data access based on data user's attributes [12]. The concept of attribute-based encryption (ABE) was first proposed by Sahai and Waters [13], and in this context can be employed to encrypt the EMRs in the medical blockchain system. The ABE scheme allows users to access the data when their attributes satisfy the data owner's requirements. And we have designed the retrieval mechanism on the sub blockchain scheme that provides better performance of accessing the patient's personal medical records.

In this paper, we propose an efficient patient-friendly system based on main-sub blockchain (PSBM) to share electronic medical records among authorized users. The sub blockchain allows the patient define who can access their EMR, while the main blockchain makes the users find the information they want in an efficient way. Moreover, the medical blockchain system is suitable for multi-task oriented applications and can also achieve load balance.

3 The Proposed PSBM Scheme

Blockchain provides an important support for the sharing of medical data. But there are still problems that the patient as the data owner lacks control over their own medical data, so an efficient patient-friendly medical blockchain scheme is needed. As for individual data users, only the data user who is authorized by the patient can access the data through the sub blockchain. But for those who are not in the attribute collection, the patient cannot authorize the data to them. And for medical institutions (including research, education and statistics), this system model allows medical staff to access to anonymous medical data through the main blockchain.

In order to ensure the data owner's management of personal medical data, patients also need to set up corresponding attributes collection and compute the hash value of each attributes collection. In advance, the patients update personal EMR adding authorized attributes collection in the sub blockchain, so in case of individual query access, the data user in the attributes collection can access the EMR at a rapid speed.

3.1 System Model

The system model includes six entities: key generation center, medical institutions, data owner, main blockchain, sub blockchain and data user. The proposed model is illustrated in Fig. 1.

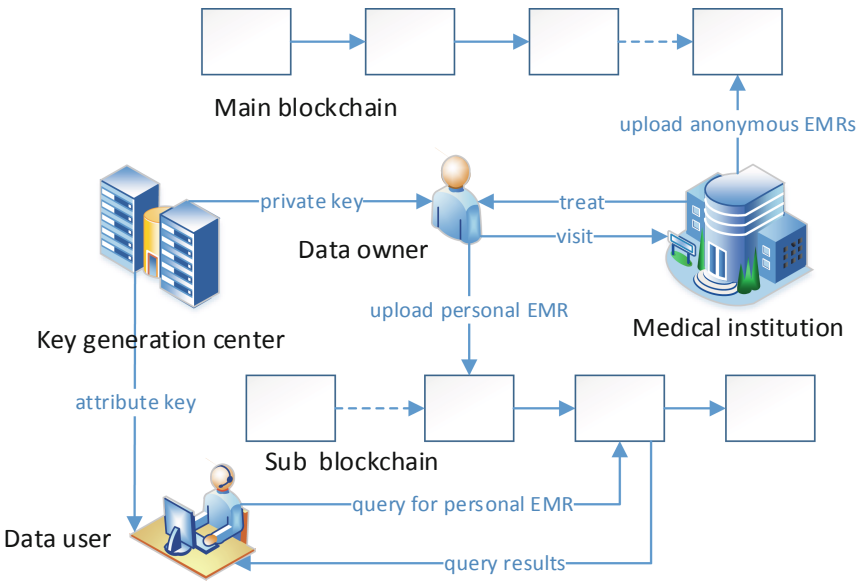

Fig. 1. System model

And the characteristics and functions of each entity are described as follows:

(1) Key generation center (KGC): responsible for generating system public parameter and creating master system key MSK. Meanwhile, the key generation center generates key pairs for patients and data users.
(2) Medical institutions (MI): they are composed of various hospitals with medical capacity. A medical institution manages its staff and provides medical services to patients. After the registration of a medical institution, KGC generates public private key pairs for the medical institution, and securely transmits the private key to the medical institution. A medical institution generates a set of attributes for its medical staff to describe their data access characteristics and generate an attribute key for them.
(3) Data owner (DO): mainly composed of the patients themselves, who can manage their EMRs stored in the sub blockchain directly. When a new medical record is inserted in the main blockchain, the data owner will compute the sub blockchain sequence number according to the patient's unique identity, private key and the main blockchain's sequence number (which block the new record is stored in the blockchain). Meanwhile, the data owner will give the record a set of attributes for authorized access, (such as hospitals, categories of doctor and title of doctor).
(4) Main blockchain (MB): used for storing medical data which is processed anonymously and every EMR's corresponding sub blockchain sequence number. EMRs are all stored in chronological order. Only medical and statistical institutions have the access to the data.
(5) Sub blockchain (SB): responsible for storing the patient's medical data by personal id and access control information. After data owner computes the sequence number, the new medical record containing access control logic will be updated in the sub blockchain.
(6) Data user (DU): as for medical institutions, they have the access to the medical data of the main blockchain. As for individual data users, only if users' attributes match the data owner's requirements, they are able to access some data on the sub blockchain.

Besides, we focus on the construction of the main blockchain and the sub blockchain. The hospital kept the patient's original medical records after the patient was treated, then the medical records were anonymized by the hospital and stored in the main blockchain. The main blockchain is for the research and statistics of medical institutions. The main blockchain is illustrated in Fig. 2.

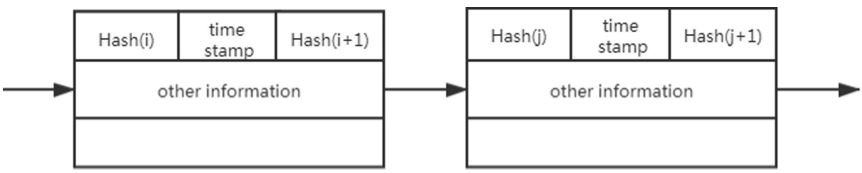

Fig. 2. Main blockchain

Every block has its own sequence number, and sub blockchain's sequence number of the same medical record is computed by the hash function on the basis of patient's id, private key and main blockchain's sequence number. What is different from the main blockchain is that the medical record is stored not by time, but by patient's id. As for patient Alice, her first block on the sub blockchian is B0. B0 is Alice's head block, which stores Alice's id, authorized attribute set for each medical record and the block sequence number corresponding to the attribute set. The sub blockchain is illustrated in Fig. 3. Therefore, when a data user makes a query, only one comparison is needed to get the result of the query. Compared to the traditional way of data retrieval, the query efficiency is greatly improved.

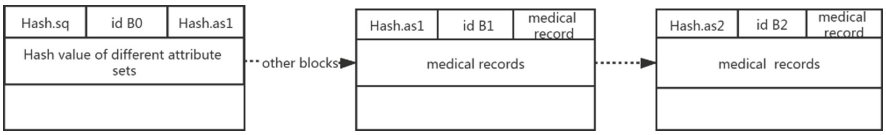

Fig. 3. Sub blockchain

3.2 Description of Proposed PSBM Scheme

We build an efficient retrieval scheme based on blockchain with support for fine-grained access control. The scheme is composed of four polynomial time algorithms, as described below (Table 1).

Table 1. Symbols used in this paper.

Symbols	Meaning of the symbols
PK	The public key
MSK	The system master key
MD	The plaintext medical document
A	The authorized attribute set A
Γ	The access strategy
K	The encryption key
C	The ciphertext medical document
I	The safe index
SK_U	The attribute key

(1) Setup(1^λ) → (*PK*, *MSK*). The key generation center operates the Setup algorithm. This is a randomized algorithm that takes no input other than the implicit security parameter λ.
The key generation center defines G_0, $G_1 \in Z_p^*$, which are two multiplicative cyclic groups of $\mathbb{G}$. And p is a big secure prime number, let g be the generator of group G_0, and define bilinear mapping e: $G_0 \times G_0 \rightarrow G_1$. Select the random hash

function H_1: {0,1}* → G_0, H_2: $\{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^l$. Key generation center sets the random number $\alpha, \beta \in Z_p^*$ and then computes bilinear pairs $Y = e(g_1, g_2)^{\alpha}$. Finally, it outputs system common parameter PK = G_0, G_1, p, $h = g^{\beta}$, Y, H_1, H_2) and master secret key MSK = (α, β).

(2) Enc(*PK*, *MD*, *A*, *Γ*, *K*) → (*C*, *I*). The data user public key *PK*, the clear personal medical document *MD*, authorized attribute set *A*, access strategy *Γ* and encryption key *K*. The outputs are encrypted medical data *C* and safe index *I*.

1. FileEnc(*MD*, *K*) → *C*. Data owner randomly selects $K \leftarrow \{0,1\}^K$ as a clear medical document symmetric encryption key. And the data owner uses *K* to encrypt medical document MD_i(i ∈ [1, *n*]), then gets the $C_i = \{\varepsilon.\mathrm{Enc_k}(D_i)|$ i [1, n]}. In the formula, *ε* represents a secure symmetric encryption scheme, and *ε*.Enc represents the encryption process.
2. IndexGen(*PK*, *A*, *Γ*, *K*) → (C, *I*). Data owner first give the authorized attribute set $A = \{A_1, A_2, \ldots, A_n\}$ for each medical document $MD = \{MD_1, MD_2, \ldots, MD_n\}$. The data owner defines the access structure *Γ*. First of all, starting from the root node *r* of the tree *Γ*, assign a polynomial q_x of order d_x for each node *x* (the q_x of the leaf node is a constant number). Let k_x be the threshold value of node *x*, and set $\deg(q_x) = d_x = k_x - 1$. The data owner randomly selects $s \leftarrow$ from the root node *r* and make $q_r(0) = s$, and selects $\deg(q_r)$ random coefficients to determine the polynomial q_r. As for other nodes *x*, set $q_x(0) = q_{\mathrm{parent(x)}}(\mathrm{index(x)})$ and selects $\deg(q_x)$ random coefficients to determine the polynomial q_x. Let Y represents all the leaf nodes of tree *Γ*, data owner gets the encrypted safe medical data *C* and index *I*.

$$\mathrm{C} = \left\{\Gamma, \bar{\mathrm{C}} = \mathrm{Ke}(\mathrm{g}, \mathrm{g})^{\alpha s}, C = h^s, \left\{C_y = \mathrm{g}^{q_{y(0)}}, C_y' = H_1(att(y))^{q_{y(0)}}\right\}\right\} \tag{1}$$

In the above expression, *s* is a random number, *att(y)* means attribute value.

(3) UserRegister(*PK*, *MSK*, *S*) → (SK_U). The data user offers the attribute set *S* to the key generation center, the key generation center inputs the public parameter *PK*, master key *MSK* and data user's attribute set *S*. Then it outputs the attribute key SK_U and gives it to the data user. When $\forall j \in S$, the key generation center randomly selects $r \in Z_p^*$. Evaluate the corresponding attribute private key:

$$\mathrm{SK}_U = \left\{E = \mathrm{g}^{\frac{\alpha+\mathrm{r}}{\beta}}, \left\{E_j = \mathrm{gH}_1(j)^{r_j}, E_j' = \mathrm{g}^{r_j}\right\}\right\} \tag{2}$$

(4) Dec(SK_U, *C*) → *MD*/⊥. Data user inputs the attribute key SK_U and encrypted medical data *C*. If the attribute key SK_U satisfies the access structure *Γ* defined by the data owner, the data user can restore symmetric key K, decrypt ciphertext medical document collection *C*. And output contains the plaintext medical document collection *MD*. Otherwise, output ⊥. K is computed as below:

$$K = \frac{\bar{C}}{\frac{e(C,E)}{A}} = \frac{Ke(g, g)^{\alpha s}}{\frac{e\left(h^s, g^{\frac{\alpha+r}{\beta}}\right)}{e(g,g)^{rs}}} = \frac{Ke(g, g)^{\alpha s} e(g, g)^{rs}}{e(g, g)^{s(\alpha+r)}} \tag{3}$$

3.3 Insert Algorithm of PMBS

While a patient p visits the hospital, the hospital will anonymize personal medical data and upload it to the main blockchain in chronological order. At the same time, p is supposed to update his or her own personal EMR on the sub blockchain.

(1) If it is the first EMR to store, the patient will compute the sub blockchain's sequence number according to patient's id, private key and main blockchain's sequence number. The head block of the patient will be used to store the hash value of the authorized attribute set.
(2) If not, the patient can directly store the hash value of the authorized attribute set in his or her head block, and the EMR will be stored in the block which is linked to the head block. The EMR of same authorized attribute set is stored in one block.
(3) If the block used to store the EMR of same authorized attribute set is full, the next block will be used for new storage. And all the EMR block's sequence number is stored in the patient's head block. The main-sub blockchain system is shown in Fig. 4.

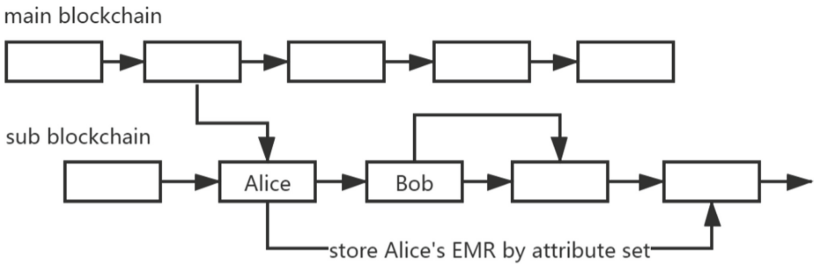

Fig. 4. The main-sub blockchain system

3.4 Query Algorithm of PMBS

While a doctor d attempts to retrieve the certain patient's EMR, d needs to register first according to UserRegister algorithm. Then d generates a query request Q (SK_U, PID) and asks the patient to compare the doctor's attributes with his or her authorized attribute set.

(1) If they are not the same, the doctor cannot visit the patient's EMR.
(2) If the doctor d's attributes match the authorized attribute set, d can visit the patient's head block in the sub blockchain and get the blockchain sequence to

another block which d can get the medical records. In the case of that block is full, d will continue to visit the next block via obtained sequence number.

(3) After d gains the encrypted medical records, d can easily decrypt them by Decryption algorithm.

4 Analysis of Performance

In this section, we verify the efficiency of the efficient patient-friendly medical blockchain system based on attribute-based encryption (PBMS). The experimental environment is on a Windows 10 (64-bit) operating system with an Intel Core i7 4 GHz processor with 8 GB RAM. The encoding is implemented by using the JPBC 2.0 library. Three groups of comparative experiments were conducted to compare the efficiency of this scheme with the existing MedRec scheme [5], MedShare scheme [14] and MedBlock scheme [7] in encryption algorithm, query algorithm and memory consumption. The experimental comparison is shown below.

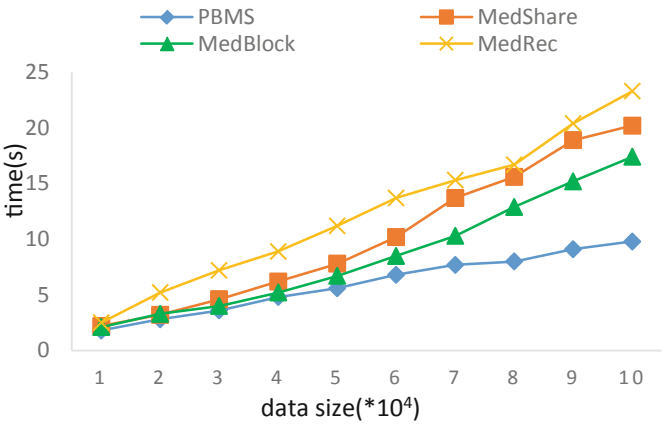

Fig. 5. Time cost for encryption

As illustrated in Fig. 5, the time cost between the other three schemes and our scheme in the encryption phase is positively correlated with the data size. And our scheme has more excellent performance in terms of time consumption than the other three schemes. This is because we use the main blockchain and the sub blockchain to work together, which can significantly reduce time overhead and achieve load balance. By contrast, MedRec scheme, MedShare scheme and MedBlock scheme show a significant increase in time consumption with the increase of data size. In general, our scheme is more effective under the condition of huge data size.

The results in Fig. 6 shows that the efficiency of data query is greatly improved. In our scheme, we adopt main-sub blockchain structure to enhance information retrieval efficiency. If a data user wants to retrieve someone's EMR information, he can directly find the corresponding block according to the block sequence number and the hash value of attribute set. The original search method needs to traverse the data on the block until finding the useful data. Compared with the traditional way of data retrieval, the efficiency of sub-blockchain increases too much. And the sub-blockchain can balance the query pressure of the main blockchain.

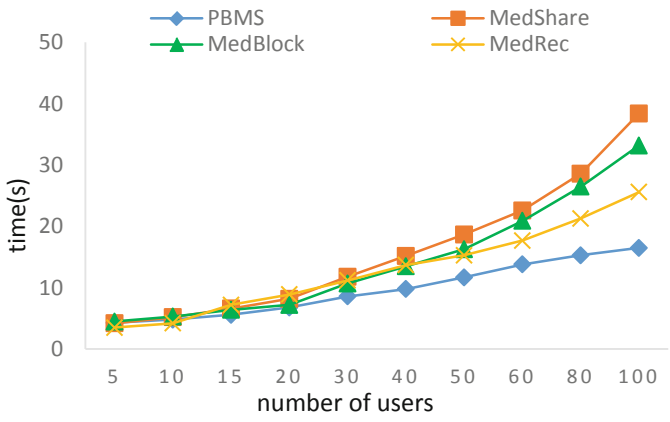

Fig. 6. Time cost for query

When the number of users is small, the time cost of query in our scheme, MedRec scheme, MedShare scheme and MedBlock scheme has small difference. The original search method can also find the EMR information in a relatively short time. However, as the number of users' increases, the advantages of PBMS over the other three schemes become more and more obvious. The records of sub blockchain can directly guide the users to find the corresponding blocks. Even if the number of users is quite large, it will not be a constraint on efficiency.

As shown in Fig. 7, memory consumption increases almost linearly as the number of attributes increases. MedRec scheme uses the least memory consumption, and our scheme costs slightly more memory than MedShare scheme and MedBlock scheme. The increase in memory consumption is due to the introduction of sub blockchain, but the storage overhead is acceptable. When the number of attributes was 100, our scheme memory consumption was 10.80 KB.

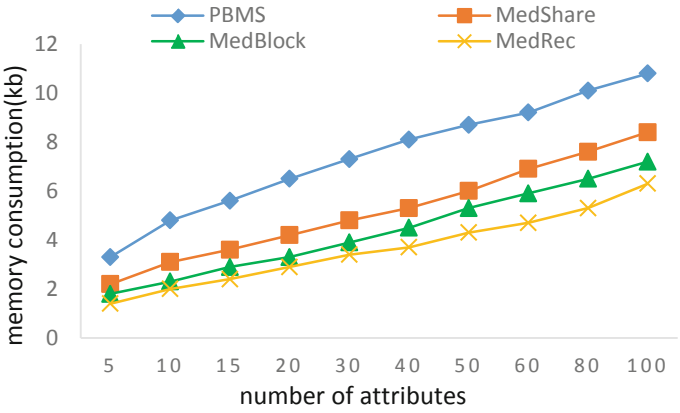

Fig. 7. Memory consumption for storage

We also compare other performances with the three schemes, it is illustrated in Table 2. What makes our scheme superior to others is that PBMS is patient-authorized, so that the patient can share and manage their medical data easily.

Table 2. Comparison between proposed system and other systems

Scheme	Tamper proof	Privacy protection	Patient-authorized access
PBMS	Y	Y	Y
MedRec	Y	N	N
MedShare	Y	N	N
MedBlock	Y	Y	N

5 Conclusion

In this paper, we focused on the practical problem of patient's privacy preserving and management over the personal electronic medical data in the EMR sharing system. We further discussed different stakeholder's practical requirements for this problem. To fulfill these requirements, we proposed a novel patient-friendly medical blockchain sharing system based on attribute-based encryption. For the convenience of sharing and managing EMRs, we designed our system by introducing a sub blockchain to reduce the overheads of query and balance the load. We have carried out several experiments to show that the query processes are efficient and our scheme is appropriate for using in the blockchain-based EMR sharing systems.

Acknowledgement. This work is supported by the key projects of the National Natural Science of Foundation of China (No. U1811263, 61572378), the major technical innovation project of Hubei Province (No. 2019AAA072), the Science and Technology Project of State Grid Corporation of China (No. 5700-202072180A-0-0-00), the Teaching Research Project of Wuhan University (No. 2018JG052). We also thank anonymous reviewers for the helpful reports.

References

1. Marwan, M., Kartit, A., Ouahmane, H.: A cloud based solution for collaborative and secure sharing of medical data. Int. J. Enterp. Inf. Syst. (IJEIS) **14**, 128–145 (2018)
2. Yang, J.J., Li, J.Q., Niu, Y.: A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Gener. Comput. Syst. (FGCS) **43**, 74–86 (2015)
3. Wu, Y., et al.: Adaptive authorization access method for medical cloud data based on attribute encryption. In: Ni, W., Wang, X., Song, W., Li, Y. (eds.) WISA 2019. LNCS, vol. 11817, pp. 361–367. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30952-7_36
4. Ding, Y., Song, W., Sheng, Y., Yan, S.: Enabling efficient multi-keyword search over fine-grained authorized healthcare blockchain system. In: The Asia Pacific Web (APWeb) (2020)
5. Goyal, V., Pandey, O., Sahai, A.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS), pp. 89–98 (2006)
6. Zyskind, G., Nathan, O., Pentland, A.: Decentralizing privacy: using blockchain to protect personal data. In: Proceedings of IEEE Symposium on Security and Privacy (S&P) Workshop, pp. 180–184 (2015)
7. Kish, L.J., Topol, E.J.: Unpatients-why patients should own their medical data. Nat. Biotechnol. **33**, 921–924 (2015)
8. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system, Bitcoin White Paper (2008)
9. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30 (2016)
10. Ajtai, M.: Generating hard instances of lattice problems. In: Proceedings of ACM Symposium on Theory of Computing, pp. 99–108 (1996)
11. Fan, K., Wang, S., Ren, Y., Li, H., Yang, Y.: MedBlock: efficient and secure medical data sharing via blockchain. J. Med. Syst. **42**(8), 1–11 (2018). https://doi.org/10.1007/s10916-018-0993-7
12. Tep, K.S., Martini, B., Hunt, R., Choo, K.K.R.: A taxonomy of cloud attack consequences and mitigation strategies: the role of access control and privileged access management. In: Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, pp. 1073–1080 (2015)
13. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_27
14. Xia, Q., Sifah, E.: MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access **5**, 14757–14767 (2017). ISSN 2169-3536