Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

A blockchain-based scheme for privacy-preserving and secure sharing of medical data

Haiping Huang[a,b,*], *Peng Zhu*[a,b], *Fu Xiao*[a,b], *Xiang Sun*[a,b], *Qinglong Huang*[a,b]

[a] *School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, Jiangsu China*
[b] *Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210023, Jiangsu China*

ARTICLE INFO

Article history:
Received 2 January 2020
Revised 4 July 2020
Accepted 14 August 2020
Available online 1 September 2020

Keywords:
Blockchain
Privacy protection
Medical data
Secure data sharing
Smart contract
Zero-knowledge proof

ABSTRACT

How to alleviate the contradiction between the patient's privacy and the research or commercial demands of health data has become the challenging problem of intelligent medical system with the exponential increase of medical data. In this paper, a blockchain-based privacy-preserving scheme is proposed, which realizes secure sharing of medical data between several entities involved patients, research institutions and semi-trusted cloud servers. And meanwhile, it achieves the data availability and consistency between patients and research institutions, where zero-knowledge proof is employed to verify whether the patient's medical data meets the specific requirements proposed by research institutions without revealing patients' privacy, and then the proxy re-encryption technology is adopted to ensure that research institutions can decrypt the intermediary ciphertext. In addition, this proposal can execute distributed consensus based on PBFT algorithm for transactions between patients and research institutions according to the prearranged terms. Theoretical analysis shows the proposed scheme can satisfy security and privacy requirements such as confidentiality, integrity and availability, as well as performance evaluation demonstrates it is feasible and efficient in contrast with other typical schemes.

1. Introduction

1.1. Motivation

Due to the rapid development of Wise Information Technology of 120 (WIT120), the number of hospitals in China have exceeded 30,000, the number of health research institutions for medical care will be over 35,000 in 2020, and the medical data is showing an exponential growth trend (Yang and Chen, 2019). Medical data is both a valuable asset for patients and a precious resource for research institutions or medical organizations to conduct disease research or commercial transactions (Dimitrov, 2016). Usually, patients expect to keep their medical data confidential due to individual privacy, but under certain conditions, for example, paid a certain remuneration, they would like to disclose partial private data to authorized organizations such as disease research institutions. Even so, patients remain concerned about privacy protection of medical data in the entire data sharing process. This indicates the first challenging problem that no one except the authorized institutions has access to patients' private medical data. And meanwhile, research institutions or medical organizations expect to obtain the medical data they really need rather than unrelated information. For example, what

* Corresponding author.
E-mail address: hhp@njupt.edu.cn (H. Huang).
https://doi.org/10.1016/j.cose.2020.102010

COVID-19 research institutions need is nucleic acid testing data from patients with COVID-19, rather than physiological data from common patients with cold symptoms. Therefore, the second challenging problem is how patients can prove to research institutions that their data meets the needs of research institutions without revealing any privacy. Furthermore, for reasons of authority or commercial interests, some research institutions or medical organizations want to have exclusive access to specific patients' medical data according to the agreement reached in advance. They expect the transactions that these patients provided them with medical data can be recorded and acknowledged but only if the patient's privacy could be protected, which becomes the third concern of this paper. Therefore, based on the challenging problems mentioned above, a solution is urgently needed to achieve secure data sharing between patients and research institutions for guarantee the maximum degree of privacy protection (Elhoseny et al., 2018).

Blockchain (Nakamoto, 2008; Wang et al., 2019a) is considered as one effective solution to the above problems according to the survey from GDPR (Tene et al., 2019), which has been applied into many scenarios such as e-government, intelligent healthcare, virtual currency, food and drug supervision, etc. As a distributed shared ledger and database, blockchain has the characteristics of decentralization, immutability, consensus mechanism, traceability, privacy-preserving, fault tolerance, and the capability to execute smart contracts. Wherein, the smart contract (Wang et al., 2019b) allows distrustful parties to communicate with each other by automatic verification and programmable execution of script on the blockchain. Therefore, aiming at the first and third challenges, based on smart contracts, we decide to utilize blockchain technology to realize the privacy protection and secure sharing of medical data, distributed consensus of transactions between patients and research institutions, and the automatic management of resources.

Furthermore, zero-knowledge proof (Goldreich et al., 1991) will be employed to address the second issue, whose function is that the prover can convince the verifier that the assertion is correct (the needs are met) without providing the verifier with any useful information (any private data). As the generator tool of zero-knowledge proof, zero-knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) (Ben-Sasson et al., 2013) has ever been applied to blockchain transactions, which hides the addresses of the transaction sender and receiver and the transaction amount to achieve anonymity and privacy-preserving. This also motivated us to migrate zk-SNARKs to medical system in order to achieve the data availability with consistent supply and demand between patients and disease research institutions, with the aid of smart contracts.

Back to the first challenging problem, although the existing blockchain-based medical systems, such as Ancile (Dagher et al., 2018), MedRec (Azaria et al., 2016), have realized the secure data storage in blocks and in cloud servers, the decentralized integration of medical data across medical organizations and the balance between privacy and accessibility of EHRs (electrical health records). However, these medical systems are not always concerned about protecting patient's privacy during the entire process of sharing and transaction of medical data. Especially, few studies have comprehensively considered the patient's privacy during the phase where information regarding medical data is transmitted back and forth among several entities involved smart contracts. In this paper, based on the existing solutions for the first challenging problem, we design a secure data sharing scheme among several entities who interact with smart contracts, where proxy re-encryption technology will be adopted to achieve the privacy-preserving of medical data. In addition, we will also devote to address these issues including the unsatisfactory transaction processing capacity and implementation efficiency caused by the current blockchain-based medical system.

1.2. *Related work*

Due to the explosive growth of medical data, the traditional centralized medical data storage schemes (Zhang et al., 2018; Miao et al., 2019; Liang et al., 2020) have been unable to meet the requirements of data availability and scalability with the risk of privacy disclosure. In order to alleviate the data storage stress and improve the quality of medical services, abundant researches are focused on blockchain to achieve privacy-preserving distributed storage and secure sharing of medical data. Vazirani et al. (2020) focused on how the introduction of blockchain can create a more efficient infrastructure to manage electronic medical records. However, they don't present a concrete scheme to improve the healthcare outcomes without compromising the privacy or security of patients. Ivan (2016) analyzed the feasibility of utilizing blockchain as a storage scheme for protecting medical data privacy. However, they had ignored the problem of identity management and user authentication when carrying out data sharing. Bendiab et al. (2018) present a novel blockchain-based trust model that allows cloud service providers to manage their trust relationships in order to realize secure data sharing without relying on a trusted third-party. Li et al. (2018) proposed a blockchain-based medical data preservation scheme (DPS), which ensures the primitiveness and verifiability of EHRs while preserving privacy for the data owner. However, the medical data has been uploaded by the user directly into the system in DPS, which is inapplicable for most intelligent medical scenarios. For safeguarding the patient's private data, Ibraimi et al. (2008) designed a fine-grained PHR disclosure scheme for medical services, which is a type-and-identity-based proxy re-encryption scheme to enable the delegator to implement different access control policies for his ciphertexts. Fimiani (2018) investigated the problem of realizing a privacy-preserving exchange of medical documents by using an improved proxy re-encryption scheme called Fuzzy Conditional Identity, where the keys are extracted directly from the biometrics of the users.

Furthermore, in the blockchain-based medical platforms, the content privacy and consensus efficiency of transactions have been paid more and more attentions. Li and Mei (2020) adopted ring signature to build a privacy data storage protocol based on the elliptic curve, which ensures the security of data and user identity privacy in blockchain applications. However, even if the ring signature has solved the anonymity problem of the sender and receiver, it cannot protect the transaction content privacy. Zheng et al. (2018) proposed a medical data shar-

ing scheme that combines blockchain, cloud computing and machine learning. This scheme can easily realize the sharing of medical data between various institutions. However, it cannot verify the integrity of cloud medical data, and data consumers are not sure whether they have received the correct medical data. Azaria et al. (2016) designed a medical information sharing platform named MedRec based on Ethereum, which realizes the decentralized secure integration of medical data across medical organizations. Nevertheless, its consensus algorithm PoW requires expensive computing load to maintain the consistency of blockchain. Xue et al. (2017) proposed a medical blockchain system MDSM based on an improved DPoS consensus algorithm, it can reduce the computing load of nodes and improve the security and efficiency of data sharing. However, at least 101 nodes of the medical institution federate servers (MIFS) and 20 nodes of the auditing federate serves (AFS) are required to start up this schema. This is no doubt that the start-up cost is high and the patient's privacy may be known by more nodes during the consensus process.

By analyzing the existing schemes, it can be found that combining blockchain with medical systems has facilitated the enhancement of service quality. Nevertheless, what cannot be ignored is that the privacy preserving of medical data between patients and disease research institutions has still remains challenging, especially the comprehensive privacy considerations when data shared among several entities involved smart contracts. Furthermore, few researches have focused on whether disease research institutions could obtain patients' medical data that meets their requirements, i.e. the data availability problem with consistent supply and demand. These issues are exactly the concerns of this paper.

1.3. *Contributions*

The goal of this paper is to provide a blockchain-based scheme for privacy-preserving and secure sharing of medical data between patients and disease research institutions. And meanwhile, the scheme devotes to solving the problem of data availability with consistent supply and demand, and realizes the efficient distributed consensus of transactions. The main contributions can be summarized as follows.

(i) A secure decentralized data sharing scheme based on blockchain is proposed to achieve privacy-preserving especially when several entities interact with the smart contract. Wherein, proxy re-encryption technology is adopted to ensure that research institutions can decrypt the shared intermediary ciphertext encrypted by the semi-trusted proxy cloud server.

(ii) In the proposed scheme, patients can prove that their medical data meets the requirements of research institutions without disclosing any privacy, by constructing a trusted zero-knowledge proof π based on zk-SNARKs and providing it to the smart contract for verification. Once the verification is passed, the transactions between patients and research institutions will be published in the blockchain for distributed consensus according to previous agreement. Wherein, PBFT consensus algorithm is selected due to the characteristic of low-cost computing power.

(iii) Security and privacy analysis and performance evaluation demonstrate that the proposed scheme achieves more desirable privacy-preserving and execution efficiency in terms of several metrics such as the speed of block generation and the number of startup nodes, compared to the existing solutions.

1.4. *Paper organization*

The rest of this paper is organized as follows. Section II describes and formalizes the preliminaries. In Section III, we make the problem statement and clarify the system model. The specific construction of our scheme is described in section IV. Section V evaluates the security and performance of the proposed scheme. Section VI concludes the whole paper.

2. Preliminaries

2.1. *Blockchain and smart contract*

A typical blockchain structure is shown in Fig. 1. Blockchain utilizes encrypted blocks to verify and store data, and employs P2P network and consensus mechanism to realize the verification, communication and trust establishment of distributed nodes.

Smart contract was introduced firstly by cryptologist Nick Szabo (Szabo, 1996) in 1994, which can facilitate safe and trusted business activities and realize complex blockchain applications by providing automated transactions without the supervision of an external entity such as banks, courts, or department of health service.

2.2. *Zero-knowledge proof*

Zero-Knowledge proof is a protocol that one party (the prover) can prove its knowledge of value to another party (the verifier), without revealing any information apart from the fact that it knows the value. Zero-Knowledge proof can be divided into interactive proof and non-interactive proof. When applied into blockchain, each node must check the validity of the transaction, and the sender exchanges information together with verification nodes, so non-interactive proof should be adopted in the blockchain system.

2.3. *Zero-knowledge succinct non-interactive arguments of knowledge*

Let C: $\mathbb{F}^n \times \mathbb{F}^h \rightarrow \mathbb{F}^l$ be an arithmetic circuit, and $\mathcal{R}_C=\{(\vec{x}, \vec{w})\} \subseteq \mathbb{F}^n \times \mathbb{F}^h$ be the corresponding circuit satisfaction relation, where $\vec{x} \in \mathbb{F}^n$ is called the statement and $\vec{w} \in \mathbb{F}^h$ is the witness. A zk-SNARK satisfies necessary properties including completeness, soundness and perfect zero-knowledge, more details regarding these properties can be found in Ben-Sasson et al. (2014).

A zk-SNARK for circuit satisfiability consists of three polynomial-time algorithms, including ***ZKPKeyGen***, ***Prove*** and ***Verify***, which will be defined and explained in Section ***IV-B***.

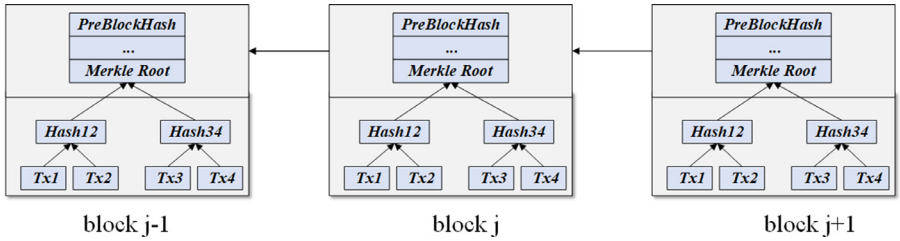

Fig. 1 – The typical structure of blockchain.

2.4. *Proxy re-encryption (PRE)*

To ensure the security of data sharing, the proxy re-encryption (Blaze et al., 1998; Ateniese et al., 2006) will be employed. It entrusts a semi-trusted proxy to transform the ciphertext encrypted with one party's public key into the intermediary ciphertext that can be decrypted by the other party's private key. During the whole process, the proxy cannot obtain any information related to the plaintext.

A PRE consists of multiple polynomial-time algorithms including ***Setup***, ***KeyGen***, ***ReKeyGen***, ***Encrypt***, ***Decrypt***, ***ReEncrypt***, and ***AuthSign***, which will be used and explained in Section ***IV-B***.

2.5. *Bilinear maps*

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ donate two multiplicative cycle groups generated with the same prime order p, A bilinear mapping e: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ has the following properties (Cheon and 0002, 2002):

1) **Bilinear**: $e(R^a, S^b)=e(R, S)^{ab}$ holds for any two $R, S\in \mathbb{G}_1$ and any two points $a, b\in \mathbb{Z}_p^*$.
2) **Non-Degeneracy**: there exits two points $R, S\in \mathbb{G}_1$ such that $e(R, S) \neq 1$.
3) **Computability**: there exists an efficiently computable algorithm for computing $e(R,S)$ for any two points $R,S \in \mathbb{G}_1$.

3. Problem statement and system model

3.1. *System model and problem statement*

Our solution combines blockchain, smart contracts, proxy re-encryption and zk-SNARK to achieve the privacy-preserving data sharing between patients and disease research institutions in intelligent medical system. The system model of our proposed scheme is shown in Fig. 2.

Totally seven entities are involved in the system model: 1) patients; 2) hospitals; 3) research institutions; 4) private key generation (PKG); 5) semi-trusted proxy cloud server; 6) blockchain; 7) smart contract. Their respective functions can be described as follows.

- Patients: as the actual owners of medical data, patients should own, control and conditionally share their private medical health data securely, and get benefits during this process.
- Hospitals: hospitals are incompletely trusted data manager and sometimes they are delegated by patients to encrypt medical data and outsource them to the semi-honest proxy cloud server. In this paper, patients can complete all tasks assigned to hospitals by themselves.
- Research institutions: research institutions are typical data consumers who need the medical data for health scientific research. They usually delegate smart contracts to publish attribute requirements for medical data. They do not trust the medical data provided by patients would meets their requirements, and they expect to be convinced of the data validity and availability by smart contract.
- Private key generation (PKG) center: As a fully trusted entity, PKG is responsible for generating the master key, system parameters, distributing public key and secret key to patients, hospitals (if necessary) and disease research institutions.
- Semi-trusted proxy cloud server: it is a semi-trusted entity responsible for storing and converting patients' original ciphertext to the intermediary ciphertext which can be decrypted by research institution's private key.
- Blockchain: blockchain is the core of our proposed scheme. In view of the tamper-resistance and traceable characteristics, the data stored in the blockchain will be kept as evidence. Furthermore, it is also responsible for executing distributed consensus of transactions.
- Smart contract: the smart contract clarifies in advance the requirements, specific format and the corresponding funding amount of medical data, and it will automatically judge the validity of zero-knowledge proof without the participation of the third-party.

In the system model, our proposed scheme mainly focuses on three closely connected scenarios.

In the first scenario, if patients believe that their medical data meets the requirements published by smart contracts, a zero-knowledge proof π generated by zk-SNARKs will be present to the smart contract for automatically judgement. The validity of π would decide the data availability with consistent supply and demand.

Once the verification is passed, the smart contract will inform the cloud server and the second scenario starts. Prior to this, patient's medical data encrypted by themselves or the authorized hospitals has been transmitted to the cloud server. The semi-honest proxy cloud server will transfer the encrypted medical data into the intermediary cyphertext based on the conversion key provided by patients. Subsequently, the intermediary cyphertext will be transmitted to the research

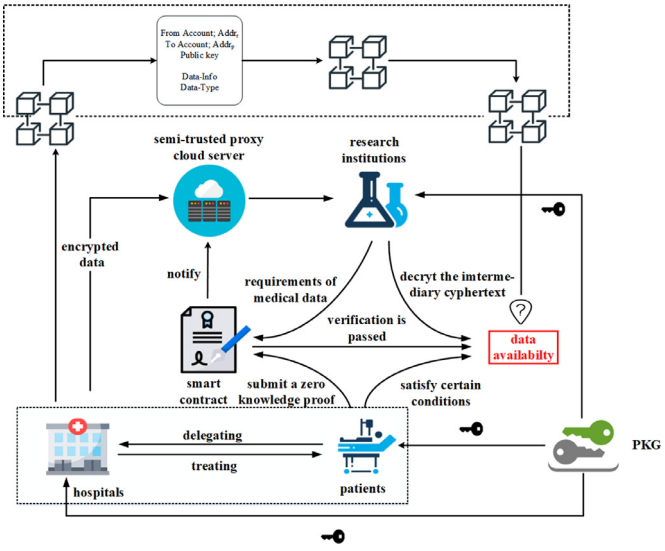

Fig. 2 – Blockchain-based scheme for privacy-preserving and secure data sharing.

institutions, who can decrypt it with its private key further to obtain the plaintext.

For authority or commercial interest considerations, in the third scenario, the transactions between patients and research institutions will be carried out distributed consensus and finally recorded in the blockchain. This means, for instance, patients are probably not permitted to provide their medical data to other research institutions if the requirements published by smart contracts clarified an exclusive license.

Under the above scenarios, the following three properties must be held: 1) Enable privacy protection of medical data; 2) Enable data availability with consistent supply and demand; 3) Enable mutual benefits between patients and disease research institutions.

3.2. *Security model and notations*

The private key generation center *PKG* is fully trusted, and it will not perform illegal manipulations. In addition, the blocks in our solution store only an index containing hashed pointers to a patient's records, and the corresponding encrypted data is outsourced and stored in the proxy cloud server. However, the proxy cloud server is considered as semi-trusted who will genuinely execute the protocol but deliberately pry into the patient's data privacy. And meanwhile, we assume that our encryption algorithm for medical data is sufficiently secure, neither an internal adversary nor an external adversary can crack the ciphertext unless obtaining the decryption key.

The notations used in this paper are given in Table 1.

Table 1 – Notation setting.

Notation	Description
λ	Security parameter
p_i	The i th patient
h_i	The i th hospital
r_i	The i th research institutions
PKG	Private key generation center
D	Patient's medical data
PK_p,PK_d	Public key of p, d
SK_p,SK_d	Secret key of p, d
$RK_{p \to d}$	Re-encryption key
EK_c	The key used to generate a zero-knowledge proof
VK_c	The key used to verify the zero-knowledge proof
σ_a	Digital signature
π	Zero-knowledge proof
$addr_p$	Blockchain account of p

4. The proposed scheme

4.1. *Blueprint of the proposed scheme*

The blueprint of our proposed scheme is composed of the following steps.

Step 1: the research institution r_i generates a zero knowledge proof π' by zk-SNARKs based on the medical data that satisfy their requirements, and then records the zero knowledge proof π', relevant calculation result R', and the hash value h' in the smart contract. And finally the smart contract will be released in the blockchain system. And meanwhile, the research institution will publish some key words of its requirements.

Step 2: the patient p_i (or authorizes and supervises the hospital h_i) executes ***Encrypt*** algorithm to encrypt his/her medical data D by PK_p, and then sends the ciphertext C_{PK_p} to the semi-trusted proxy cloud server.

Step 3: the patient p_i submits a transaction to blockchain for record, at the same time, he/she executes ***AuthSign*** algorithm to sign the transaction. It is noted that our scheme stores the patient's hash value of medical data on the blockchain based on the Hyperledger fabric.

Step 4: when the patient p_i wants to obtain some reward from research institutions r_i without exposing his/her

medical data directly. He/she needs to construct the circuit C according to the computing tasks of decentralized application based on smart contract, and executes ***Prove*** algorithm to generate a trusted zero-knowledge proof π based on his/her medical data on the premise that the patient considers her/his medical data conform to the key words of research institution's published requirements.

Step 5: the patient p_i submits the zero-knowledge proof π to the smart contract. By ***Verify*** algorithm, the smart contract will automatically compare the zero knowledge proof π, the calculation result R and the hash value h from patient with the zero knowledge proof π', the calculation result R' and the hash value h' calculated by the research institution, respectively.

Step 6: if the zero-knowledge proof verification is successful, the smart contract will notify the patient p_i to execute ***ReKeyGen*** algorithm to generate the re-encryption key $RK_{p\to d}$ (conversion key) with the public key PK_d of research institution. And then the patient p_i sends the re-encryption key $RK_{p\to d}$ to the semi-trusted proxy cloud server, where $RK_{p\to d}$ is encrypted by the public key of cloud server.

Step 7: the semi-trusted proxy cloud server decrypted the re-encryption key $RK_{p\to d}$ and executes ***ReEncrypt*** algorithm to convert the ciphertext C_{PK_p} into the intermediary ciphertext $C_{PK_{p\to d}}$ that can be decrypted by the research institution r_i, and then the proxy cloud server sends the ciphertext $C_{PK_{p\to d}}$ to r_i.

Step 8: the research institution r_i executes ***Decrypt*** algorithm to get the medical data D through its' private key EK_d. In this process, the semi-trusted proxy cloud server cannot obtain any information related to the plaintext.

Step 9: finally, a transaction is submitted to verification nodes by the smart contract. The transaction records the data sharing information between the patient p_i and the research institution r_i, and it will be published on the blockchain after verification with PBFT consensus algorithm.

4.2. *Specific implementation of our scheme*

The specific implementation of our proposed scheme is divided into ten phases which will be described respectively as follows.

4.2.1. *Initialization phase*

PKG first inputs a security parameter λ, chooses $\mathbb{G}_1$ and $\mathbb{G}_2$ be multiplicative cycle groups generated by the same prime p, and sets e: $\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a cryptographic bilinear map. And then *PKG* selects four secure hash functions H: {0, 1}$*\to${0,1}k, $H1$: {0, 1}$* \to \mathbb{G}_1$, $H2$: $\mathbb{G}_2 \to${0,1}k, $H3$: $\mathbb{G}_1 \times$ {0,1}$k \times$ {0,1}$l \to \mathbb{Z}_p^*$. Finally *PKG* randomly selects $a, b, c \in \mathbb{Z}_p^*$, $g, h \in \mathbb{G}_1$ are the different generators of $\mathbb{G}_1$, and then the public parameters and master secret key will be generated by ***Setup***$(1^\lambda) \to (PK, MSK)$, where $PK=(p, \mathbb{G}_1, \mathbb{G}_2, e, g, h, H, H1, H2, H3)$, $MSK=(a, b, c)$.

The patient p_i provides ID_p as his/her unique identifier to *PKG* who will generates the public/private key pair (PK_p, SK_p) of the patient using ***KeyGen***$(MSK, PK, ID_p) \to (PK_p, SK_p)$. And hospitals$\{ h_1, h_2, \ldots h_n \}$ (if necessary) and research institutions $\{ r_1, r_2, \ldots r_n \}$ can get key pairs respectively through the same procedure.

PKG randomly selects $t, x, y, z \in \mathbb{Z}_p^*$ and computes the following parameter values:

$$A1 = \frac{c+t}{a+b\cdot ID_p} A2 = h^t A3 = g^t$$

$$B1 = \frac{a+x}{a+b\cdot ID_p} B2 = \frac{b+y}{a+b\cdot ID_p} B3 = \frac{z}{a+b\cdot ID_p}$$

$$D1 = h^x D2 = h^y D3 = h^z$$

Finally the patient's private key $SK_p = (A_1, A_2, A_3, B_1, B_2, B_3, D_1, D_2, D_3)$ will be achieved, where (A_1, A_2, A_3) is used to decrypt the ciphertext, and $(B_1, B_2, B_3, D_1, D_2, D_3)$ is used to construct the conversion key $RK_{p\to d}$.

4.2.2. *Smart contract released phase*

The research institution r_i generates a zero-knowledge proof π' by zk-SNARKs based on its requirement for medical data such as age, height, weight, blood type, heart rate, disease type, diagnostic data, and treatment data. In our scheme, the patient is taken as the dominant role, so the concrete generation of zero knowledge proof will be described in ***Zero Knowledge Proof Generation Phase*** from the patient's perspective**,** and the similar generation procedure of research institution's zero knowledge proof will not be repeated here. And then the research institution r_i records the zero knowledge proof π', the calculation result R', and the hash value h' in the smart contract, which will be released in the blockchain system. And meanwhile, some key words from research institution's requirement will be released by smart contract.

4.2.3. *Join the network phase*

Several entities including patients, hospitals and research institutions that participate in the blockchain should be registered in fabric-ca. The fabric-ca will assign a blockchain address $addr_p$ and grant different permissions according to the roles of participating users, and meanwhile it is also responsible for verifying user identity and issuing related certificates such as the Enrollment Cert (E-Cert) and the Transaction Cert (T-Cert) based on their identifiers.

4.2.4. *Encryption phase*

After the patient's medical data produced, the patient p_i (or authorizes and supervises the hospital h_i) will encrypt his/her medical data $D=<d_1, d_2, \ldots, d_n>$ by ***Encrypt***$(PK, PK_p, <d_1, d_2, \ldots, d_n>) \to C_{PK_p}$, where $C_{PK_p}=(c_{pk_1}, c_{pk_2} \ldots c_{pk_n})$.

PKG randomly selects $r, s \in \mathbb{Z}_p^*$, and calculates the following parameter values,

$$c_{pk_1} = D \cdot e(g,\ h)^{c(r+s)}$$

$$c_{pk_2} = g^{\,r}$$

$$c_{pk_3} = h^{\,s}$$

$$c_{pk_4} = e(g,\ h)^{(a+b\cdot IDp)(r+s)}$$

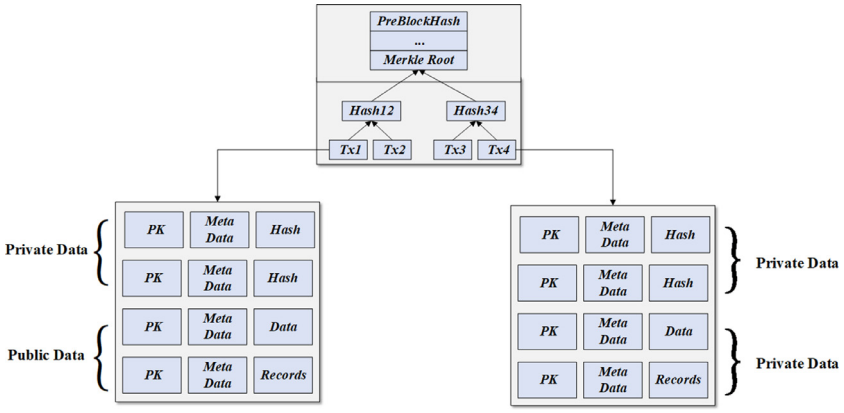

Fig. 3 – Transaction form.

And then the patient (or the authorized hospital) uploads the ciphertext C_{PK_p} to the semi-trusted proxy cloud server for storage. We assume that the semi-trusted proxy cloud server cannot modify patients' medical data, and it will dutifully perform our specified operations.

4.2.5. *Data recorded in blockchain phase*

Our scheme stores an index containing hashed pointers to the patient's records on the blockchain based on the Hyperledger Fabric platform. The details of medical data will be outsourced to the cloud server. The patient p_i submits the hash value of his medical data $D=<d_1, d_2,\ldots, d_n>$ to generate a transaction form as shown in Fig. 3, and then attaches his/her digital signature $\sigma_a=AuthSign(SK_p, H(<d_1, d_2,\ldots, d_n>))$ on the transaction form. If the transaction is verified by the verification nodes, it will be recorded on the blockchain.

4.2.6. *Zero knowledge proof generation phase*

The patient p_i completes the initial judgement whether his/her medical data conforms to the key words of the research institution's requirements. When the patient p_i expects to check whether his/her medical data really meets the specific attributes required by the research institution, he/she needs to attach his/her digital signature on his/her medical data, which was submitted to zk-SNARKs in order to generate a zero-knowledge proof $\boldsymbol{\pi}$. Wherein, the digital signature of p_i and $\boldsymbol{\pi}$ will be constructed in the following steps:

Step 1: according to the patient's ID_p, the current local time T and the patient's private medical data D, the extended information $\delta=(D,T,ID_p)$ can be generated.

Step 2: take the extended information $\delta=(D,T,ID_p)$ as input and fill a random number r for hash operation, $H(\delta, r)$ can be calculated.

Step 3: generate the digital signature $\sigma_a=\text{AuthSign}(SK_p, H(\delta, r))$.

Step 4: the patient p_i constructs the circuit C: $\mathbb{F}^n \times \mathbb{F}^h \rightarrow \mathbb{F}^l$ obtained from the calculation task of decentralized application based on the smart contract. The circuit C takes the public parameter vector $<PK_1, PK_2 \ldots PK_n>$, a private medical data set $<d_1, d_2,\ldots, d_n, r>$ and the auxiliary data $<ID_p, T>$ as input, where ID_p, T and r are the patient's identification, timestamp and random number, respectively. And then a result R and a hash value h can be output to verify the data authenticity and availability.

$C(<d_1, d_2,\ldots, d_n>) \rightarrow (R, h)$

The circuit structure diagram is shown in Fig. 4.

Step 5: the security parameter λ and the circuit C obtained from the computing task will be taken as input parameters in order to calculate the key pair, where EK_c is used to generate a zero-knowledge proof and VK_c is used to verify the zero-knowledge proof.

$$ZKPKeyGen(1^{\lambda}, C) \rightarrow (EKc, VKc)$$

Step 6: ***Prove*** algorithm takes the following parameters as input: the zero-knowledge proof generation key EK_c, the patients' medical data D, signature σ_a, the result R and the hash value h generated in Step 4, and then a credible zero-knowledge proof π will be output.

$$Prove(EKc, D, R, h, \sigma_a) \rightarrow \pi$$

4.2.7. *Zero knowledge proof verification phase*

The patient submits the zero-knowledge proof π to the smart contract. The smart contract will automatically verify whether the zero-knowledge proof π meets the requirements of the research institution without the attendance of a third-party.

$$Verify(VKc, PKp, \pi, R, h, \sigma_a) \rightarrow (True\ or\ false)$$

Firstly, the patient's digital signature σ_a will be verified with the patient's public key PK_p, and then the zero knowledge proof π will also be checked with the verification key VK_c by zk-SNARKs. If the verifications are both completed, the smart contract will compare the zero knowledge proof π, the calculation result R and the hash value h calculated based on patient's medical data with the zero knowledge proof π', the calculation result R' and the hash value h' calculated based on the research institution's requirements, respectively. If the verifications are all completed, a result like reject (false) or accept (true) will be output.

4.2.8. *ReEncryption phase*

If the verification of zero-knowledge proof is successful, then the patient p_i generates the conversion key $RK_{p \rightarrow d}$ with the

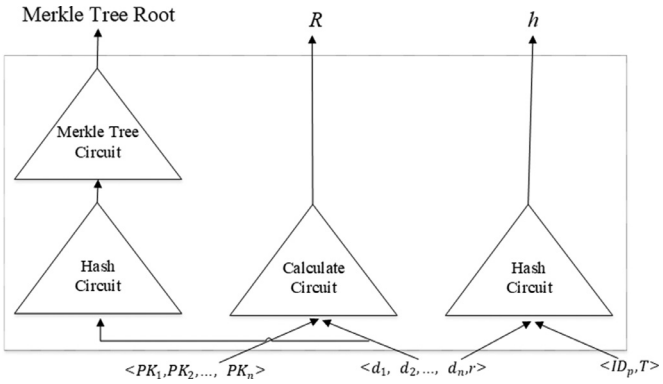

Fig. 4 – Circuit structure diagram.

public key PK_d provided by the research institution r_i as follows:

$$ReKeyGen(PK,\ SKp,\ PKd) \rightarrow RK_{p\rightarrow d}$$

PKG randomly selects $k_1, k_2 \in \mathbb{Z}_p^*$ and computes the following parameter values:

$$rk_1 = (k_1B_3 + B_1) + (k_2B_3 + B_2)*IDp$$

$$rk_2 = (D_1D_3^{k_1})(D_2D_3^{k_2})^{IDp}$$

$$RK_{p\rightarrow d} = (rk_1, rk_2)$$

And then the patient sends the conversion key to the semi-trusted proxy cloud server, which can be encrypted by the public key of cloud server. The proxy cloud sever will transfer the ciphertext C_{PK_p} into the intermediary ciphertext $C_{PK_{p\rightarrow d}}$, which can be decrypted by research institution's secret key SK_d. Subsequently, the proxy cloud server sends the intermediary ciphertext $C_{PK_{p\rightarrow d}}$ to the research institution.

The semi-trusted proxy cloud server needs to figure out the results as follows:

$$c'_{pk_1} = c_{pk_1}$$

$$c'_{pk_2} = c_{pk_2}$$

$$c'_{pk_3} = \frac{c_{pk_3}^{k_1}}{e\left(c_{pk_2}, rk_2\right)}$$

$$C_{PK_{p\rightarrow d}} = \left(c'_{pk_1}, c'_{pk_2}, c'_{pk_3}\right)$$

4.2.9. *Decryption phase*

The research institution r_i acquires the intermediary ciphertext $C_{PK_{p\rightarrow d}}$ from the proxy, and then it can decrypt the ciphertext through its SK_d. In this process, the semi-trusted proxy cloud server cannot obtain any information related to the plaintext.

$$Decrypt\left(PK,\ C_{PK_{p\rightarrow d}},\ SKd\right) \rightarrow D$$

The research institution r_i decrypt the intermediary ciphertext $C_{PK_{p\rightarrow d}}$ and get the value of D.

$$D = \frac{c_{pk_1} \cdot e\left(c_{pk_2}, A_2\right)}{C_{pk_1}^{A_1}}$$

4.2.10. *Consensus phase*

After the research institution has decrypted and obtained the patient's medical data, the smart contract will submit the transaction to verification nodes, which requires the digital signatures from the patient and the research institution. If the transaction is examined by verification nodes via PBFT (Castro and Liskov 2002) consensus algorithm, it will be published and recorded on the blockchain.

We assume that there is a total of 3f +1 verification nodes and only one leader node, which is calculated by the formula $P = V \bmod |R|$, where P is the primary node number, V is the view number, and $|R|$ is the number of duplicate nodes. The other remainders are accounting nodes. Each verification node broadcasts the transaction sent from the smart contract to the whole network. The work flow can be detailed as follows.

Step 1: after the leader node receives the transactions, the leader sorts the transactions firstly (if necessary) and assigns serial numbers to the transactions, and then multicasts a PRE-PREPARE message with the transactions and serial numbers to other accounting nodes.

Step 2: after receiving transactions from the leader node, each accounting node verifies whether the signatures, timestamps, serial numbers are valid. If valid, the accounting node multicasts a PREPARE message containing the signature of authentication result.

Step 3: if an accounting node receives more than 2f PREPARE messages from different nodes, it indicates that the PREPARE phase has been completed and the accounting node multicasts a COMMIT message to other accounting nodes.

Step 4: if an accounting node receives more than 2f+1 different commit message (including itself), it considers that the COMMIT phase is completed and all accounting nodes have reached a consensus to record these transactions to a new block.

Step 5: finally, the accounting node returns the corresponding reply to the smart contract who generated the transactions. If the consensus fails, the leader will be changed and the PRE-PREPARE phase will be restarted once again.

5. Analysis of our scheme

In this section, we will evaluate the proposed scheme from the three aspects.

1) Whether the proposed scheme can satisfy the basic security and privacy requirements for medical data sharing based on blockchain.
2) Several metrics such as "less computing cost", "fewer startup nodes" and "privacy protection" will be used to performance evaluation between the proposed scheme and the existing medical data sharing schemes based on blockchain (Azaria et al. 2016; Xue et al. 2017; Kuo 2018).
3) The time to generate the zero-knowledge key pairs, the time to generate and verify the zero-knowledge proof and the size of the zero-knowledge proof by using libSNARK ([CSL STYLE ERROR: reference with no printed form.]) will be analyzed.

5.1. *Security and privacy-preserving analysis*

5.1.1. *Confidentiality*

In our scheme, all medical data are encrypted by patients using a secure encryption algorithm before uploaded to the semi-trusted proxy cloud server. We have assumed that the encryption algorithm for medical data is sufficiently secure in Security Model, neither an internal adversary nor an external adversary can crack the ciphertext without obtaining the decryption key. So the semi-trusted proxy cloud server or other malicious attackers cannot deduce any information about the content of any ciphertext.

Furthermore, the encrypted medical data can be re-encrypted as the intermediary ciphertext using the conversion key provided by the patient. Only research institutions that have been authorized by the data owner can decrypt the intermediary ciphertext to get the valuable plaintext data. Smart contracts and other entities even have no opportunities to touch the encrypted medical data.

Patients adopts the public key of cloud server to encrypt the conversion key (re-encrypted key) to prevent adversary from cracking the re-encrypted key.

5.1.2. *Availability*

In our scheme, only authorized entities can use their private keys to decrypt the patient's medical data. In addition, patients can generate a fully trusted zero-knowledge proof π based on their own medical data and submit it to smart contracts on the blockchain. Based on the characteristics of zero-knowledge proof, π can be used to verify whether patients' medical data meets certain conditions suggested by research institutions. This feature ensures data availability with supply and demand matching.

5.1.3. *Integrity*

In our scheme, patients need to attach their digital signature to the zero-knowledge proof generated by their medical data, while the private key of the digital signature can only be kept by themselves and cannot be obtained by other entities, which ensures the authenticity of the zero-knowledge proof. The patients' medical data recorded in the blockchain has already reached consensus by PBFT algorithm. The order and the transaction of blocks are protected with a hash chain, the hash value for each block is unique and the hash values of the other blocks would be changed once countering tampering attacks. This feature ensures data integrity.

5.1.4. *Privacy-preserving*

At the stage of registration, patients or research institutions will be checked strictly by fabric-ca to ensure that all participators of the blockchain are legitimate, and then the fabric-ca will generate a pseudo identity for each participator. Thus, the participator privacy will be protected since the pseudo identity is employed instead of true identity in the subsequent processes. During the data sharing process, the patient's data privacy would not be disclosed by any entity who participate the interactions with smart contracts, and smart contracts can only obtain the zero-knowledge proof π instead of the original private data.

Furthermore, the research institutions just publish some key words instead of the entire requirements in order to achieve partial privacy protection. This way prevents the adversary from forge the medical data according to the entire requirements.

5.1.5. *Traceability*

Our scheme will provide a data availability with consistent supply and demand. Once patients and medical institutions reach a consensus, their behavior of sharing medical data will be stored in the blockchain. If either side has an illegal operation, for example, the patient sold his/her medical data to other research institutions without following the previous exclusive license agreement, it will be held accountable.

5.1.6. *Avoid single point of failure*

A decentralized storage system fabric is employed in our scheme, which effectively solves the single point of failure problem. All entities in our scheme monitor all transactions and messages. Besides, access control enabled by the blockchain technique is running in a peer-to-peer manner among decentralized entities.

5.2. *Performance evaluation*

We compare the blockchain-based medical data sharing schemes MedRec (Azaria et al. 2016), ModelChain (Kuo 2018), MDSM (Xue et al. 2017) with the proposed scheme in terms of three metrics (less computing cost, fewer startup nodes, and privacy protection, respectively).

The scheme in Azaria et al. (2016) uses the PoW consensus mechanism that requires abundant computing power to maintain the consistency of blockchain, and meanwhile it needs lots of startup nodes. The consensus algorithm POI suggested in Kuo (2018) also needs great computing power

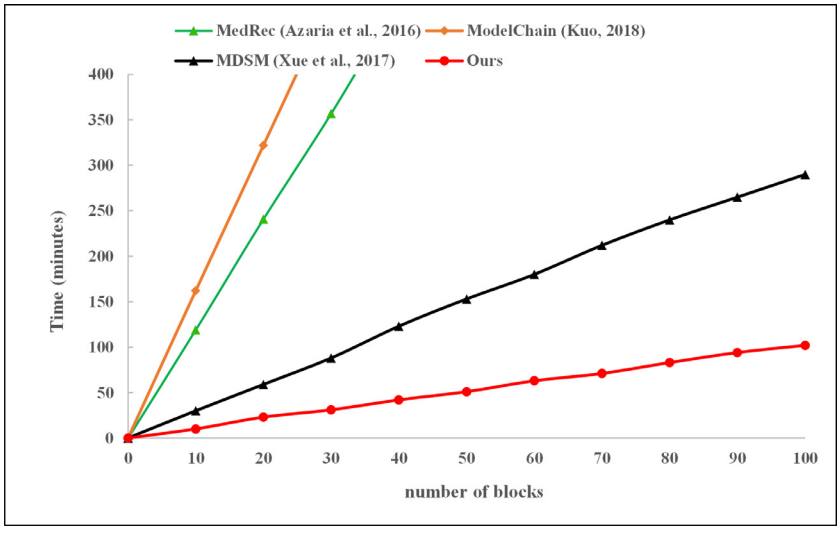

Fig. 5 – Comparison of different schemes in terms of block generation time.

Table 2 – Performance comparisons of the four schemes (Support √ Non-Support ×).

	Less computing cost	Fewer startup nodes	Privacy protection
MedRec(PoW)	×	×	×
ModelChain(PoI)	×	×	×
MDSM(DPoS)	√	×	√
Our scheme(PBFT)	√	√	√

and startup nodes. Moreover, both schemes in Azaria et al. (2016) and Kuo (2018) don't provide privacy protection of patient's medical data. The medical data sharing scheme in Xue et al. (2017) designed an improved consensus mechanism DPoS, which can improve the efficiency, but it requires at least 121 nodes to start. PBFT consensus algorithm is selected in our scheme, which avoids performing mining calculations, requires lower computing power and does not need to set the proportion of votes manually, so it satisfies the metric of less computing cost. Moreover, our scheme needs only four nodes to start and run, with lower start-up cost. In contrast, MDSM requires a fixed Medical Institution Federate servers (MIFS) with 100 nodes and Audit Federate servers (AFS) with 20 nodes, so our scheme meets the metric of fewer startup nodes. Finally, the medical data submitted to smart contract is generated to a zero-knowledge proof, which avoids the exposure of the original data, so it meets the demand of privacy protection. Thus, From Table. 2, it can be found that our scheme satisfies all the metrics.

In the smart medical system based on blockchain, several schemes like MedRec adopt the PoW algorithm, which takes about ten minutes to generate one block, that is unacceptable in highly concurrent smart medical scenarios. However, MDSM adopts DPoS consensus algorithm innovatively, which decreases the block generation time to 3 minutes. Furthermore, our proposed scheme is also compared with the other three ones in terms of block generation time. As shown in Fig. 5, our scheme achieves the optimal performance with 33% growth rate of block generation speed compared with the rank-2 MDSM scheme. Specifically, we conduct the experiments on block generation time of different schemes on a Ubuntu 18.04 with an Intel Core i7-4770M CPU @3.40GHz 8GB of RAM.

Next, we conduct the following experiments on the same environments and set the security parameter λ with 128 bits. We store the hash value of patients' medical data and the shared information between patients and research institutions on fabric platform. The implementation of zero-knowledge proof is based on a zk-SNARK of libSNARK, provided by the Zerocoin Electric Coin Company.

Due to adopting the non-interactive zero-knowledge proof (NIZK) model, the biggest bottleneck of our scheme is the time consume to generate the NIZK proof. We simulated the model's workflow and mainly evaluate the time to generate a NIZK key pairs, the time to generate a NIZK proof, the time to verify a NIZK proof, and the size of a NIZK proof. We repeat each experiment for 100 times and calculate the average of these metrics.

As shown in Figs. 6–8, in our scheme, the time to generate the proving key EK_c and verification key VK_c is about 16 seconds, which will not increase with the number of circuit inputs. Specifically, even the medical data as the input of circuit is constantly increasing, the time to generate a NIZK proof key pair will not increase, which greatly improves scheme scalability. Notably, the time to verify a NIZK proof increases linearly with the number of circuit inputs. However, even the number of circuit inputs is 1000, the verification time is less than 1 second, and it is still an acceptable time constraint.

Furthermore, as shown in Table 3, the verification key size increases from 3.5 KB to 31.5 KB and the NIZK proof size increases form 12.9KB to 125.4KB. It is a direct consequence of the increase of circuit inputs and the result remains within the acceptable range (Backes et al. 2015).

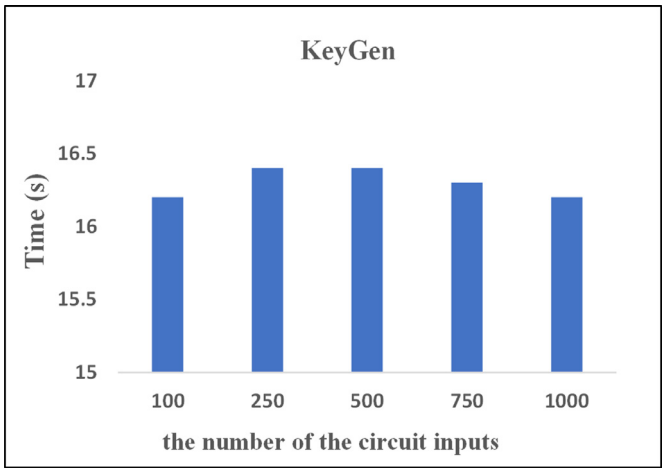

Fig. 6 – The time to generate a NIZK key pair.

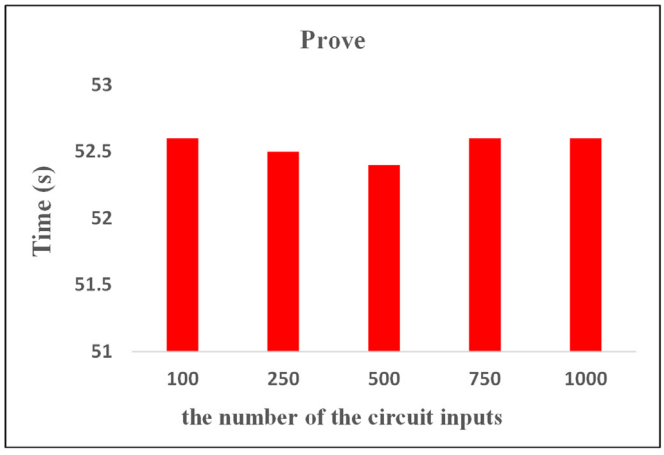

Fig. 7 – The time to generate a NIZK proof.

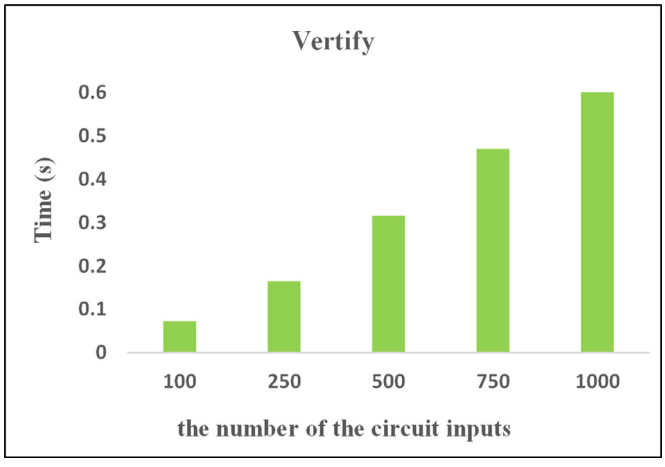

Fig. 8 – The time to verify a NIZK proof.

Table 3 – The size of proving key, verification key, the proof.

Inputs	Proving key size	Verification key size	Proof size
100	15.3 MB	3.5 KB	12.9 KB
250	15.3 MB	8.2 KB	31.6 KB
500	15.3 MB	16.0 KB	62.9 KB
750	15.3 MB	23.8 KB	94.1 KB
1000	15.3 MB	31.5 KB	125.4 KB

Table 4 – Comparison between our scheme and PGHR.

	PGHR	Our scheme
KeyGen	299 s	16.3 s
Prove	491 s	52 s
Vertify	0.062 s	0.614 s
proving key size	319 MB	15.3 MB
Verification key size	31 KB	125.4 KB

Next, we compare our scheme with PGHR (Backes et al. 2015) based on zk-SNARK as well which considers 1000 authenticated inputs. It can be seen from Table 4, our scheme can achieve the following advantages in contrast with PGHR: 18 × speed-up (16.3s vs. 299s) of the time to generate a NIZK key pairs, 20 × reduction (15.3MB vs. 319MB) of the proving key size, and 8 × speed-up (52s vs. 491s) in generating a NIZK proof. The reason lies in the KeyGen in our scheme contains only one multiplicative cycle groups $\mathbb{G}_1$ more than PGHR, which will decrease the time to generate a NIZK key pairs and the size of proving key.

However, our scheme has to perform some additional computation to verify the NIZK proof, so the time to verify a zero-knowledge proof (0.614s vs.0.062s) and the verification key size (125.4KB vs. 31KB) are slightly worse than PGHR, but the results still can be considered feasibly.

6. Conclusion

The growing demand for health has led to a booming development of hospitals and medical institutions, which has also facilitated the exponential increase of medical and health data. Researchers have been seeking a trade-off that allows massive amounts of medical data to become a valuable resource for research institutions while at the same time to maintain data privacy-preserving as much as possible. In view of this challenging problem, a secure data sharing scheme of intelligent medical system was proposed, which combined blockchain, smart contract and zero-knowledge proof to address two issues: one is privacy protection of medical data when shared by several entities; the other is data availability and consistency between patients (supply) and research institutions (demand).

Specifically, the verification of zero-knowledge proof enabled smart contracts to automatically judge whether the patient's medical data meets the given requirements from research institutions without revealing patients' privacy. Once verified, the proxy re-encryption mechanism would be employed to transfer the encrypted medical data to the intermediary ciphertext which could only be decrypted by the authorized research institutions. Finally, for the consideration of bilateral interests, the transaction between patients and research institutions was submitted to distributed consensus through PBFT algorithm.

Security and privacy analysis have shown our proposal could achieve confidentiality, availability, integrity and privacy-preserving. In addition, performance evaluation based on experiments demonstrated the proposed scheme obtained more satisfactory implementation efficiency compared with other typical schemes.

In the next work, we plan to further improve the efficiency of generating zero-knowledge proofs by optimizing the implementation process. How to resist the conspiracy attacks launched by several entities will become one of the issues that need to be addressed in the future.

Author Statement

Haiping Huang: Conceptualization, Methodology, Scheme design, Software; **Peng Zhu**: Data curation, Writing-Original draft preparation, Experiment; **Fu Xiao**: Supervision, Investigation, Validation; Xiang Sun: Writing-Reviewing and Editing; **Qinglong Huang**: Software, Validation.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowlegements

This work was supported by the National Key Research and Development Program [grant number 2018YFB0803403]; the National Natural Science Foundation of China [grant number 61672297, and 61872194]; the Key Research and Development Program of Jiangsu Province [grant number BE2017742].

REFERENCES

Ateniese G, Fu K, Green M, Hohenberger S. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans. Inf. Syst. Secur. 2006.

Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016, 2016.

Backes M, Barbosa M, Fiore D, Reischuk RM. ADSNARK: nearly practical and privacy-preserving proofs on authenticated data. Proceedings - IEEE Symposium on Security and Privacy, 2015.

Ben-Sasson E, Chiesa A, Garman C, Green M, Miers I, Tromer E, et al. Zerocash: decentralized anonymous payments from bitcoin. Proceedings - IEEE Symposium on Security and Privacy, 2014.

Ben-Sasson E, Chiesa A, Genkin D, Tromer E, Virza M. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). SNARKs for C: verifying program executions succinctly and in zero knowledge; 2013.

Bendiab K, Kolokotronis N, Shiaeles S, Boucherkha S. WiP: a novel blockchain-based trust model for cloud identity management. Proceedings - IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, IEEE 16th International Conference on Pervasive Intelligence and Computing, IEEE 4th International Conference on Big Data Intelligence and Computing and IEEE 3, 2018.

Blaze M, Bleumer G, Strauss M. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Divertible protocols and atomic proxy cryptography; 1998.

Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst. 2002.

Cheon JH, 0002 DHL. Diffie-Hellman problems and bilinear maps. IACR Cryptol. ePrint Arch 2002.

Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. 2018.

Dimitrov D V. Medical internet of things and big data in healthcare. Healthc. Inform. Res. [Internet] 2016;22(3):156. Available from: http://synapse.koreamed.org/DOIx.php?id=10.4258/hir.2016.22.3.156.

Elhoseny M, Abdelaziz A, Salama AS, Riad AM, Muhammad K, Sangaiah AK. A hybrid model of Internet of Things and cloud computing to manage big data in health services applications. Fut. Gener. Comput. Syst. [Internet] 2018;86:1383–94. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0167739X17322021.

Fimiani G. Supporting privacy in a cloud-based health information system by means of fuzzy conditional identity-based proxy re-encryption (FCI-PRE). In: Proceedings - 32nd IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2018. 2018.

Goldreich O, Micali S, Wigderson AVI. Proofs that yield nothing but their validity or AII languages in NP have zero-knowledge proof systems. J. ACM 1991.

Ibraimi L, Tang Q, Hartel P, Jonker W. A type-and-identity-based proxy re-encryption scheme and its application in healthcare. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2008.

Ivan D. Moving toward a blockchain-based method for the secure storage of patient records. NIST Work Blockchain Healthc. 2016.

Kuo TC-N-M. Modelchain: decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. arXiv Prepr arXiv180201746. 2018;

Li H, Zhu L, Shen M, Gao F, Tao X, Liu S. Blockchain-based data preservation system for medical data. J. Med. Syst. [Internet] 2018 Aug 28;42(8):141. Available from: http://link.springer.com/10.1007/s10916-018-0997-3.

Li X, Mei Y. A Blockchain Privacy Protection Scheme Based on Ring Signature. IEEE Access 2020;8:76765–72.

Liang J, Qin Z, Xiao S, Zhang J, Yin H, Li K. Privacy-preserving range query over multi-source electronic health records in public clouds. J. Parallel Distrib. Comput. 2020.

Miao Y, Tong Q, Choo K-KR, Liu X, Deng RH, Li H. Secure Online/offline data sharing framework for cloud-assisted industrial internet of things. IEEE Internet Things J. [Internet] 2019;6(5):8681–91. Available from: https://ieeexplore.ieee.org/document/8736869/.

Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Consulted 2008:1–9 Consulted. 2008. doi:10.1007/s10838-008-9062-0stem.

Szabo NSmart. contracts: building blocks for digital free markets. Extropy J. Transhuman Thought 1996.

Tene O, Evans K, Gencarelli B, Maldoff G, Zanfir-Fortuna G. GDPR at year one: enter the designers and engineers. IEEE Secur. Priv. 2019.

Vazirani AA, O'Donoghue O, Brindley D, Meinert E. Blockchain vehicles for efficient medical record management. npj Digit Med [Internet]. 2020;3(1):1–5. Available from: http://dx.doi.org/10.1038/s41746-019-0211-0

Wang H, Wang Q, He D. Blockchain-based private provable data possession. IEEE Trans. Depend. Secur. Comput. [Internet] 2019a. PP(c):1–1. Available from: https://ieeexplore.ieee.org/document/8884171/.

Wang S, Ouyang L, Yuan Y, Ni X, Han X, Wang FY. Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Trans. Syst. Man Cybern. Syst. 2019b.

Xue TF, Fu QC, Wang C, Wang XY. A medical data sharing model via blockchain. Zidonghua Xuebao/Acta Autom Sin 2017.

Yang Y, Chen T. Analysis and visualization implementation of medical big data resource sharing mechanism based on deep learning. IEEE Access [Internet] 2019;7:156077–88. Available from: https://ieeexplore.ieee.org/document/8884176/.

Zhang Y, Xu C, Li H, Yang K, Zhou J, Lin X. HealthDep: an efficient and secure deduplication scheme for cloud-assisted eHealth systems. IEEE Trans. Ind. Inform. 2018.

Zheng X, Mukkamala RR, Vatrapu R, Ordieres-Mere J. In: 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services, Healthcom 2018. Blockchain-based personal health data sharing system using cloud storage; 2018.

libsnark [Internet]. Available from: https://github.com/scipr-lab/libsnark