A Decentralized Threshold Signature Scheme of Blockchain-Based Medical Cyber Physical Systems

Xianfei Zhou
Wuhu Institute of Technology
Jing Huang
Anhui Normal University
Fulong Chen (long005@mail.ahnu.edu.cn)
Anhui Normal University
Yuqing Tang
Anhui Normal University
Canlin Wang
Anhui Normal University

Research Article

Keywords: Blockchain Technology, Security Storage, Cryptography, MCPS

Posted Date: September 16th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-869835/v1

A Decentralized Threshold Signature Scheme of Blockchain-Based Medical Cyber Physical Systems

Xianfei Zhou[a], Jing Huang [b], Fulong Chen[b,*], Yuqing Tang[b], and Canlin Wang[b]
[a]Wuhu Institute of Technology, Wuhu, Anhui 241002, China
[b]Anhui Normal University, Wuhu, Anhui 241002,China

Abstract—With the rapid development of medical information, the medical cyber system is rapidly transforming, and medical information sharing faces new challenges. Blockchain technology is a revolutionary technology. It has the characteristics of tamper-proof and privacy-preserving, and has natural protection for big data systems, that can be used in medical systems. In this paper,we proposed to store medical cyber physical data in a mixed blockchain with private blockchain and consortium blockchain in order to realize the secure storage of medical cyber physical data by the tamper-resistant and sharing of blockchain technology. In the system, a threshold signature system based on blockhain is also proposed. Aiming at the situation that medical accidents are easy to occur in multidisciplinary joint consultation in the medical process, this paper proposes to use threshold signature for joint consultation. Using the security and threshold of threshold signature, treatment can be carried out when the threshold number is reached, and medical data can be uploaded to the consortium blockchain. The security analysis and performance analysis show that the scheme has advantages in safety and performance and is suitable for the medical environment to a certain extent.

Index Terms—Blockchain Technology, Security Storage, Cryptography,MCPS

1 INTRODUCTION

In the medical cyber physical system, medical data security is very important, e.g., the integrity, effectiveness and authenticity of medical data. However, medical information security is facing new challenges. First of all, it lacks of unified planning of medical cyber physical system platform [1] to manage various sources and rapid updating massive medical data, which causing disordered data standards, difficult data sharing, and serious information isolation. Second, patients have not participated in the accessing control strategy of medical information, and division of authority in the medical information system is not clear, which can not realize the personalized privacy protection of patients [2].

In the medical cyber physical system, patient's medical data security and privacy can not be ignored. Data security means the integrity, validity and authenticity of medical data[3]. The safe storage, transmission, and access of the medical cyber physical system are the most important guarantee for medical data sharing and informatization, ensuring the data that can complete the medical diagnosis and treatment without leakage, loss, or tampering. Blockchain is a distributed secure data storage system, which has the characteristics of tamper-proof, decentralization, and data encryption [4]. The decentralization of blockchain can solve the trust problem for the medical cyber physical system, data encryption can protect data from being tampered. The distributed architecture is also fit for the development direction of intelligent medical in the future.

Sangeetha et al. [5] proposed the blockchain storage method for electronic health records, saving the data into the blockchain, making the data easy to query and be more secure. Now, most of the research and application of "MCPS + blockchain" is on the top application or architecture design [6–8], ignoring the bottom data's storage, transmission and access security. Only when the bottom data is guaranteed, the security of the top application and architecture can be more improved.

Blockchain system utilizes methods such as hash function, digital timestamps, asymmetric encryption, and digital signature in cryptography to solve problems such as data integrity and data security.

Digital signature in the blockchain system uses asymmetric encryption principle. The process needs to have both public key and private key pairs. The security of a digital signature depends on the key used in the signature. Threshold signature technology can distribute the signature key to other users in a threshold way, which can partly solve key leakage and key loss in key management [9]. In the (t, n) threshold signature system, the original signer gives n secret shares. In the signature process, only when no less than t participants agree to cooperate, can generate a valid group signature. Otherwise, can not recover the signature representing the group member.

The paper proceeds as follows. Section 2 discusses previous studies related to our research. Basic concepts about the threshold signature in Section 3. Section 4 describes the proposed Blockchain_based model. Section 5 describes threshold scenarios and the threshold signature working process. Section 6 describes the security and the performance efficiency analysis. The conclusion and future work are presented in Section 7.

2 RELATED WORKS

2.1 BlockChain

Blockchain is a distributed storage network, and all the data is linked by timestamps in the form of data blocks. It adopts data encryption technology, and the data blocks are divided into data block header and block body. The information of the block header includes the hash information and nonce values of the front block, ensuring that each block is different and can access all the blocks through the hash information. The block body contains the information to be saved and transmitted[10].

According to the degree of openness, blockchain can be divided into three categories: public blockchain, private blockchain, and consortium blockchain.

Public blockchain: Any node of the public blockchain is open to everyone, the famous public blockchain is bitcoin [11]. It has the characteristic of full openness and decentralization, and everyone in the network can access the data and can not tamper it.

Private blockchain: private blockchains is a blockchain system that open to individuals or entities. Permissions of each node in the system require the organization to assign, and the amount of data open to each node is determined by the organization depending on the situation. it is a centralized system, but the data read and write is very fast [12].

Consortium blockchain: consortium blockchain has the characteristic between private blockchain and public blockchain. It is run by several organizations. Each organization manages one or more nodes, and the data are allowed to access in the system, it is a partial-decentralized blockchain.

A.Zhang et al. [13] proposed an e-Health system via consortium and gived out the security and privacy-preserving data sharing method. The data store in consortium blockchain and could access with keyword search. Azaria et al. [14] used ethereum blockchain to realize a medical information sharing platform combining medical blockchain and big data. C.Zhang et al. [15] proposed a medical blockchain system based on Consortium blockchain, which was a multi-node maintenance and sharing system, and prevented medical data from being tampered with or leaked and used to solve these medical problems.

2.2 Threshold signature

In recent years, there are a lot of research achievements around blockchain-based aggregate signature [16], multi-signature [17], and ring signature [18]. Threshold signature is a kind of multi-signature. The threshold signature scheme can improve security and privacy in many scenarios.

According to the manager's identity, the threshold signature scheme can be divided into two types: with trusted center[19]and without trusted center [20]. In the threshold signature scheme with trusted center, the trusted center plays the role of manager. It undertakes most of the management tasks, which can not avoid the authority deception of the trusted center. In contrast,the threshold signature scheme without trusted center does not need to consider centralization problems. In order to propose a threshold signature scheme based on blockchain, we need to consider the decentralization of blockchain.

Secret sharing was first proposed by Shamir [21] in 1979, and a (t, n) threshold secret sharing scheme based on Lagrange interpolation polynomial was proposed. However, the scheme could not prevent the fraud of the secret distributor and the participants, and the secret shares obtained by the participants can only be used once. If there were multiple keys to be shared simultaneously, the secret shares needed to be distributed multiple times.

Asmuth and Bloom [22] applied the CRT(Chinese Remainder Theorem) and proposed a threshold secret sharing scheme based on the CRT. Compared with Shamir's secret sharing scheme, this scheme had less computation, but the scheme didn't verify the correctness of the data during transmission.

B.Wang et al. [20] proposed (t,n) Threshold Signature Scheme without a trusted center. Using Shamir(t,n) threshold scheme, modular operation over the finite field $GF(p)$ and Lagrange interpolation polynomial, designed a verifiable multi-secret sharing threshold scheme, which solved the problem of member's private key revealed caused by traditional secret sharing scheme, but the scheme didn't consider the actual signature member's identity information.Y.Cheng et.al. [23] proposed a verifiable (t,n) threshold secret sharing scheme by combining ElGamal scheme with Asmuth-Bloom scheme. The scheme designed effective measures to prevent the secret share from being tampered in the process of distribution. Also, it provided a method to verify whether the participants were given the correct secret shares. However, the security of this scheme is based on the difficulty of solving discrete logarithm problems in finite fields.

T.Wang et al. [24] proposed a threshold group signature scheme without a trusted center. In the scheme, the signature organizer had the power of selecting signature members. When the threshold signature was synthesized, the private key was added to verify the threshold signature corresponding to the public key. The organizer completely controlled authority of giving out a signature, and the scheme was vulnerable to attackers. Al-Zubaidie et al. [25] proposed PAX (Pseudonymization and Anonymization with the XACML) modular system in the health-care system. the system was used to solve the privacy problem in the electronic health-care system and the security access decision issues for patient data, and adopted the threshold scheme based on Shamir. In this scheme, proved that Shamir scheme should use threshold at least three or more to prevent information leakage. However, the characteristics of other threshold schemes and compared with other threshold scheme were not discussed.

3 PRELIMINARIES

3.1 digital signature

Digital signature is a cryptographic protection technology that uses cryptography technology to confirm the source of data and data integrity. It uses public key cryptography algorithm, that's digital signatures employ asymmetric cryptography. The signer first encrypts the message with the receiver's public key, and then encrypts the message again with his private key. The encrypted ciphertext is called digital signature. After it is sent to the receiver, the receiver uses the signer's public key to decrypt it. In this algorithm, only the signer has his own private key, so the receiver can believe that the message is from the signer.

Digital signature ensures that the data received by the receiver are correct. The receiver can verify the signature of the sender, others can not forge the signature of the message, and the sender can no longer offset the signature of the message after the data is sent, so that the digital signature can ensure the security of the data in the distributed system.

the signature process consists of three steps [26]:

- $G(p)\ \underline{generate\quad key->}\ (sk, pk)$. sk is the private key, and pk is public key.

- $Sig(sk, m)$ $\underline{generate \quad signature->}$ (sig). m is a plaintext message, sig is the generated signature.
- $Ver(pk, m, sig)\underline{verify \quad signature->}(True, Flase)$. Verifies whether the data is modified according to the public key pk and plaintext m. If the result is $True$, the verification is successful; else if it is $False$, the verification is failed.

At present, the commonly used signature algorithms are elliptic curve digital signature and threshold signature. The elliptic curve digital signature algorithm is mainly based on the elliptic curve discrete logarithm problem, if there is a way to find a private key, the security of system is affected. Threshold signature was proposed by Y.Desmedt in 1987 [27]. The threshold signature mechanism allows any t of n signers to generate signatures for messages, but less than t signers can not generate valid signatures. A threshold signature mechanism can build a robust signature system and prevent some signers from illegal behavior.

Threshold signature is a combination of threshold secret sharing technology and digital signature. Threshold secret sharing technology, that is divide the secret into n sub secret, sending to different participants, any sub secret will not disclose any information about the original secret, when recovering the secret. As long as the number of legitimate participants are no less than the threshold, then use their secret shares reconstruct the secret. Otherwise it can not be reconstructed. There are two classic secret sharing algorithms, one is Shamir's, using polynomial evaluation to create a secret share, and then use polynomial interpolation to recover the secret. The other is Asmuth and Bloom's algorithm, that a (t,n) threshold secret sharing based on the CRT.

3.2 Shamir secret sharing algorithm

Shamir's (t, n) secret sharing algorithm divides secret s into n sub secrets. Any t sub secrets can recover s, while any $t-1$ sub secrets can not recover s. In this scheme, $t, n \in N, t \leqslant N$, n participants compose a set $Q = \{Q_1, Q_2, \ldots, Q_n\}$, and D is dealer of the secret shares, If these n participants share the secret s, D uses the allocation algorithm to divide the s into the n sub share $\{s_1, s_2, \ldots, s_n\}$ and send the sub shares s_i secretly to each participant Q_i $(1 < i < n)$, Q_i and secretly save the share.

Distribution of secret share: set F_q as q-ary finite field, q is a prime and $q > n$. The secret is $s(s \in F_q)$, the process of sharing distribution discribes as below:

- D randomly selects the $t-1$ elements $\{A_1, A_2, \ldots, A_{t-1}\}$ in the F_q, then constructs the $t-1$ polynomial $f(x) = s + \sum_{i=1}^{t-1} A_i x^i \bmod q$, and $f(0) = s$.
- for $1 \leqslant i \leqslant n$, D calculates the value $y_i = f(x_i)$ corresponding to each participant Q_i.
- for $1 \leqslant i \leqslant n$, D sends the (x_i, y_i) secretly to the participant Q_i.

Secret recover: Any $k(k >= t)$ participants selected from the $Q = \{Q_1, Q_2, \ldots, Q_n\}$, the participants hold the secret shares $\{(x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)\}$, use this set to construct equations

$$\begin{pmatrix} 1 & x_1 & x_1^{t-1} \\ 1 & x_2 & x_2^{t-1} \\ \vdots & \vdots & \vdots \\ 1 & x_l & x_k^{t-1} \end{pmatrix} \begin{pmatrix} s \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{pmatrix}$$

solving the above equations with t variants, while $k >= t, s, a_1, a_2, ...a_{t-1}$ is its only solution then can recover the secret s.

3.3 Asmuth-Bloom algorithm

(1) Initialization. Suppose n participants compose a set $Q = \{Q_1, Q_2, \ldots, Q_n\}$, the threshold value is t, s is the secret, select a large prime p, and a set of $m = \{m_1, m_2, \ldots, m_n\}$, satisfy the following conditions

- $m_1 < m_2 < \cdots < m_n$, that $m_1, m_2, \ldots, m_n$ strictly monotonic increasing
- $\{(m_i, m_j) = 1 \mid i \neq j\}, m_i, m_j$ mutual prime
- $\{(m_i, p) = 1 \mid i = 1, 2, \cdots, n\}, m_i, p$ mutual prime
- $M = \prod_{i=1}^{t} m_i > p \prod_{i=1}^{t-1} m_{n-i+1}$

(2) Secret share. $M = \prod_{i=1}^{t} m_i$, obvious thatM/p is greater than the product of any other $t-1's$ m_i, randomly selects an integer B, and the number B satisfies the formula $B \in [0, [\frac{M}{p}] - 1]$, calculate $s' = s + Bp$, evidently know that $s' \in [0, M-1]$, generate secret shares, that is $s_i = s' \bmod m_i (i = 1, 2, \ldots, n)$.

(3) Secret recovery. After at least the t participants submit their secret shares. It is assumed that the secret shares submitted by the participants is $s_1, s_2, \ldots, s_t$, the congruence equations are constructed as follow:

$$y = \begin{cases} s' = s_1 \bmod m_1 \\ s' = s_2 \bmod m_2 \\ \quad \vdots \\ s' = s_t \bmod m_t \end{cases}$$

Solving the above equations, in $[m_1, m_2, \ldots, m_n]$ scope, they have a unique solution. The solution is $s' = \sum_{i=1}^{t} M \times r_i \times s_i \bmod M$, among them $r_i = M_i^{-1}$ is $M_i \bmod m_i$ modular inversion, that is $r_i M_i \equiv 1 \bmod m_i, \forall i \in (1, 2, \ldots, n)$, and can get the secrets $= s' - Bp$.

4 Blockchain-Based on Medical Cyber Physical Systems

4.1 system model

A medical cyber physical system based on blockchain is proposed to solve the data security storage, privacy-preserving, and data sharing. We construct a mixed blockchain system combining private and consortium blockchain. Each hospital has a local server and clients in the system, and each hospital constructs its own private blcokchain. The consortium blcokchain is composed of private blockchain. The system includes three main roles: patient, medical staff, and other users.

A patient should first register in the system to generate a public key ID and a private key password when going to the hospital. Medical staff also require registering corresponding public-private key pair in the system. After the doctor gives medical opinions to the patient, and conducts relevant examinations, the patient's ciphertext is stored on the local server, the hash value and key index of the ciphertext are stored on the hospital private blockchain. Private blockchain has higher storage speed, better privacy, better security, and low cost of storage. While the security index composed of private blockchain block identification, patient identity,

and keyword index is stored on the consortium blockchain[28]. The medical data in the mixed medical blockchain is authorized by the medical supervision organization and public to the all participating nodes. A Byzantine fault-tolerant mechanism[29] is used to attach new blocks to the consortium blockchain. The system model diagram is shown in Fig. 1.

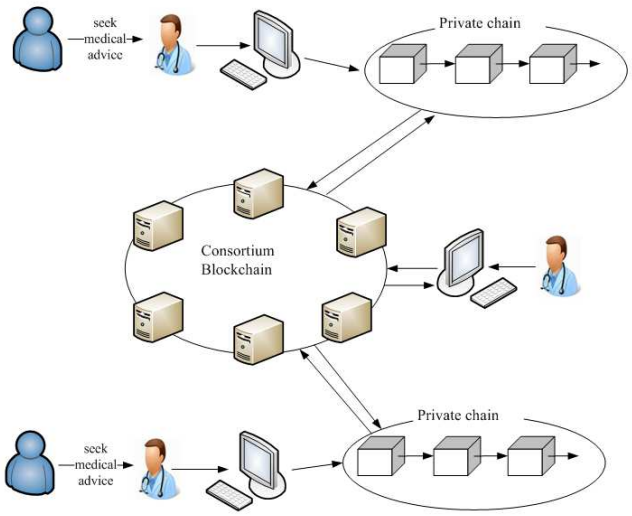

Fig. 1. The architecture of mixed medical blockchain.

The relationship among patient's medical records, blockchain and cluster storage is shown in Fig. 2. The hash tree composed of a large number of electronic medical records is stored on the blockchain. The content of electronic medical records is stored on the cloud storage platform composed of multiple computing centers, that is all the electronic medical records are stored by cluster storage. Through the unified access interface users can transparently access and utilize the patient's medical records in all storage devices. Medical cyber physical data comes from clinical

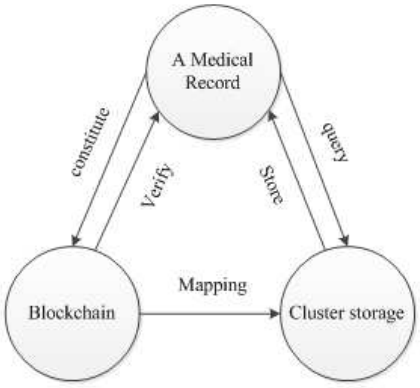

Fig. 2. The relationship diagram of MCPS

data, sensor data, medical images, doctor written instructions and prescription. The component of medical cyber physical data is shown in Fig. 3. In the system, the medical cyber physical data contains the specific information of each medical data, including patient ID, hash of patient health data, patient signature, doctor ID, doctor signature.

Patient ID	Health Data Hash	Patient Signature	Doctor ID	Doctor Signature

Fig. 3. Component of medical cyber physical data

Patients can obtain the private key after registration and identity authentication in the hospital's computing center, Randomly generate 256 bits data. The private key represents the patient's ownership of the data. If the private key is lost, the data access will be lost.

The public key is the patient's ID. The public key and the private key are generated in pairs, and the public key can generate the corresponding unique address, which can confirm the location of the patient's health data. The address is calculated by the public key. The public key is used as the input, and use hash function to generate the address.

Patient signature: the patient uses the private key to encrypt the medical data digest and the public key of user and doctor. One is to prove that the message is actually sent with the patient signature, and the other is to confirm the integrity of the message.

Doctor signature: doctors use private key to encrypt medical data digest, in order to confirm the authenticity of medical data.

4.2 The working procedure of the mixed medical blockchain

In this system, the medical source data is stored on the cloud storage platform of the data center. Still, there are great hidden dangers when the patient's electronic medical records are directly stored on the cloud storage platform or database. Therefore, the ciphertext of the patient's medical source data records are stored on the hospital cloud server. After the medical source data is hashed, a hash tree is generated and stored in the private chain of the hospital. The hospital server extracts the private chain block ID, patient identity and keyword index on the private chain to build a new transaction on the consortium chain, and other nodes in the consortium chain are responsible for verifying the transaction. If the verification passes, a new block on the consortium chain will be generated. Patients and doctors transparently access the consortium chain through the unified access interface to query medical data records, Then find the medical data stored on the cloud storage platform and decrypt it to get the actual source data.

The data structure in the private blockchain is shown in Table I. It consists of block header and block body. The block header includes: timestamps,block ID, block size and hash of the previous block. The timestamps show the generation time of the block. The block body is the tansction including the medical cyber physical data. The component of it has discussed above. Including patient ID, hash of patient health data, patient signature, doctor ID, doctor signature. The doctor's signature is helpful to track doctors.

Table I. Data structure of private blockchain

Block Head				Block Body
Time stamps	Private chain ID	Block Size	Previous Block Hash	transactions: medical cyber physical data

The generation of medical data blocks in the system are as follows:

Step 1. The patient registers and obtains the account number and public-private key pairs on the hospital server and shows the account number when seeing a doctor. The doctor establishes electronic medical records and keywords for the patient. The patient encrypts the data with his public key to get the ciphertext.

Step 2. The doctor uploads the hash value of the electronic medical record ciphertext and the keyword index composed of keyword ciphertext and evidence to the private blockchain to generate a new transaction.

Step 3. Hospital server, as a node of the consortium blockchain, building new blocks for the consortium blockchain. After the new block is created, the other nodes in the consortium are responsible for verifying the effectiveness of the new block.

The data structure in the consortium blockchain is shown in Table II. The nodes on the consortium chain extract the information index on the block to obtain the private chain block ID. Through the private chain block ID, the nodes on the consortium chain can get the hash value of the medical record ciphertext.

Table II. Data sturcture of consortium blockchain

Block Head				Block Body		
Time Stamps	Consortium chain ID	Block Size	Previous Block Hash	Hospital Server ID	Private chain index	Hospital Server Signature

The operations between the patient and the medical consortium chain mainly include request authentication and data decryption.

If the patient goes to another hospital for treatment, when the doctor needs to know the patient's past medical history, the patient generates a search trap and uploads it to the consortium chain. The nodes on the consortium chain search and obtain the hash value of the medical record ciphertext and feed it back to the hospital server. The hospital server compares the hash value of the electronic medical record ciphertext. If it is the same, the medical record ciphertext will be sent to the nodes on the consortium blockchain. The node on the consortium chain returns the medical record ciphertext to the patient, and the patient can decrypt the ciphertext.

The operation between doctor and medical consortium blockchain mainly includes request authentication and data download.

After passing the security authentication, the doctor download data from the medical consortium chain. After the security authentication between the doctor and the patient, they obtain access to the data logic. The complete patient medical record data = data (downloaded from the medical consortium blockchain) + data logic (obtained from the patient).

5 THRESHOLD SIGNATURE SCHEME IN BLOCKCHAIN BASED ON MCPS

5.1 Application scenario description of threshold signature

In the previous section, the blockchain system based on private blockchain and consortium blockchain, storing data in the blockchain system, and applying blockchain technology to the medical data problem, can effectively protect patient privacy.

In some cases, it is difficult to get the final treatment plan in one department because of the complexity of patients' actual disease. In order to effectively save the cost and time of refer to a different hospitals, The mode of multidisciplinary consultation can be adopted. Only when the number of doctors' signatures on the treatment plan meets the threshold value can the hospital make the final treatment plan for patients. The threshold signature scheme is applied to the medical cyber physical system based on mixed medical blockchain, ensuring the system's security and tamper resistance [30].

This section designs a system model for the threshold group signature scheme of medical consortium blockchain, suppose the hospital develops a patient treatment plan requires n doctors to form a treatment group, the receiving doctor is a group member, the final treatment plan for the patient is produced when the t threshold characteristics is met. In this case, the doctor create the block with his own signature in private blockchain, and the consortium blockchain store the hospital synthetic signature of the medical record.

A patient P goes to the hospital to receive the outpatient treatment of doctor D. For the actual disease of patient P, doctor D can start the multidisciplinary consultation mode when it is difficult for one person to get the final treatment plan. Only when the number of doctors' signatures on the treatment plan meets the threshold value can the hospital make the final treatment plan for the patient. Doctor D uses threshold signature to guarantee multidisciplinary consultation, showing the basic workflow of the blockchain. The private key and public key of the patient are stored in the patient's electronic device. The application scenario process of threshold signature is described as below:

Step 1. When first using the system, the patient should first register in the system and the system will give the public key PUB_KEY_P, private key PRV_KEY_P. also the doctor get his public key PUB_KEY_D and private key PRV_KEY_D.

Step 2. Patient P has a complicated disease and finds doctor D through the registration system.

Step 3. Patient P arrives at doctor D's consulting room, and patient P receives the public key PUB_KEY_P to generate a query transaction list and uses its own private key PRV_KEY_P for digital signature SIG_P. Obtain the transaction list with its own information from the system. The system uses the public key PUB_KEY_P and digital signature SIG_P to verify P's identity in the key and authentication architecture. It returns the transaction sheet containing the patient's information after pass verification. The query transaction will be saved in each verification node's local database, waiting for the packer to pack into the new block. After the patient decrypts with the private key, the decrypted information(excluding the patient's private key) is sent to the doctor client and displayed on the doctor's computer.

Step 4.First, Doctor D signs the treatment plan(corresponding share signature), packages the public key PUB_KEY_D in the form of private blockchain data structure and upload it to the private blcokchain of the hospital for group's other $n-1$ doctor verification. Then, other doctors in the group download the transaction from the private chain through the server for correctness verification (share verification), and if it is correct, the verification transaction will be broadcast, that is, other doctors sign on the treatment scheme and broadcast it to the private chain of the hospital in the form of transaction. Then, doctor D collects the transaction on the chain for verification, and if the number of effective transactions verified meets or exceeds number t, A signature SIG_H is generated. After the treatment plan, and package the transaction data (composite signature) into the block and broadcast to the whole network on behalf of the hospital's

final treatment plan.

Step 5. If the lower limit of threshold signature is not reached, the signature can not be generated. At this time, doctor D can transfer the patient to another hospital.

5.2 Architecture of blockchain threshold signature system

Through the previous discussion, compared with the scheme based on Lagrange interpolation, the scheme based on CRT had less computation [31]. A threshold signature scheme suitable for a medical consortium based on CRT is used to realize the threshold signature in multidisciplinary consultation [30]. The framework of the system is shown in Fig. 4:

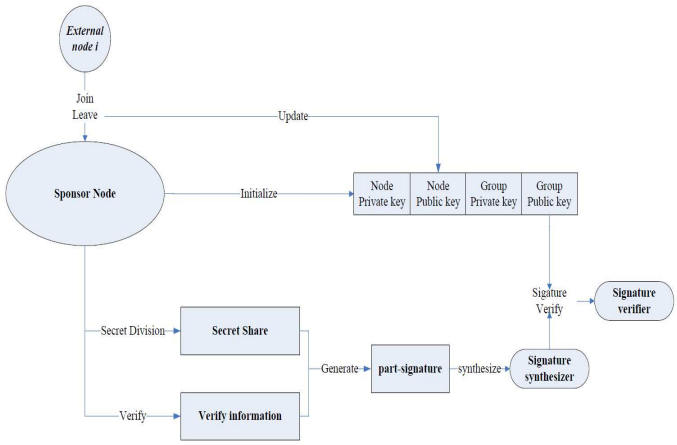

Fig. 4. Architecture of blockchain threshold signature system

Its working process consists of the following steps:

Step 1. The sponsor node invites external nodes to join the process to form a group. In this system, each node can act as a signature synthesizer and a signature verifier.

Step 2. Threshold signature initialization. Generates the parameters needed by the signature algorithm, generates its own private key and public key for each node, and broadcasts public key to other nodes in the group.

Step 3. The system divides the secret of the node, and broadcasts the secret share to other nodes to provide other nodes to generate part-signature.

Step 4. Each node in the system solves the secret information according to the CRT for the received secret share, generates a part-signature, and broadcasts it to the signature synthesizer.

Step 5. The signature synthesizer synthesizes the received part-signatures and only needs no less than t part-signatures to synthesize the final signature and sends the signature to the signature verifier.

Step 6. The signature verifier verifies the synthesized signature information and then feeds back the signature result to the sponsor.

5.2.1 detailed design of blockchain threshold signature system

The following describes the detailed design process of threshold signature for the consortium blcokchain. The symbols used in the detailed design are listed, and their contents are shown in Table III

Step 1. Initialization of the sponsor node

The sponsoring node invites the external nodes to form a set $Q = \{Q_1, Q_2, \ldots, Q_n\}$, contains n nodes participating in the joint consultation signature in the medical blockchain, and t is the threshold value. Two big prime numbers p and q are selected. A set of positive integer sequences $d = \{d_1, d_2, \ldots, d_n\}$, and generating element g on a prime field $GF(p)$ are also selected. q and d satisfy the Asmulth-Bloom scheme, and the message to be signed is m, let $D = \prod_{i=1}^{t} d_i$, public information$\{n, t, g, p, q, d, D\}$ to all the other nodes.

Table III. Symbols used in threshold signature

Symbol	Description	Symbol	Description
Q	Member set	E_i	Private key of node i
r_i	Sub secret of node i	K_i	Public key of node i
B_i	Arbitrary integer of node i	G	Group private key
Y_{ij}	Secret share shadow	C	Group public key
m	Message to be signed	g	Generator of GF(p)
p	Large prime	S_i	Part-signature of node i
q	Prime of group public key	S	Complete signature

Setp 2. Generate secret share

The blockchain nodes cooperate with each other. Blockchain node Q_i randomly selects the sub secret r_i and the integer B_i. The sub secret r_i and the integer B_i are selected secretly by the current blockchain node, and they do not need to be broadcast them to other nodes. As long as the node does not actively disclose these two parameters, others can not obtain them.

The selection of r_i and B_i meet the following conditions:

$$0 < r_i < [q/n] \tag{1}$$

$$0 < B_i < [D/q - 1]/n \tag{2}$$

Node Q_i calculates the secret share Y_{ij}
let $x_i = r_i + B_i q$

$$Y_{ij} = x_i \bmod d_j \tag{3}$$

Q_i preserves the value of Y_{ij} and public g^{r_i} ,g^{B_i} , and broadcast $Y_{ij}(i \neq j)$ to node Q_j .

Step 3. Verify node information

The blockchain node Q_i calculates the verification information u_i ,w_{ij} and v_{ij}, and verifies the correctness of the information .

$$u_i = g^{x_i} \bmod p \tag{4}$$

$$w_{ij} = (x_i - Y_{ij})/d_j \tag{5}$$

$$v_{ij} = g^{w_{ij}} \bmod p \tag{6}$$

And broadcast u_i and v_{ij} in the blockchain network. In addition, after receiving the information u_i and Y_{ij}, the node Q_j verifies the correctness of the secret share through the following formula:

$$g^{r_i} \cdot g^{B_i q} \bmod p = u \tag{7}$$

$$((g^{r_i} \bmod p)((v_{ij})^{d_j} \bmod p)) \bmod p = u \tag{8}$$

If the u_i satisfies the above equations(7) and (8), then the secret share shadow Y_{ij} send by the member Q_i is true, and the message is trusted; otherwise, the blockchain node Q_j will ask the node Q_i to re-transmit the message again.

Step 4. Generate blockchain node key and group key.

According to the verification above, if the verification result is correct, the node Q_j calculates its own private key.

$$E_j = \sum_{i=1}^{n} Y_{ij} \bmod d_j \tag{9}$$

So the node pubic key is $K_j = g^{E_j}$.

According to the number of secrets selected by each blockchain node can generate the group privte key and group public key. The group private key is $G = \sum_{i=1}^{n} r_i$, and the group public key is:

$$C = \prod_{i=1}^{n} g^{r_i} \bmod p = g^{\sum_{i=1}^{n} r^i} \bmod p \tag{10}$$

Step 5. Generate signature

In this threshold scheme, any t blockchain nodes use their private key to generate their own part-signature, and t part-signature can compose the signature of message m.

First, generate part-signature. the node Q_i chooses a integer $\varphi_i \in GF(p)$,and calculate δ_i.

$$\delta_i = g^{\varphi_i} \bmod p \tag{11}$$

Q_i received δ_i and calculated

$$\delta = g^{\sum_{i=1}^{t} \varphi_i} \bmod p = \prod_{i=1}^{t} g^{\varphi_i} \bmod p = \prod_{i=1}^{t} \delta_i \bmod p \tag{12}$$

the δ is a coefficient of the formula to compose a part-signature.

Then Q_i continues to calculate the other coefficient L_i

$$L_i = \frac{D}{d_i} \times h_i \times E_i \bmod D \tag{13}$$

in the formula (13) $h_i \equiv (\frac{D}{d_i})^{-1} \bmod d_i$,$(i = 1, 2, \ldots, n)$. Node Q_i calculated the part-signature S_i by equation (14)

$$S_i = E_i \cdot m + \delta \cdot L_i \tag{14}$$

After receiving the part-signature$\{m, \delta, S_i\}$ send by t blockchain nodes, the signature synthesizer synthesizes the signature Z. It should be noted that every node can assume the role of signature synthesizer in the blockchain scenario, The calculation formula of the completed signature is as follows:

$$S = \sum_{i=1}^{t} (S_i \bmod D) \bmod q \tag{15}$$

Then the completed signature of message m is $\{m, \delta, S\}$.

Step 6. Verify the signature

After receiving the signature information m is $\{m, \delta, S\}$, the verifier uses the group public key C to verify the validity of the signature according to the following equation (16):

$$g^S = \delta^{m \times \delta} \times C \bmod p \tag{16}$$

If the equation(16) is true, the signature is valid and accepted.

6 ANALYSIS OF THE SCHEME

6.1 security anaylsis of the mixed blockchain

(1) All information on the medical consortium chain is public and can not be tampered and arranged according to a certain sequence. The distributed consensus mechanism of medical consortium blockchain makes trust based on cryptographic algorithm without relying on trusted third party. Once the data is written into the private chain and consortium chain, it cannot be tampered, because each block saves the hash of its previous block, it is almost impossible to modify the data of a block, which requires at least 51 percent of the computing power of the whole network. The hash of the original data of medical records is saved in the medical consortium chain. Any changes to the original data will cause the change of its hash value, so it directly ensures the privacy-preserving of medical records.

(2) Data can not be forged. Blockchain itself has tamper proof characteristics, combined with identity authentication technology and cryptography related technologies. The medical data records stored on the private chain use the patient's private key to encrypt the ciphertext of the medical records. The consortium chain's data contains hash of private chain. Unless the attacker steals the user key, he can not obtain the complete perceptual data and forge these data.

(3) After receiving the data from consortium chain, the patient decrypts the ciphertext with his own private key, obtains the hash and signature of the original record, verifies the integrity and authenticity of the record. Only authorized users can obtain the decryption key, check the real records. Even if the enemy obtains the records from the storage, he can not obtain any real information of the medical records due to the stored ciphertext, so as to ensure the security of the medical record data.

To evaluate the proposed architecture of mixed medical blockchain, we compared it with the existing system based on blockchain technology. At present, the main medical blockchain systems are MDSM [13], MedRec [14] and MedicalChain[15], and the comparison results with the existing solutions are as follows.

Table IV. The comparison of different systems

system	Consensus	computing power	Access Control	Privacy preservation
Alg.in[13]	PoS	Small	No	YES
Alg.in[14]	PoW	Big	YES	YES
Alg.in[15]	PoI	Big	YES	YES
Proposed	PBFT	Small	No	YES

From Table IV, compared with PoW algorithm and PoI algorithm, PBFT consensus algorithm has less computing power, and does not need to pay, requires less running nodes, and does not need "mining" operation. Moreover, this scheme combines private blockchain and consortium blockchain, effectively controls the rapid growth of data in the consortium blockchain, which is consistent with the needs and characteristics of the medical system.

6.2 security analysis of the threshold scheme

(1) In this scheme the secret shares are generated by all participants. No single node can know the group private key, which effectively avoids the authority deception of the trusted center.

(2) The scheme can distinguish the fraud between member nodes, and each member must public the real u_i and v_{ij}. If Q_i provides the fault secret share shadow Y_{ij}, it can be detected by $u_i v_{ij}$ through verification equations (3) to(8).

(3) In the verification process, each member's sub secret r_i is secure. Although the member Q_i public g^{r_i}, but through $g^{r_i} \bmod p$ to solve r_i is still a discrete logarithm problem , so the member sub secret r_i will not be disclosed. In the process of verifying Y_{ij} ,each member Q_i is required to public the verification information through the equation equations (4) to(6). Through u_i to slove x_i is a discrete logarithm,so u_i is safe, on other hand, if attackers want to through v_{ij} to get x_i, they must know w_{ij}, and get v_{ij} from w_{ij} is still a discrete logarithm problem. So x_i is safe ,and r_i is safe too.

(4) The group private key G is secure and reusable. Through the group public key C to calculate group private key G belongs to the problem of discrete logarithm. Therefore, unless all members cooperate, no one can obtain the group private key G. In the part-signature generation process, each member calculates the part-signature. Use the formula (14), do not directly use or expose any information of the group private key G. The group private key G can still be reused after one signature.

(5) If a malicious node Q_i' wants to replace the blockchain node Q_i to generate secret shares, the malicious node Q_i' randomly selects the secret numbers r_i' and B_i'. Because $r_i' \neq r_i$,$B_i' \neq B_i$, then $r_i' + B_i' q \neq r_i + B_i q$, so $Y_{ij}' \neq Y_{ij}$, and other nodes receive the broadcast information $g^{r_i'}$,$g^{B_i'}$ from malicious node Q_i'. Through verification, it is easy to verify $g^{r_i'} \cdot g^{B_i' q} \neq g^{r_i} \cdot g^{B_i q}$. Therefore, node Q_i' can not replace any other blockchain nodes to forge r_i and B_i.

(6) If a malicious node Q_i' wants to replace the blockchain node Q_i to generate the private key of node, the malicious node may intercept the Y_{ij} send by the other $n-1$ nodes to construct the private key of the blockchain node. However, the other nodes keep their own Y_{ii} which can not be obtained by the attacker. From $Y_{ii} = (r_i + B_i q) \bmod d_i$,the attacker may attempt to obtain r_i and B_i by intercepting g^{r_i} and g^{B_i} , so as to calculate Y_{ii}. However, solving r_i and B_i through g^{r_i} and g^{B_i} is a discrete logarithm problem, and the attacker can not obtain them through calculation, so the attacker cannot forge the private key of the blockchain node.

(7) If a malicious node wants to forge the completed signature, the attacker randomly selects φ_i', calculates δ_i', δ' and part-signature S_i', and synthesized the signature S'. In the signature verification process, because $S' \neq S$,so $g^{S'} \neq \delta^{m\delta} \cdot C \bmod p$,the attacker can not pass the verification and the signature is invalid, so the attacker cannot forge the signature.

6.3 Performance Efficiency analysis

The proposed threshold signature scheme based on CRT, that has less computationally difficult than the interpolation algorithm based on Lagrange. The signature algorithm proposed in this paper is compared with the literature based on Lagrange interpolation[32, 33].

In the following, we compare the proposed scheme in terms of computation to show the advantages of this scheme in this respect. Since the key generation process of threshold signature is not frequent, the amount of computation required by the process has little impact on the practicability of the scheme. Therefore, we mainly compare the schemes in the signature generation and verification stage.the symbols are defined in Table V.

Table V. Modulus symbols description

Symbol	Description
M_m	Modular Multiplication
M_e	Modular exponentiation
M_d	Modular Addition

Compared with modular exponential operation and modular multiplication the computation modular addition can be ignored, so it will not be discussed below. Table VI is computational complexity contrast based on the existing scheme based on Lagrange interpolation and proposed scheme. It can be seen from Table VI

Table VI. Computational complexity of schemes

Scheme	Signature generation	Signature verification
Alg.in[32]	(8t+1)M_m+(2t+2)M_e	$2M_m$
Alg.in[33]	4tM_m+2tM_e	M_m +M_e
Proposed	(2t)M_m+tM_e	M_m

that for signature generation and signature verification, our scheme is better than[32, 33]. As a decentralized distributed network, the algorithm is required to be more efficient due to the limited computing resources.

7 Conclusions and Future Works

In this paper, we apply blockchain technology to the medical system, and propose the combination of private chain and consortium chain as data storage platform for safety storeage and accessing. In the system, the medical record itself is saved in the cloud server of each hospital. The doctor packages the patient's medical data ciphertext and uploads it to the private chain of the hospital. The hospital server packages the data block from the private blockchain to the consortium blockchain, waits for other nodes in the consortium to confirm, and connects the block to the consortium chain. In this way, patients can obtain their own data at any node in the consortium and authorize it to other data users. The medical data of patients themselves are not stored in the consortium chain. It reduces data storage redundancy. At the same time, aiming at the situation that medical accidents are easy to occur in multidisciplinary joint consultation in the medical process, a threshold group signature suitable for medical consortium is proposed. The whole process of threshold signature group formation, secret share creation, node verification, node key and group node key creation, threshold signature creation and verification are given. The security and execution efficiency of the system are analyzed. The mixed medical blockchain proposed in this scheme can realize secure storage, and the threshold signature can also improve the security and privacy in the medical system. At the same time, it also ensures the rights and security of patients and doctors.

In the research work of this paper, the secure transmission of data based on private blockchain and consortium blockchain is not described in this paper, and the distribution and creation of threshold signature can not start when there is no doctor specified in threshold signature, which is also encountered in some emergency medical scenarios, These are the key contents to be studied in the next step of system design.

ACKNOWLEDGMENTS

Funding: This research was funded by National Natural Science Foundation of China under Grant No. 61972438 ; Key Research and Development Projects in Anhui Province under Grant No. 202004a05020002; Outstanding youth talent support project in Anhui Province under Grant No.gxyq2019200;Quality engineering project in Anhui Province under Grant No.2020xsxxkc481

REFERENCES

[1] I. Lee, O. Sokolsky. Medical Cyber Physical Systems. In Proceedings of IEEE International Conference and Workshops on Engineering of Computer Based Systems, 2010, pp.743-748.

[2] R. Wang, S. Yu, Y. Li, et al. Medical Blockchain of Privacy Data Sharing Model Based on Ring Signature, Journal of UEST of China, 2019, vol.48, no.06, pp.886-892.

[3] H. Shu, P. Qi, Y. Huang, et al. An Efficient Certificateless Aggregate Signature Scheme for Blockchain-Based Medical Cyber Physical Systems. Sensors, 2020, vol.20, no.05, pp.1521-1545.

[4] A. Liu, X. Du, N. Wang, et al. Research Progress of Blockchain Technology and its Application in Information Security. Journal of Software, 2018, vol.29, no.07, pp.2092-2115.

[5] R. Sangeetha, B. Harshini,A. Shanmugapriya, et al. Electronic Health Record System using Blockchain. International Journal of Multidisciplinary technovation, 2019, vol.01, no.02, 2019, pp.57-61.

[6] A. Dubovitskaya, Z. Xu, S. Ryu, et al. Secure and Trustable Electronic Medical Records Sharing using Blockchain. Amia Annual Symposium Proceedings, 2017, pp.650-659.

[7] X. Cheng, F. Chen, D. Xie, et al. Design of a Secure Medical Data Sharing Scheme Based on Blockchain. Journal of Mdeical Systems, 2020,vol.44, no.02, pp.52-60.

[8] C. Chen. Toward Security and Confidentiality in Personal Health Records via Blockchain Technology. Basic and Clinical Pharmacology and Toxicology, 2020, vol.126, no.05, pp.10-28.

[9] B. Tu, Y. Chen. A Survey of Threshold Cryptosystems. Journal of Cryptologic Research, 2020, vol.07, no.01, pp.1C14.

[10] X. Fan. Winners, Losers and Watchers of Financial Technology. Financial View, 2017, no.021, pp.42-43.

[11] B. Vivekanadam. Analysis of Recent Trend and Applications in Block Chain Technology. Journal of ISMAC, 2020, vol.02, no.04, pp.200-206.

[12] D. Guegan. Public Blockchain versus Private blockhain. Universit Paris1 Panthon-Sorbonne, 2017.

[13] A. Zhang, X. Lin. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain.Journal of Medical systems, 2018, vol.42, no.08, pp.122- 140.

[14] A. Azaria, A. Ekblaw, T. Vieira, et al. Medrec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of 2nd International Conference on Open and Big Data (OBD), 2016, pp.25-30.

[15] C. Zhang, Q. Li, Z. Chen. Medical Chain: Alliance Medical Blockchain System. Acta Automatica Sinica, 2019, vol.45, no.08, pp.1495-1510.

[16] Y.Gao, J. Wu. Efficient Multi-party Fair Contract Signing Protocol based on Blockchains. Journal of Cryptologic Research, 2018, vol.5, no.5, pp.556C567.

[17] N. Aitzhan, D. Svetinovic. Security and Privacy in Decentralized Energy Trading through Multi-signatures. Blockchain and Anonymous Messaging Streams, IEEE Transactions on Dependable and Secure Computing, 2016, vol.15, no.05, pp.840C852.

[18] Y. Liu, R. Li, X. Liu. Enhancing Anonymity of Bitcoin Based on Ring Signature Algorithm. In Proceedings of the 13th International Conference on Computational Intelligence and Security (CIS 2017), 2017, pp.317C321.

[19] Y. Liang, X. Zhang, Z. Zheng. Electronic Cash System based on Certificateless Group Signature. Journal of Communications, 2016, vol.37, no.5, pp.184-190.

[20] B. Wang, J. LI. A(t,n) Threshold Signature Ccheme Without a Trusted Party. Chinese Journal of Computers, 2003, vol.26, no.11, pp.1581-1584.

[21] A. Shamir. How to Share a Secret. Communication of the ACM, 1979, vol.22, no.11, pp.612-613

[22] C. Asmuth, J. Bloom. A Modular Approach to Key Safeguarding. IEEE Transactions on Information Theory, 1983, vol.29, no.2, pp.208-210.

[23] Y. Cheng, H. Liu. The Asmuth-Bloom Verifiable Threshold Sharing Scheme. Natural Science Journal of Harbin Normal University, 2011, vol.27, no.3, pp.35-38.

[24] T. Wang, S. Hou. Research on Threshold Signature Scheme and its Security Analysis. Computer Engineering and Applications, 2018, vol.54, no.13, pp.123-130.

[25] M. Al-Zubaidie, Z. Zhang, J. Zhang. PAX: Using Pseudonymization and Anonymization to Protect Patients' Identities and Data in the Healthcare System. International Journal of Environmental Research and Public Health, 2019, vol.16, no.09, pp.1490-1499.

[26] L. Wang, M. Hu, Z. Jia. A Signature Scheme Applying on Blockchain Voting Scene Based on the Asmuth-Bloom Algorithm. IEEE 4th International Conference on Computer and Communications, 2018, pp.2372-2378.

[27] Y. Desmedt. Society and Group Oriented Cryptography: a New Concept.CRYPTO 1987, Lecture Notes in Computer Science. 1987, vol.293, pp.120-127.

[28] H. Han, M. Huang, Y. Zhang. An Architecture of Secure Health Information Storage System Based on Blockchain Technology. In Cloud Computing and Security.ICCCS 2018, Lecture Notes in Computer Science, 2018, vol.11064, pp 578-588.

[29] T. Ding, S. Chen. Improved PBFT Consensus Mechanism Based on Credit-Layered Mechanism. Computer Systems and Applications, 2020, vol.29, no.05, pp.255-259.

[30] J. Chen. Research on Threshold Group Signature Scheme in Blockchain Mode. Northwestern Normal University, 2020.

[31] Y. Cheng, Z. Jia, M. Hu. Threshold Signature Scheme Suitable for Blockchain Electronic Voting Scenes. Journal of Computer Applications, 2019, vol.39, no.9, pp.2629-2635.

[32] X. Fu. Proactive Threshold RSA Signature Scheme Based on Polynomial Secret Sharing. Journal of Electronics and Information Technology, 2016, vol.38, no.09, pp.2280-2286.

[33] Y. Zhu, B. Wang, C. Cai. A novel smart-card based authentication scheme using proactive secret sharingInternational Journal of Computer and Communication Engineering, 2016,vol.05, no.03, 196-205.