Hindawi
Security and Communication Networks
Volume 2022, Article ID 2719951, 14 pages
https://doi.org/10.1155/2022/2719951

Research Article

B-SSMD: A Fine-Grained Secure Sharing Scheme of Medical Data Based on Blockchain

Jialiang Yuan,[1,2] **Yan Ma**,[2] **Wei Luo**,[2] **and Gang Han**[2]

[1]*Faculty of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China*
[2]*School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China*

Correspondence should be addressed to Jialiang Yuan; 634660981@qq.com

Received 18 February 2022; Accepted 3 October 2022; Published 3 November 2022

Academic Editor: Helena Rifà-Pous

The application of blockchain technology in the medical information system is gradually triggering profound changes, which has heterogeneous, cross-domain, and open network characteristics. However, today's electronic medical systems fall short of ensuring the confidentiality and safe sharing of medical data, which poses serious threats to their authenticity and accuracy. Moreover, most of the current blockchain medical systems are under great transmission and storage pressure. Based on the aforementioned security and performance considerations, this paper proposes a fine-grained secure sharing scheme of medical data based on blockchain (B-SSMD). We design a three-chain model to store patient information, medical staff information, and medical records hierarchically. The integration of IPFS technology and the encryption algorithm ensures secure and efficient off-chain data storage. The user classification is realized by assigning attributes, and the attribute encryption technology is adopted for secondary encryption of the key and ciphertext path. Meanwhile, through hierarchical encryption, the risk of a system attack is greatly reduced. Our scheme not only solves the problems of low throughput and poor stability in the single chain model but also improves the data confidentiality and enables medical data to be managed more safely and efficiently in the sharing process. We provide the security and performance analysis and it is confirmed that our scheme has higher security and controllability.

1. Introduction

The development of artificial intelligence, big data, and blockchain technology has brought new opportunities and challenges to the medical data system [1]. With the continuous growth of electronic medical records, medical images, and other medical data, its security requirements are increasingly stringent. Compared with traditional big data, medical data has its own particularity. Medical records are not only highly sensitive personal information for clinical diagnosis and treatment but also affect the development of the whole medical industry. Electronic medical records (EMRs) sharing can help doctors obtain a previous medical history and examination data, which greatly reduces the treatment burden of patients and the waste of medical resources caused by repeated examinations. Therefore, medical record sharing is considered as a promising method to improve the quality of medical services. Meanwhile, the sharing model should have a privacy protection mechanism for medical data.

The traditional centralized medical system and semi-trusted cloud storage are difficult to achieve a balance between privacy protection and data sharing. The current information security issues in electronic medical systems are mainly to solve the secure collection, transmission, application, and sharing of information in a highly heterogeneous network environment [2]. As an emerging technology, blockchain is decentralized, traceable, and tamper-proof, ensuring data security and transparency that can be used for EMRs management in the medical field. In addition, blockchain can enable individuals to manage, access, and update their EMRs securely by authorizing specific entities, such as patients and medical departments [3]. However, problems such as data security and privacy protection still exist in the medical blockchain system. It is necessary to establish appropriate authentication, authorization, and

privacy protection encryption mechanisms to ensure that authorized entities can access the correct patient data at the right time.

Hence to ensure the secure sharing of the EMRs, in this paper, we propose a fine-grained secure sharing scheme of medical data based on blockchain (B-SSMD), which is privacy-preserving and data-decentralized. Blockchain can meet the demands in the medical data sharing process by hierarchical data storage, and it can guarantee the security and strict fine-grained data access. The data recorded on blockchain is tamper-resistant, synchronous, and light-loaded to achieve stability. In our proposal, the sensitive medical data is double encrypted and the ciphertext and its index path are stored and distributed to further improve the data confidentiality. In this way, patient privacy can be well protected from intruders, and data can be shared safely among different users. The main contributions are as follows:

(i) The three-chain fusion method enables the hierarchical storage of medical data, reducing the data security threats that exist in the previous simplex data storage method based on blockchain.

(ii) The InterPlanetary File System (IPFS) technology provides the underlying distributed data storage, with the role of secure and efficient off-chain data storage. The IPFS path is encrypted and stored on the consortium blockchain to reduce the on-chain storage burden.

(iii) The data sharing process P/MSISP provides more security and is more efficient for end users by integrating the three-chain model and IPFS for information storage, update, and sharing.

(iv) The Ciphertext-Policy Attribute-based Encryption (CP-ABE) is applied to encrypt the symmetric encryption key and the ciphertext path, in order to achieve more secure and flexible management of medical data, as well as fine-grained data access control.

The remainder of this paper is organized as follows: in Section 2, related work is presented. In Section 3, we briefly introduce some preliminaries. Section 4 shows the scheme framework and the implementation of B-SSMD in detail. Section 5 analyzes the security of B-SSMD. In Section 6, the performance analysis of the scheme is proposed. Finally, we conclude the paper in Section 7.

2. Related Work

Nowadays, medical information system plays an important role in patient health record management, patient data monitoring, etc. and has become an effective way to solve the shortage of medical resources. With the emergence of new technologies and new requirements, medical information systems have increasingly demanding requirements for data processing, sharing, and security protection capabilities. At present, studies have shown that cloud computing [4, 5] is a key technology to improve the medical system. Considering the privacy of user data, medical data stored in the cloud are encrypted, and there are a lot of data sharing scenarios in the cloud environment [6]. When medical data are stored in the cloud server, the key problem is how to prevent unauthorized users from illegally access and how to share data among authorized users efficiently [7, 8]. Li et al. [9] proposed a novel patient-centric framework and a suite of mechanisms for data access control to personal health records stored in semitrusted servers. The system divides the users into multiple security domains that reduces the key management complexity but requires the interaction among multiple attribute authorities and leaks attributes privacy in the access policy. Wang [10] presented a secure data sharing scheme built from bilinear pairings that provides the flexible utility of data while solving the privacy and security challenges for data sharing. Liang et al. [11] proposed a decentralized ABE scheme that can safely share cloud storage of personal health records (PHRs). In the two schemes above, the medical record files are encrypted with the public key using an encryption algorithm and stored in the cloud storage server. However, due to the higher requirements of cloud storage for data confidentiality, such schemes do not encrypt the key and ciphertext path, and thus the data confidentiality and security need to be further improved.

With the explosive growth of medical data, the use of outsourced clouds to store sensitive information is vulnerable to many security threats [12, 13]. In order to store and manage massive amounts of medical data more efficiently and securely, the emergence of blockchain technology has a huge impact on the medical information system. Blockchain has the characteristics of multiparty maintenance, nontampering, and decentralized storage [14–17], and it can complement the security issues in cloud storage. For instance, by introducing blockchain, the problem of potential single point failure of the center authority can be solved to some extent. Meanwhile, blockchain enables patients to be regarded as the main entities and centers of an entire healthcare ecosystem [18–20]. Therefore, blockchain technology has brought new opportunities for the development of medical information system and related work has been studied. Liu et al. [21] proposed a blockchain-based privacy protection data sharing scheme for electronic medical records. In this scheme, they use a single consortium blockchain to reserve indexes of EMRs and achieve data sharing. Lee et al. [22] designed a blockchain-based data storage solution for telecare medical information systems. The social network information transfer protocol stores data using blockchain technology so that a data owner can authorize access to data by relevant users. Madine et al. [23] proposed a blockchain medical system that allows patients to control medical records. They integrate blockchain-based system with the IPFS and trusted reputations-based oracles to fetch, store, and retrieve PHRs. However, in the above schemes, the traditional single chain model is used, and thus the storage capacity of the blockchain is limited and the data storage and access methods on the traditional blockchain are relatively simple. For the blockchain with a single chain structure, all accounts, contracts, transactions, and other

information are stored on one chain, which does not ensure privacy protection but also causes slow response due to a large amount of redundant data. The single-chain blockchain scheme has poor scalability, low throughput, and lacks a flexible and secure way to update, store, and share data. Therefore, a more effective blockchain network structure is needed to improve the security and efficiency of the system.

In terms of storing and sharing EMRs, uploading patient medical data to all nodes in the blockchain network will increase the risk of medical data leakage, and problems such as data privacy protection and cloud storage data security access exist. For hospitals, the large amount of data stored in the third-party cloud is not reassuring [24–27]. To better achieve privacy protection in medical big data sharing across medical information systems, some research studies have been implemented. Wang et al. [28] presented a model for data access control and sharing using blockchain and used attribute-based encryption to control and share enterprise data. In this scheme, users are divided into two categories, and an access control policy tree is established according to the attributes of visitors. Alniamy and Bradley [29] proposed an architecture model by combining Hyperledger blockchain technology and Attribute-based Encryption scheme in a decentralized environment. In their work, all data access requests are processed through the blockchain and all permissions are assigned by data owner of the document. Wang et al. [30] proposed a decentralized secure cloud storage access control framework by using the Ethereum blockchain technology. The data owner can append an effective access period for the data user and store an access period time of information on the Ethereum blockchain. In the above-given blockchain based access control scheme, the user groups in the medical system are not specifically divided, and only the two major user principals, patients, and doctors, are the research objects. Hence, the schemes lack fine-grained security protection mechanism and cannot fully meet the needs of high granularity and high security of medical information system.

Our paper takes aim at solving the above problems. In our scheme, we exploit three-chain blockchain structure to make the hierarchical stored medical data sharing process more secure and effective with a symmetric encryption key and IPFS path encrypted. The user group are fine-grained divided and their access strategies are designed in detail. The logics are implemented by chaincode, which is the smart contract in FISCO BCOS Caliper.

3. Preliminaries

In this section, we briefly review the relevant knowledge.

3.1. Blockchain. Recently, blockchain technology has attracted increasing attention. As an emerging technology, it has many application values in medical treatment because of the decentralized, transparent, and secure characteristics. Blockchain is essentially a distributed database technology. As shown in Figure 1, each node on the blockchain includes two parts, a block header and a block body. It utilizes technologies such as distributed timestamp protocol, longest chain algorithm, and related encryption algorithms (such as SHA-256) to achieve a distributed consensus mechanism and user anonymity.

Blockchains can be divided into public blockchains, private blockchains, and consortium blockchains. Anyone in the public blockchain can participate in the consensus process. The private blockchain is only open to individual person or entity. And, the consortium blockchain allows a number of authorized parties to participate in.

In response to data security and patient privacy issues in medical information system, we adopt the form of consortium blockchain to build a secure information sharing system. Compared with public blockchains, it can control user nodes inside and outside the network through a flexible access mechanism for better privacy protection. In addition, it also has the advantages of lower cost, higher performance, and strong scalability.

3.2. CP-ABE. Attribute-based encryption (ABE) belongs to asymmetric encryption technology essentially, which can realize one-to-many data encryption communication [31]. The encryption schemes are divided into key policy attribute-based encryption (KP-ABE) and ciphertext policy attribute-based encryption (CP-ABE). The access control policy in KP-ABE is associated with the key, while the access policy in CP-ABE applied in this paper is associated with the ciphertext. The decryption policy is embedded in the ciphertext during encryption, and the user's attributes are embedded in the private key when the key is generated. If and only if when the attribute set meets the attribute policy, the user can decrypt it. The CP-ABE scheme usually contains four algorithms as follows.

3.2.1. Initialization. The initialization process generates the public parameter P_k and the master key M_k by inputting the security parameter λ.

$$\text{Setup}(\lambda) \longrightarrow (P_k, M_k). \tag{1}$$

3.2.2. Private Key Generation. Takes the master key M_k and the attribute set S as input to output the user attribute private key S_k.

$$\text{KeyGen}(M_k, S) \longrightarrow S_k. \tag{2}$$

3.2.3. Encryption. Passes in the public parameter P_k, access structure T, and plaintext M. Then the algorithm encrypts the plaintext M and generates the ciphertext C.

$$\text{Encrypt}(P_k, T, M) \longrightarrow C. \tag{3}$$

3.2.4. Decryption. Inputs the public parameters P_k, the ciphertext C and the user private key S_k. If the attributes contained in the user attribute private key S_k meet the access

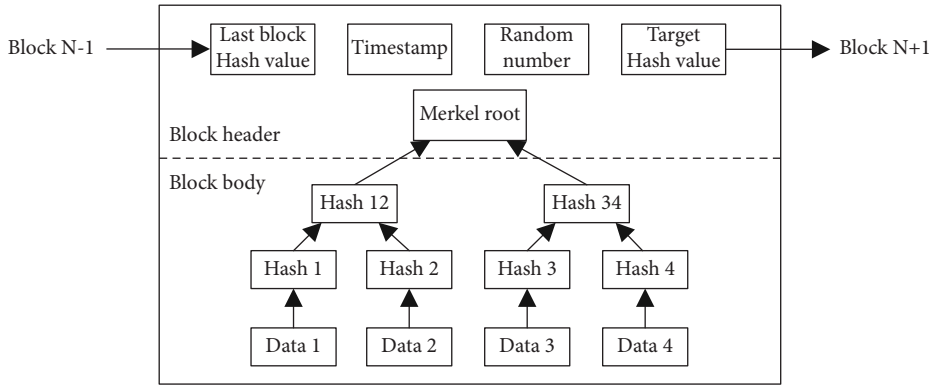

Figure 1: Blockchain structure.

structure T contained in the ciphertext, the ciphertext C can be decrypted.

$$\text{Decrypt}(P_k, C, S_k) \longrightarrow M. \tag{4}$$

3.3. IPFS. The InterPlanetary File System (IPFS) is a persistent and distributed network transmission protocol for storing and sharing files. This file system can be accessed in a variety of ways, including FUSE and HTTP. When a file is uploaded to the IPFS system, the file and all the blocks in it will be given a unique fingerprint called cryptographic hash, which uniquely identifies the file uploaded to IPFS, so that the user can search via the hash string. When other nodes in the system have the same file, the encrypted hash can be applied to download the file from multiple nodes at the same time. IPFS has the following advantages.

3.3.1. Fast Download Speed. It utilizes the BitTorrent protocol to make data transmission faster on the IPFS network.

3.3.2. High Security. Its decentralized feature enables data storage more secure, and data files cannot be downloaded or uploaded due to a node failure.

3.3.3. Low Redundancy. IPFS is a block storage model based on content addressing. Each file is clearly identified in the global namespace based on content addressing, reducing the redundancy of network storage.

3.4. Symbol Description. In Table 1 lists the all notations that will be used in this paper.

4. B-SSMD: Blockchain-Based Secure Sharing System of Medical Data

4.1. System Architecture. The B-SSMD system proposed in this paper is devised in a four-layer architecture, consisting of a storage layer, blockchain network layer, API layer, and application layer, as shown in Figure 2. The function of each layer is described as follows.

Table 1: Notations and their meanings.

Notation	Meaning
M	Medical record
P	Patient
D	Doctor
H	Hospital
U	User
I_i	I_P Patient information, I_d doctor information
w	Access control strategy
T	Time
C	Ciphertext
T	IPFS path
ϑ	Attacker
K	Key
A	Attribute

4.1.1. Storage Layer. The system adopts the on-chain and off-chain hybrid storage scheme. The bottom layer uses IPFS distributed storage technology to store symmetrically encrypted data. The blockchain in the system is divided into three categories, patient information blockchain (PIB), medical staff information blockchain (MSIB), and medical record information blockchain (MRIB).

4.1.2. Blockchain Network Layer. This layer is to perform the functions of the blockchain in the system and realize functions such as data update, status synchronization, and access control.

4.1.3. API Layer. In this layer, by calling API, block broadcast transmission, etc., are realized.

4.1.4. Application Layer. The function of this layer is to realize user registration, information retrieval, authority management, etc.

4.2. Three-Chain Model. The B-SSMD system proposed in this paper applies the PIB/MSIB/MRIB three-chain model to store patient information, medical staff information, and medical records in three different information blockchains. The system has a strict access

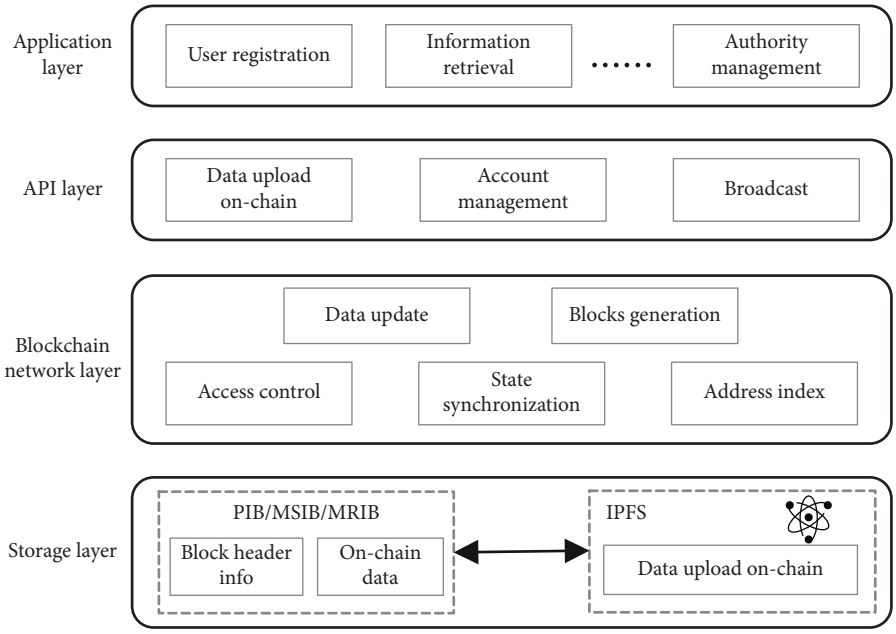

Figure 2: B-SSMD system architecture.

mechanism. Only legal users who have passed the administrator's security authentication are allowed to share and maintain blockchain node information and access system data. The data of the three information chains have considerable adhesion, and the system has strict access control strategies. Thus, it is difficult for attackers to invade the system. Since the encrypted data is classified and hierarchically stored in different blockchains, when an attacker attempts to crack all medical information of a user, all the data of the three blockchains must be acquired at the same time and decrypted. Since the three-chain model realizes the distributed storage of users' medical information, and the system adopts strict access control strategies, hence obtaining data from three blockchains simultaneously is quite difficult. Additionally, in order to relieve the node load of the blockchain and further strengthen the system stability, the hash address of IPFS is stored on-chain and the encrypted data is stored off-chain in this scheme.

The three-chain model of the system is shown in Figure 3, and the implementation mechanism is as follows.

4.2.1. Patient Information Blockchain (PIB). Nodes in this blockchain record patient detailed information $I_p(I_n, I_s, I_a, I_{IDn}, I_{\text{tel}})$, such as the patient's name I_n, gender I_s, age I_a, ID number I_{IDn}, telephone number I_{tel}, etc. PIB node information is associated with MRIB node information, that is, the medical records $M(M_t, M_s, M_d)$ of a patient P_i in the hospital H_1 are written and stored on MRIB by doctor D_1. When P_i is transferred to hospital H_2, the system should only query the medical information $M(M_t, M_s, M_d)$ of P_i on the blockchain $\text{MRIB}_{D_2} \longrightarrow M$ when the doctor D_2 needs. The system grants the data access authority to relevant doctors according to the access control policy w to avoid node information leakage.

4.2.2. Medical Staff Information Blockchain (MSIB). MSIB records the detailed information of medical staff $I_d(I_n, I_s, I_a, I_{IDn}, I_{\text{tel}}, I_h, I_o, I_p, I_e)$. Similar to the patient information, it should also record the served hospital I_h, department I_o, the level I_p and related evaluations I_e of doctors. The medical staff information is stored on-chain, and the patient P_i can quickly acquire the basic situation of the doctor D_i by reading the information of $D_i\text{MSIB}_{p_i} \longrightarrow I_d$ through system access control policy w. Meanwhile, patients can also evaluate the doctor's treatment level and satisfaction as a reference for other users. Compared with traditional medical systems, this scheme can realize the two-way interaction of doctor-patient information and improve the flexibility of data access and processing.

4.2.3. Medical Records Information Blockchain (MRIB). It records the relevant medical record information $M(M_t, M_s, M_d)$ of the patient, mainly including the treatment time M_t, the treatment location M_s, the detailed treatment situation M_d, etc. The medical record information is unilaterally written by the doctor D_i. Since the MRIB node contains the patient's important sensitive information related to life safety, the information released by D_i should include the doctor's digital signature $M' = (\text{sig}_{\text{Data}} \| M)$, so that this digital signature can ensure the nonrepudiation of the diagnosis information of doctors and hospitals when medical disputes occur.

4.3. System Scheme. In the B-SSMD system proposed in this paper, the medical data is processed by symmetric encryption, and the key K is double-encrypted through CP-ABE. Finally, the obtained ciphertext group is stored off-chain in IPFS, and the returned index address, data ID, time,

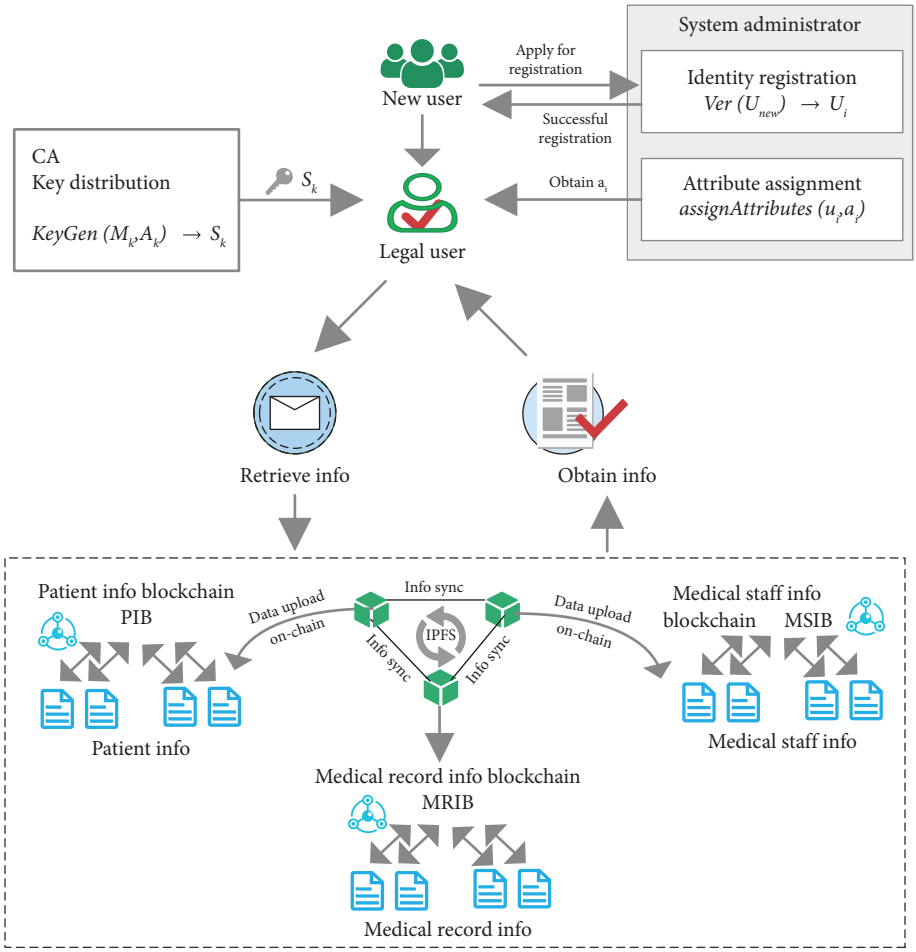

Figure 3: B-SSMD three-chain model.

and other data are uploaded on the blockchain. Meanwhile, the scheme assigns authorities based on user attributes to realize fine-grained data access. The scheme achieves medical data security sharing through the following phases.

4.3.1. Initialization. The security parameter λ is taken as input, the public parameter P_k and the master key M_k are generated by the Certificate Authority (CA) for secure storage.

4.3.2. Identity Registration. A new user u_{new} should register unique accounts at first, and the system administrator should verify the identity and qualification $\text{Ver}(u_{\text{new}})$. When u_{new} is successfully verified, the system automatically adds the user $\text{addUser}(u_i)$, so that u_{new} becomes a legal user u_i and obtains the corresponding attributes. When the user logs off, the administrator executes the user delete operation $\text{deleteUser}(u_i)$ and deletes the user information and attributes. The system parameters are shown in Tables 2 and 3.

The system administrator judges whether u_{new} has been registered through comparing the legal user information to determine whether u_i can join the system. The user addition operation $\text{addUser}(u_i)$ is described as follows (see Algorithm 1).

Table 2: User attribute.

User	Attribute
Doctor	Staff ID, department B, level P
Patient	Patient ID, consultation department B

Table 3: Parameter set.

Set	Meaning
$\mathbf{U_d}$	Doctor user set $U_d = \{u_1, u_2 \ldots u_n\}$
$\mathbf{U_p}$	Patient user set $U_p = \{u_1, u_2 \ldots u_n\}$
$\mathbf{B}$	Department set $B = \{B_1, B_2 \ldots B_n\}$
$\mathbf{G}$	Doctor level set $G = \{1, 2, 3, 4, 5\}$
$\mathbf{A_d}$	Doctor attribute set $A_d = \{D_{ID}, D_B, D_G\}$
$\mathbf{A_p}$	Patient attribute set $A_p = \{P_{ID}, P_B\}$

When u_i proposes to log off, the system administrator executes the user deletion program $\text{deleteUser}(u_i)$ as follows (see Algorithm 2).

After u_i has joined the system, the administrator should assign corresponding attributes. The user attribute assignment program $\text{assignAttributes}(u_i, a_i)$ is expressed as follows (see Algorithm 3).

4.3.3. Key Distribution. The system performs the key distribution algorithm $\text{KeyGen}(M_k, A_k)$, CA calculates the

(1) if: $u_{\text{new}} \notin U_d \vee U_p$
(2) $u_{\text{new}} \longrightarrow u_i$
(3) $U' = U \cup \{u_i\}$
(4) else:
(5) User already exists

Algorithm 1: AddUser(u_i).

(1) if: $u_i \in U_d \vee U_p$
(2) $U' = U/\{u_i\}$
(3) else:
(4) User does not exist

Algorithm 2: DeleteUser(u_i).

(1) if: $u_i \in U_d$
(2) allow (AssignA_d to u_i)
(3) else if: $u_i \in U_p$
(4) allow (Assign A_p to u_i)
(5) else:
(6) Unable to assign

Algorithm 3: AssignAttributes(u_i, a_i).

user's private key S_k based on the registrant attribute set $a \in A_k$ and sends it to the data visitor through a secure channel for storage. The process is as follows:

$$\text{KeyGen}(M_k, S) \longrightarrow S_k \longrightarrow \text{User}. \tag{5}$$

4.3.4. Data Encryption. The data owner (patient or doctor) provides the corresponding access control strategy w according to the visitor's attributes, randomly generates a symmetric encryption key K to encrypt data $C_1 = \text{Enc}_1(\text{Data}, K)$, and encrypts the key K through CP-ABE $C_2 = \text{Enc}_2(P_k, K, w)$.

4.3.5. Data Upload on Blockchain. The data owner stores the ciphertext group (C_1, C_2) off-chain in IPFS. The returned path L is encrypted through CP-ABE to obtain the path ciphertext $C_L = \text{Enc}_2(P_k, L, w)$, and relevant data such as C_L and time T are uploaded onto the blockchain.

4.3.6. Ciphertext Access. A legal visitor who meets the access control policy w can use the attribute key S_k to decrypt C_L obtained on the blockchain according to the decrypted access path $L = \text{Dec}_2(P_k, C_L, S_k)$ to retrieve and extract (C_1, C_2) stored in IPFS. Through decrypting the extracted data C_2 to acquire the symmetric key $K = \text{Dec}_2(C_2, S_k, P_k)$, the user can decrypt the shared data with the obtained key $K\text{Data} = \text{Dec}_1(C_1, K)$.

The access control strategy $w(r_i, p)$ in the scheme is specifically described as follows.

The user's information access authority on the three blockchains PIB, MSIB, and MRIB includes add (i), delete (d), change (u), and check (s). The system determines the access authority by judging the user attributes A_d, A_p, where the doctor-level attribute G is assigned to the hospital president $(G = 5)$, director $(G = 4)$, head nurse $(G = 3)$, doctor $(G = 2)$ and nurse $(G = 1)$. The system must assure all entities/stakeholders (patient, doctor, hospital president, department director, head nurse, nurse, etc.) granular access to medical data at a role level.

Strategy 1 Patient information blockchain (*PIB*). First, the system verifies the user's attribute ID. If the user is a doctor $u_{ID} \longrightarrow D$, the authority will be assigned based on the doctor's attribute level G. Among them, the president $(G = 5)$ can view all patient information in emergency situations. The director, head nurse and nurses $(3 \le G < 5 \vee G = 1)$ can only view the patient information in this department B_i. The doctor $(G = 2)$ can only view the received patient information. If the user is a patient $u_{ID} \longrightarrow P$, since the basic information of the patient is stored on PIB, only the patient user is assigned the authority to add, delete, modify, and check (i, d, u, s) the personal data (see Algorithm 4).

Strategy 2 Medical staff information blockchain (*MSIB*). First, the system verifies the user's attribute ID. If the user is a doctor $(u_{ID} \longrightarrow D)$, the authority will be assigned based on the doctor's attribute level G. Among them, the president $(G = 5)$ can view the information of all medical staff in this hospital. The director and head nurse $(3 \le G < 5)$ can only view the medical staff information in this department. The doctor and nurse $(1 \le G < 3)$ can add, delete, modify, and check (i, d, u, s) the own information. A patient $(u_{ID} \longrightarrow P)$ can query the information of relevant doctors and add evaluation (see Algorithm 5).

Strategy 3 Medical record information blockchain (*MRIB*). First, the system verifies the user's attribute ID. If the user is a doctor $(u_{ID} \longrightarrow D)$, the authority will be assigned based on the doctor's attribute level G. In MRIB, the president $(G = 5)$ can view the medical records of all patients under emergency. The director, head nurse, and nurses $(3 \le G < 5 \vee G = 1)$ can only view the medical records of patients in this department B_i. The doctor $(G = 2)$ can view and update the medical records of the received patients. A patient $(u_{ID} \longrightarrow P)$ can only view the personal medical records (see Algorithm 6).

4.4. Information Sharing Process P/MSISP. The information sharing process in B-SSMD includes two parts. One is the Patient information sharing process (PISP). The scheme realizes the information sharing of medical records among patients and medical staff. In PISP, PIB, and MRIB are the subjects of data storage and update, medical staff are the data visitors. Another is the Medical staff information sharing process (MSISP), which realizes the information sharing between patients and medical staff. In MSISP, MSIB is used for data storage and update, and patients are the data visitors.

(1) if: $u_{ID} \longrightarrow D$
(2) if: $G = 5$
(3) allow (Assign s of PIB_{all} to u_d)
(4) if: $3 \le G < 5 \vee G = 1$
(5) allow (Assign s of PIB_{B_i} to u_d)
(6) if: $G = 2$
(7) allow (Assign s of $\text{PIB}_{u_p \text{ of } u_d}$ to u_d)
(8) else if: $u_{ID} \longrightarrow P$
(9) allow (Assign i, d, u, s of PIB to u_p)
(10) else:
(11) No permission

Algorithm 4: Patient information strategy.

(1) if: $u_{ID} \longrightarrow D$
(2) if: $G = 5$
(3) allow (Assign s of MSIB_{all} to u_d)
(4) if: $3 \le G < 5$
(5) allow (Assign s of MRIB_{B_i} to u_d)
(6) if: $1 \le G < 3$
(7) allow (Assign i, d, u, s of MSIB to u_d)
(8) else if: $u_{ID} \longrightarrow P$
(9) allow (Assign s, i of $\text{MSIB}_{u_d \text{ of } u_p}$ to u_d)
(10) else:
(11) No permission

Algorithm 5: Medical staff information strategy.

(1) if: $u_{ID} \longrightarrow D$
(2) if: $p_d = 5$
(3) allow (Assign s of MRIB_{all} to u_d)
(4) if: $3 \le G < 5 \vee G = 1$
(5) allow (Assign s of $\text{MRIB}_{u_p \text{ of } B_i}$ to u_d)
(6) if: $G = 2$
(7) allow (Assign s, i of $\text{MRIB}_{u_p \text{ of } u_d}$ to u_d)
(8) else if: $u_{ID} \longrightarrow P$
(9) allow (Assign s of MRIB to u_d)
(10) else:
(11) No permission

Algorithm 6: Medical record information strategy.

The blockchain data access process consists of three steps, uploading user hash data on-chain, reading the node data on-chain, and updating the data on-chain. The scheme model is shown in Figure 4, and the specific process is as follows.

4.4.1. Patient Information Sharing Process (PISP). Patient information upload. The patient uploads the encrypted data and the encrypted key $(C_1 \| C_2)$ to IPFS and obtains the access path L of the ciphertext. The user sends the information $I(\text{Data}_{\text{ID}}, P_{ID}, C_L, w, T)$ including the data Data_{ID}, the data owner (patient) P_{ID}, the access control strategy w, the path ciphertext C_L, and the release time T on *PIB*. In order to identify the data source, the patient's digital signature must be uploaded.

$$\begin{aligned} (C_1 \| C_2) &\longrightarrow \text{IPFS}, \\ \left\{ I(\text{Data}_{\text{ID}}, P_{ID}, C_L, w, T) \| \sigma_p(I) \right\} &\longrightarrow \text{PIB}. \end{aligned} \tag{6}$$

Medical staff access data on PIB/MRIB. The data visitor (doctor) D obtains the data path as ciphertext C_L from PIB and MRIB, decrypts it to obtain the path $L = \text{Dec}_2(P_k, C_L, S_k)$ and finds the encrypted data $(C_1 \| C_2)$ in IPFS. Then, decrypt and read the key $K = \text{Dec}_2(P_k, C_2, S_k)$ and acquire the data $\text{Data}_p = \text{Dec}_1(C_1, K)$. For the patient's first consultation, D should not access the information of the

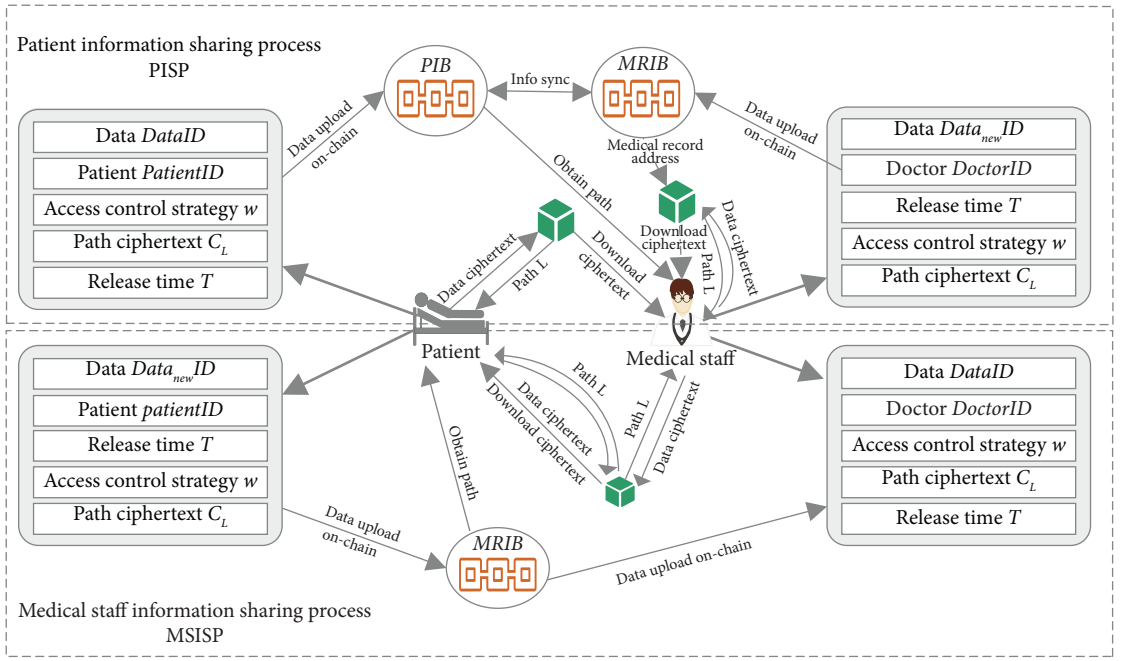

Figure 4: Information sharing process.

patient P on MRIB. For patients who have been transferred or visited multiple times, D can view the previous medical records M by accessing the information on MRIB, and the patient do not need to be checked again. The information access process can be expressed as follows:

$$\frac{\text{PIB}}{\text{MRIB}} \longrightarrow \{L = \text{Dec}_2(P_k, C_L, S_k)\} \longrightarrow \text{IPFS} \longrightarrow (C_1 \| C_2) \longrightarrow \{K = \text{Dec}_2(P_k, C_2, S_k), \text{Data}_p = \text{Dec}_1(C_1, K)\}. \tag{7}$$

Medical staff update data on MRIB. After the data visitor (doctor) D reads the patient information, a new medical record M' will be generated. At this time, D uploads the data and the encryption key $(C_1 \| C_2)$ to IPFS. Then encrypt the obtained path to ciphertext C_L, and the information $I(\text{Data}_{\text{newID}}, \text{Doctor}_{\text{ID}}, C_L, w, T)$, including data $\text{Data}_{\text{newID}}$, the visitor $\text{Doctor}_{\text{ID}}$, the visit time T and access control strategy w, together with the doctor's digital signature $\sigma_d(I)$, will be uploaded on the blockchain. The information update process is shown as follows:

$$\begin{aligned} (C_1 \| C_2) &\longrightarrow \text{IPFS}, \\ \{I(\text{Data}_{\text{newID}}, \text{Doctor}_{\text{ID}}, C_L, w, T) \| \sigma_d(I)\} &\longrightarrow \text{MRIB}. \end{aligned} \tag{8}$$

4.4.2. Medical Staff Information Sharing Process (MSISP). The information of medical staff is mainly used as the data sharing content and the information is obtained by users such as patients in this scheme.

Medical staff upload information. The doctor uploads the encrypted data and encrypted key $(C_1 \| C_2)$ to IPFS then stores the obtained information $I(\text{Data}_{\text{ID}}, \text{Doctor}_{\text{ID}}, C_L, w, T)$ including the encrypted path C_L, data Data_{ID}, the data owner (doctor) $\text{Doctor}_{\text{ID}}$ and time T on MSIB. In order to identify the data source, the doctor's digital signature must be uploaded simultaneously.

$$\begin{aligned} (C_1 \| C_2) &\longrightarrow \text{IPFS}, \\ \{I(\text{Data}_{\text{ID}}, \text{Doctor}_{\text{ID}}, C_L, w, T) \| \sigma_d(I)\} &\longrightarrow \text{MSIB}. \end{aligned} \tag{9}$$

Patient access data on MSIB. When the patient views relevant information of the doctor, the encrypted path C_L in IPFS from MSIB should be obtained, and decrypt it $L = \text{Dec}_2(P_k, C_L, S_k)$. Then, retrieve the data $(C_1 \| C_2)$ in IPFS and view the medical staff information after decryption.

$$\text{MSIB} \longrightarrow \{L = \text{Dec}_2(P_k, C_L, S_k)\} \longrightarrow \text{IPFS} \longrightarrow (C_1 \| C_2) \longrightarrow \{K = \text{Dec}_2(P_k, C_2, S_k), \text{Data}_d = \text{Dec}_1(C_1, K)\}. \tag{10}$$

Patient update data on MSIB. The patient can evaluate the medical staff, and the evaluation information, namely, the updated data $\text{Data}_{d\text{new}}$, should be uploaded on the blockchain. The patient stores the encrypted data and encrypted key $(C_1 \| C_2)$ in IPFS. The obtained encrypted path C_L and the information $I(Data_{\text{newID}}, P_{ID}, T, w, C_L)$ including data $\text{Data}_{\text{newID}}$, the data visitor P_{ID}, the visit time T and access control strategy w will be uploaded on the blockchain. In order to identify the source of the new data, the patient's signature must be submitted.

$$\begin{aligned} (C_1 \| C_2) &\longrightarrow \text{IPFS}, \\ \{I(\text{Data}_{\text{newID}}, P_{ID}, T, w, C_L) \| \sigma_p(I)\} &\longrightarrow \text{MSIB}. \end{aligned} \tag{11}$$

5. Security Analysis

The security of data storage and sharing is an important feature of B-SSMD. In this scheme, the access control strategy is strict and the encrypted data is hierarchically stored in the three blockchains. The processes from data storage to data sharing are all secure.

5.1. Data Privacy Preservation. In the user authority distribution strategy in section 4.3, the user U should satisfy the corresponding attribute relationship for data access. Assuming that the attacker ϑ is a gynecologist with the attributes $A_d = \{D_{ID}, D_B, D_G\}$, where $D_{ID} = \vartheta_{ID}, D_B = B_{\text{gynecology}}, D_G = 2$. If ϑ intends to acquire the patient data of orthopedics, as the attribute A_d of ϑ does not satisfy the orthopedic doctor attribute, $D_B \neq B_{\text{orthopedics}}$, the obtained path ciphertext C_L from the blockchain, decrypted through the key S_k of ϑ, is invalid, that is, $L \neq \text{Dec}_2(P_k, C_L, S_k)$. Therefore, the privacy property is ensured in B-SSMD, and the medical staff in the system cannot steal any data beyond the limit of authority.

5.2. Resistance to Single-Point-of-Failure Attacks. B-SSMD is built through three consortium blockchains PIB/MSIB/MRIB. Users on each blockchain do not need to trust each other before and thus any node cannot control the whole blockchain system. Since the patient data Data_p, the medical staff data Data_d and medical record M are stored decentralized within the scheme rules, data between nodes are mutually independent, the attacker ϑ attacking one or some nodes will not cause the entire system paralyzed. Besides, the system uploads encrypted data to IPFS and blockchains, and the use of decentralized storage can resist single-point-of-failure attacks.

5.3. Resistance to Impersonation Attacks. The user U uses private key S_k to encrypt data $C_1 = \text{Enc}_1(\text{Data}, K)$, $C_2 = \text{Enc}_2(P_k, K, w)$, and store $\text{Data} = (C_1 \| C_2)$ in IPFS. Assuming that the attacker ϑ steals the data at this time, since ϑ cannot decrypt C_1 and C_2, the user's identity information will not be changed. The user U encrypts the IPFS address index $C_L = \text{Enc}_2(P_k, L, w)$, and uploads $\text{Data} = I(\text{Data}_{ID}, P_{ID}, C_L, w, T)$ on the blockchain. Assuming that the attacker ϑ is stealing data at this time, since ϑ cannot decrypt C_L, the address index in IPFS cannot be queried, and user information cannot be obtained. ϑ does not have the ability to change user identity information. Thus, ϑ fails to perform an impersonation attack.

5.4. Resistance to Replay Attacks. The B-SSMD system uses the blockchain technology as the overall architecture, and the user U uploads the data of PIB/MSIB/MRIB including the access time T of U.

If the attacker ϑ obtains the information returned by the blockchain node and plans to launch a replay attack, the time T needs to be modified, whereas the data signature σ_i needs to be modified at the same time. Since the attacker ϑ cannot obtain a valid signature generated by a legal user, the system prevents replay attacks.

If the system has successfully verified the user's identity $\text{Ver}(u_{\text{new}})$, assuming that the attacker ϑ steals the user identity information $\{U_{ID}, U_A\}$ returned by the system, obtains the data requested by the user $\text{request} = \{\text{Data}_1 \| T'\}$ at the same time, and pretends to be the user to send data $\{\text{Data}_1 \| T'\}$ to the system, when the system obtains two timestamps $\{T, T'\}$, it is judged that the time difference $T - T' > \Delta T$ indicating a replay attack exists in the system. Therefore, the proposed scheme can resist replay attacks.

5.5. Resistance to Malicious Tampering Attacks. A legal blockchain contains a large number of nodes. When data is uploaded to the blockchain, each node will back up the data. Meanwhile, due to the distributed storage performance of the blockchain ledger, a single node cannot modify data on the chain.

Suppose a node in the blockchain system is an attacker ϑ, when ϑ attacks, it needs to improve its own computing power so that the computing power can obtain more than 50% of the control right before the attack can succeed. Since the B-SSMD system proposed in this paper exploits the three-chain model, when a patient completes a visit, the system requires the patient and the medical personnel to update the three PIB/MSIB/MRIB blockchains respectively. It can be seen that the data update speed in the legal chain is very fast, so the attacker cannot get control. At the same time, as the hospital is an institution with strong credibility in the society, there is little possibility of a large-scale active attack on the blockchain system. Therefore, the system can resist malicious tampering attacks.

5.6. User Group Members Update. In Section 4.3, the system administrator can add and delete users $\text{addUser}(u_i)$ and $\text{deleteUser}(u_i)$. In the process of a new user applying to join the system, the administrator compares the system internal user set $U_i = \{u_1, u_2 \ldots u_n\}$, each legal user has a unique U_{iID}, and the system administrator only needs to determine whether the new user U_{newID} corresponds to the internal legal user U_{iID}. If $U_{\text{newID}} \neq U_{iID}$, the user identity meets the requirements for joining the system, otherwise the verification fails and the user cannot join the legal user group. When the user is deleted, if $U_{\text{newID}} = U_{iID}$, the user identity meets the logout requirements, otherwise the verification fails and the user cannot be deleted.

6. Performance Analysis

In this section, we give a performance evaluation of the system, with an emphasis on the probability of effective attacks and performance comparison. For running our experiments, we used a 2.3 GHz Quad-Core Intel Core i5 CPU, 8 Gb LPDDR3 RAM, and 512 Gb SSD hard disk drive.

6.1. System Ability to Attack Resistance. Suppose that the probability of an attacker ϑ generating a node is p_{AC}, and the probability of a legal blockchain generating a node is p_{BC}, when the honest node BC generates z blocks, the probability of an effective attack is a Poisson distribution and the expectation is $\lambda = z \times (p_{AC}/p_{Bc})$. The probability that ϑ generates k blocks is $\lambda^k/k!e^{-\lambda}$. At this time, the number of blocks generated by ϑ behind the honest node is $(z-k)$ and the probability that the length of AC exceeds that of BC is $(p_{AC}/p_{Bc})^{(z-k)}$. Thus, the probability of an effective attack is

$$p = \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} e^{-\lambda} \times \begin{cases} \left(\frac{p_{AC}}{p_{Bc}}\right)^{(z-k)}, & k \le z, \\ 1, & k > z, \end{cases} \tag{12}$$

namely,

$$\begin{aligned} p &= \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(\frac{p_{AC}}{p_{Bc}}\right)^{(z-k)} + \sum_{k=z+1}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \\ &= 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - \left(\frac{p_{AC}}{p_{Bc}}\right)^{(z-k)}\right). \end{aligned} \tag{13}$$

In this paper, we compare the proposed scheme with the related EMRs sharing schemes in Liu et al. [21] and Cao et al. [32] in terms of the ability to attack resistance. The scheme [21] adopts blockchain with single chain mode. Although it meets the characteristics of tamperability and anonymity, the probability of effective attacks is still high. An attacker ϑ only needs to damage one chain to attack the system effectively. The probability of an effective attack in the scheme [21] can be described as follows:

$$P_{\text{scheme}[15]} = p. \tag{14}$$

The scheme [32] adopts a consortium blockchain to share sensitive data related to patient privacy while sharing the nonsensitive parts on the public blockchain. This scheme exploits a hybrid double-chain structure and is superior to the scheme [21] to some extent. The probability of an effective attack in the scheme [32] can be described as follows:

$$P_{\text{scheme}[16]} = p^2. \tag{15}$$

The B-SSMD system proposed in this paper applies the PIB/MSIB/MRIB three-chain model. The patient information, medical personnel information, and medical records are updated at the same time during the medical treatment process, and the node generation speed of the three chains is almost the same. Thus, the probability of an effective attack in our scheme decreases exponentially and the security performance is better than the scheme [21, 32]. The probability of an effective attack in this scheme can be described as follows:

$$P_{B\text{–SSMD}} = p^3. \tag{16}$$

In the experiment, by setting the probability p_{AC} as 0.1, 0.2, and 0.3, respectively, the probability $P_{B\text{–SSMD}}$ is tested to verify the higher security of our scheme. Meanwhile, by setting $p_{AC} = 0.3$, it is verified that the ability to attack resistance in our scheme is superior to that in the scheme [21, 32].

As shown in Figure 5, when $p_{AC} = 0.1$, the probability of the attacker's effective attack is almost 0. As the probability p_{AC} increases, when p_{AC} reaches 0.3 and the number of nodes generated by the legal blockchain $z > 6$, the probability of an effective attack is almost 0. In the actual medical system, the number of nodes generated by the blockchain far exceeds 6. Thus, it is almost impossible for ϑ to attack this system effectively.

In Figure 6, when $p_{AC} = 0.3$ and the number of blocks generated by the legal chain is 1, the probability of effective attacks of our proposed scheme B-SSMD is about 0.2, while this probability of scheme [21] is about 0.7 and the probability in the scheme [32] also reaches about 0.4. With the increase of the number of blocks, the probability of effective attacks will be relatively reduced. In our scheme, when the number of blocks reaches about 5, the probability of an effective attack has approached 0, However, when the number of blocks generated in the scheme [21] reaches 10, there is still the possibility of being effectively attacked. And, in the scheme [32], when the number of blocks generated reaches 8, the probability of a successful attack approaches 0.

It can be seen that the performance of attack resistance in the B-SSMD system has been greatly improved. Especially under the condition of huge data access amount in the current medical system, the update speed of blocks in the legal blockchain is relatively fast, so the probability of effective attacks in the practical application of this scheme is very low.

6.2. Block Efficiency and Throughput. Throughput is a measure of the system's ability to deal with transactions per unit time, which is directly related to the system's block efficiency and consensus mechanism [33]. In this paper, TPS (Transactions per second) is used to represent throughput, as shown in the following equation:

$$\text{TPS} = \frac{\text{SumTransaction}}{\text{Time}}, \tag{17}$$

where *SumTransaction* is the number of EMR information contained in a single block, and *Time* is the block generation time of a single block.

In order to verify the throughput efficiency of our scheme, we build a blockchain network for the model simulation test. During the operation of the system model, the number of blocks for each consensus group is N, and all nodes are honest nodes. Our results in Table 4 show that, as the number of nodes increases, the throughput decreases gradually. For example, when the number of nodes increases from 4 to 14, the throughput decreases from 996 TPS to 761 TPS. Also, the proposed model is about 142 times higher than the bitcoin network which uses the POS consensus mechanism, and about 13 times higher than the Ethernet network that using the POW consensus mechanism.

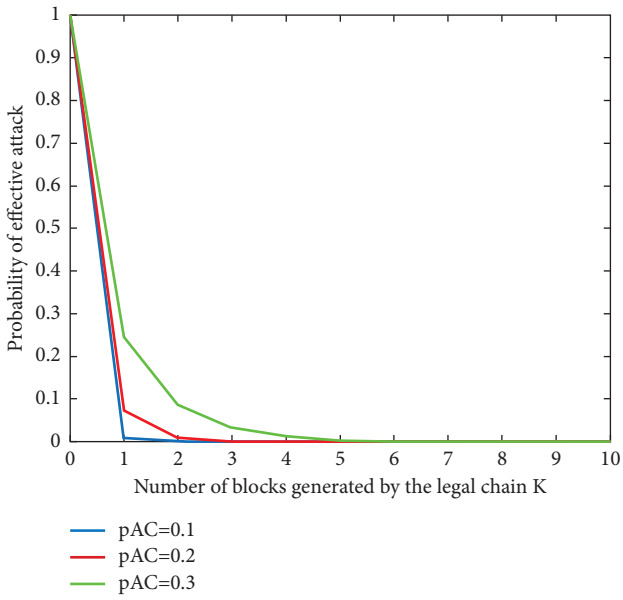

Figure 5: Probability of effective node attacks.

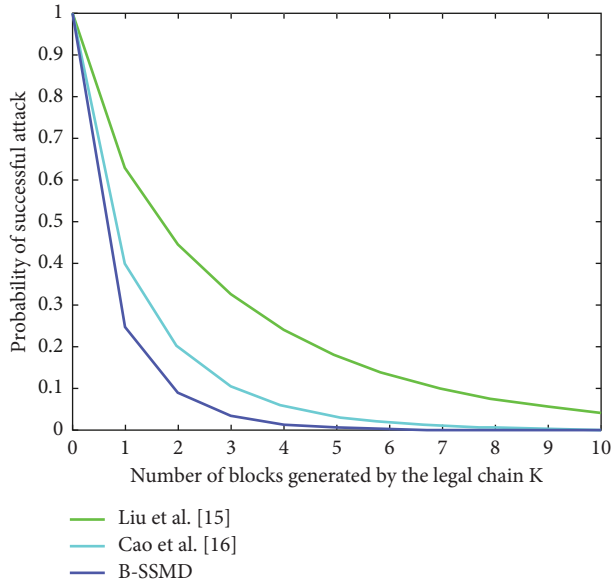

Figure 6: Comparison of effective attack probability.

Table 4: The throughput of B-SSMD.

Number of nodes	TPS
4	996
6	964
8	927
10	885
12	812
14	761

Table 5: Number of data request confirmation.

Test duration/s	Data request confirmation amount
100	9717
200	19230
300	29006
400	38794
500	48493

Besides, we conduct a test on B-SSMD using FISCO BCOS as the blockchain platform of the system and use a docker container to simulate 4 nodes with Caliper tools to send requests using a smart contract to view data. The amount of data requests confirmed in the blockchain transaction pool within a fixed time is shown in Table 5.

Table 6: Scheme comparison.

Scheme	Mainchain pressure	Blockchain structure	Security	Division granularity	Encryption mode
Liu et al. [21]	++	Single	+	−	Public key
Cao et al. [32]	+	Hybrid double	−	−	Hash
Malamas et al. [34]	−	Hierarchical	+	+	CP-ABE
Proposed scheme	−	Hybrid three	++	++	Three-layer

Table 7: Security comparison.

Scheme	Liu et al. [21]	Cao et al. [32]	Malamas et al. [34]	Lee et al. [22]	Proposed scheme
Resistance to single-point failure	×	×	×	√	√
Resistance to impersonation	×	×	√	√	√
Resistance to replay attacks	×	×	×	√	√
Resistance to malicious tampering	√	√	√	√	√
User group members update	×	×	×	×	√

It can be seen that the transaction amount can be stabilized above 96 transactions/s, indicating that the system can achieve its high-quality transaction processing capacity.

6.3. Performance Comparison. As shown in Table 6, by comparing with the blockchain-based medical data sharing schemes proposed in [21, 32, 34], it shows that the B-SSMD scheme adopts a three-chain distributed structure to reduce the burden on the mainchain, and the three-layer encryption and fine-grained access control improve the security of data sharing.

In Table 7 describes the security flaws of our scheme and other schemes, and it shows that most previously developed schemes do not have important security attributes. The proposed scheme not only resists possible attacks but also explains in detail overall operation and process. Therefore, compared with the schemes proposed in [21, 22, 32, 34], the B-SSMD in this paper has considerable advantages.

7. Conclusion

We focus on the medical data sharing scheme based on blockchain and proposes the B-SSMD system scheme. Through integrating the three-chain model with IPFS technology, by adopting the method of storing data on-chain and index path off-chain, it realizes a high degree of distribution of data storage and solves the defects of the centralized storage in traditional medical systems. In addition, by utilizing the three-layer encryption and fine-grained access control, the P/MSISP data sharing process is proposed, which protects the user privacy and improves the data security. Finally, the security analyzes prove our scheme to be secure, and the simulation experiments demonstrate our scheme is feasible. For further research work, one possible improvement is the transferability of the B-SSMD system. Not only in medical environments, but in other scenarios, how to use the three-chain model to solve the problem of data sharing is work that we can explore in the future.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant no. 62102312), the Natural Science Basic Research Program of Shaanxi (Grant no. 2021JQ-722), Young Talent Fund of University Association for Science and Technology in Shaanxi (Grant no. 20210119), Communication Soft Science of Chinese Ministry of Industry and Information Technology (Grant no. 2021R45), and the Scientific Research Program funded by Shaanxi Provincial Education Department (Grant no. 20JK0906).

References

[1] B. A. Tama, B. J. Kweka, Y. Park, and K.-H. Rhee, "A critical review of blockchain and its current applications," in *Proceedings of the International Conference on Electrical Engineering and Computer Science*, pp. 109–113, Palembang, Indonesia, December, 2017.

[2] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: a systematic literature review," *Journal of Biomedical Informatics*, vol. 46, no. 3, pp. 541–562, 2013.

[3] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain meets cloud computing: a survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2009–2030, 2020.

[4] C. Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski, and L. Fang, "Secure keyword search and data sharing mechanism for cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 6, pp. 2787–2800, 2021.

[5] J. G. Li, N. Y. Chen, and Y. C. Zhang, "Extended file hierarchy access control scheme with attribute-based encryption in cloud computing," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 2, pp. 983–993, 2021.

[6] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, and L. Fang, "A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 5, 2021.

[7] C. Ge, Z. Liu, J. Xia, and L. Fang, "Revocable identity-based broadcast proxy re-encryption for data sharing in clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1214–1226, 2021.

[8] Y. Wang, S. Sun, J. Wang, J. K. Liu, and X. Chen, "Achieving searchable encryption scheme with search pattern hidden," *IEEE Transactions on Services Computing*, vol. 15, no. 2, pp. 1012–1025, 2022.

[9] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

[10] H. Wang, "Anonymous data sharing scheme in public cloud and its application in E-health record," *IEEE Access*, vol. 6, pp. 27818–27826, 2018.

[11] P. Liang, L. Zhang, L. Kang, and J. Ren, "Privacy-preserving decentralized ABE for secure sharing of personal health records in cloud storage," *Journal of Information Security and Applications*, vol. 47, pp. 258–266, 2019.

[12] Y. Zhang, M. K Qiu, C. W. Tsai, M. H. Hassan, A. Alamri, and Health-Cps, "Healthcare cyber-physical system assisted by cloud and big data," *IEEE Systems Journal*, vol. 11, no. 1, pp. 88–95, 2017.

[13] N. Armstrong, B. H. Jin, D. S. Kim et al., "Threat-specific security risk evaluation in the cloud," *IEEE Transactions on Cloud Computing*, vol. 9, no. 2, pp. 1–13, 2018.

[14] S. NaKamoto and Bitcoin, "A peer-to-peer Electronic Cash System," 2022, https://bitcoin.org/bitcoin.pdf.

[15] Y. Yuan and F. Y. Wang, "Blockchain: the state of the art and future trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, 2016.

[16] B. Zhao, L. Fang, H. Zhang et al., "A digital watermark management system based on smart contracts," *Sensors*, vol. 19, no. 14, p. 3091, 2019.

[17] M. Banerjee, J. Lee, and K. KR. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018.

[18] B. Shen, J. Guo, and Y. Yang, "MedChain: efficient healthcare data sharing via blockchain," *Applied Sciences*, vol. 9, no. 6, p. 1207, 2019.

[19] S. M. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 11, pp. 4613–4641, 2020.

[20] J. P. Dias, H. S. Ferreira, and A. Martins, "A blockchain-based scheme for access control in e-health scenarios," in *Proceedings of the 10th International Conference on Soft Computing and Pattern Recognition*, pp. 238–247, Porto, Portugal, April, 2020.

[21] J. W. Liu, X. L. Li, L. Ye, H. L. Zhang, X. J. Du, and M. Guizani, "BPDS: a blockchain based privacy-preserving data sharing for electronic medical records," in *Proceedings of the IEEE Global Communications Conference*, pp. 1–6, Abu Dhabi, UAE, February, 2018.

[22] T. F. Lee, H. Z. Li, and Y. P. Hsieh, "A blockchain-based medical data preservation scheme for telecare medical information systems," *International Journal of Information Security*, vol. 20, pp. 589–601, 2020.

[23] M. Madine, A. A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for giving patients control over their medical records," *IEEE Access*, vol. 8, pp. 193102–193115, 2020.

[24] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-based data preservation system for medical data," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–13, 2018.

[25] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, "Blockchain-based approach for e-Health data access management with privacy protection," in *Proceedings of the IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks*, Limassol, Cyprus, September, 2019.

[26] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, and L. Fang, "Revocable attribute-based encryption with data integrity in clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 5, 2021.

[27] Y. Zhang, M. Cui, L. Zheng, R. Zhang, L. Meng, D. Gao et al., "Research on electronic medical record access control based on blockchain," *International Journal of Distributed Sensor Networks*, vol. 15, no. 11, Article ID 1550147719889330, 2019.

[28] X. L. Wang, X. Z. Jiang, and Y. Li, "Model for data access control and sharing based on blockchain," *Journal of Software*, vol. 30, no. 6, pp. 1661–1669, 2019.

[29] A. Alniamy and D. T. Bradley, "Attribute-based access control of data sharing based on hyperledger blockchain," in *Proceedings of the 2nd International Conference on Blockchain Technology*, pp. 135–139, Berkeley, CA, USA, July, 2020.

[30] S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on blockchain," *IEEE Access*, vol. 7, pp. 112713–112725, 2019.

[31] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 321–334, Berkeley, CA, USA, May, 2007.

[32] Y. Cao, Y. Sun, and J. Min, "Hybrid blockchain–based privacy-preserving electronic medical records sharing scheme across medical information control system," *Measurement and Control*, vol. 53, no. 7-8, pp. 1286–1299, 2020.

[33] S. Kaur, S. Chaturvedi, A. Sharma, and J. Kar, "A Research Survey on Applications of Consensus Protocols in Blockchain," *Security And Communication Networks*, vol. 2021, Article ID 6693731, 2021.

[34] V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester, "A hierarchical multi blockchain for fine grained access to medical data," *IEEE Access*, vol. 8, pp. 134393–134412, 2020.