Hindawi
Security and Communication Networks
Volume 2022, Article ID 9889263, 11 pages
https://doi.org/10.1155/2022/9889263

*Research Article*

# A Blockchain-Based Privacy Preservation Scheme in Mobile Medical

**Haiying Wen, Meiyan Wei, Danlei Du, and Xiangdong Yin**

*School of Information Engineering, Hunan University of Science and Engineering, Yongzhou 425199, China*

Correspondence should be addressed to Haiying Wen; wenhaiying1022@huse.edu.cn

Received 21 June 2021; Revised 8 October 2021; Accepted 27 January 2022; Published 22 March 2022

Academic Editor: Honghao Gao



With the rapid development of mobile medical, how to establish an effective security mechanism to protect data security and privacy while users enjoy medical services has become an urgent problem to be solved. Aiming at the easy leakage of privacy in mobile medical terminals and untrustworthy data, we make use of a role-separated mechanism to generate trusted anonymous certificates. We propose a lightweight identity authentication scheme and adopt blockchain to protect the security of medical data. Meanwhile, in view of the problems of transparency and visibility of blockchain information, we adapt the searchable encryption algorithm to realize ciphertext processing in the whole life cycle. Experiments show that our scheme can reduce the cost of computation on the basis of ensuring traffic. In the process of dynamic updating of ciphertext keywords, except the keyword identifier, less information is leaked to the server, which protects privacy of users.

## 1. Introduction

Medical problems including medical care access and quality are common around the world. Medical resources are in short supply and it is difficult to distribute them evenly. Large numbers of individuals do not receive the quality care that they need [1]. Even geographical problems such as economic differences between different regions, topography, and topography bring various difficulties to medical health. These problems are especially obvious in the developing countries with large populations. It is obvious that the traditional medical model with major hospitals as the core has been unable to adapt to the development needs of the current era. Mobile medical, which mainly uses mobile communication technologies such as PDAs, smart phones, and satellite communications to provide users with medical services and data exchange, has successfully replaced the traditional medical model as the new darling, with the help of cloud center [2].

The concept of mobile medical originated from the telemedicine monitoring and medical treatment for astronauts conducted by NASA. Later applications such as the use of portable mobile devices to collect various body data have it further developed. As an innovative technology in the Internet plus medical mode, mobile medical can realize applications such as medical rescue, remote monitoring, and intelligent medical care. It is of great significance for promoting medical reform.

Mobile service composition [3, 4] meets the needs of people for medical services under the current social development. This demand is mainly reflected in the two aspects of distribution and data. To a certain extent, mobile medical has broken through the limitation of space and time in the traditional medical mode. Mobile medical empowers patients and health providers proactively to address medical conditions through near real-time monitoring and treatment, no matter the location of the patient or health provider.

In addition, a large amount of data (Internet traffic) is generated in the process of physical examination and treatment of patients, and doctors can use these data to make more reliable and accurate diagnoses. Mobile medical not only saves a lot of time spent on queuing up for registration, but also greatly reduces the pressure on the infrastructure brought by disease treatment. Through mobile sensors, medical devices, and remote patient monitoring products,

there are avenues through which medical care delivery can be improved. Mobile medical can help lower costs and connect people to care providers.

However, these mobile medical-related technologies are still incomplete [5]. They have certain flaws in the preservation of privacy. With the development of mobile medical, medical data are showing exponential growth. Meanwhile, these data collected by terminal equipment in mobile medical mode are closely related to users' physiological characteristics, geographic locations, images, and other private information [6].

In addition, with the rapid development of network intrusion technologies, personal medical data are facing risks of intentional or unintentional intrusion and access by unauthorized users. Due to the incomplete privacy preservation technologies, lacks, data security, and privacy preservation have become the main reason restricting the development of modern medical services. Due to the limitation of terminal resources and the sensitivity of medical information, existing privacy preservation technologies are difficult to directly apply. The design of specific security authentication, information integration, data access control, and data integrity verification schemes for mobile health environment is an important topic in the field of mobile health at present and in the future, and it is also a key link for the large-scale application of mobile medical in practice.

In this paper, we mainly discuss privacy preservation solutions of mobile terminals in Internet medical, which integrates the application of lightweight authentication, blockchain technology, anonymous certificates, and searchable encryption technology to realize the encrypted calculation and ciphertext of mobile medical device data. Data sharing has been implemented, and privacy preservation of medical data has been implemented.

## 2. Related Works

For the storage and transmission of medical data, scholars around the world have conducted a lot of researches. In 2012, Patra et al. [7] proposed a cloud-based model to process private data for patients. Through his framework, medical personnel and policy makers can use the cloud-based model to provide remote medical services to patients. This model stores all necessary data in a single cloud. By encouraging patients to share data in the cloud, patients can obtain medical staff services. Disease diagnosis and control can be performed through remote treatment. In 2014, Ye et al. [8] proposed a well-organized authentication and access control scheme based on the attributes of the perceived IoT access control layer.

In 2015, Zyskind et al. [9] proposed a privacy preservation platform, which uses third-party equipment to provide services and allows users to modify authorization while following the access control policies reserved on the blockchain. The proposed decentralized platform contains three objects: service providers, mobile phone users, and nodes that maintain the blockchain. Two types of transactions can be defined in the blockchain network in the platform: Tdata for data storage and recovery and access time and Taccess for access control management. The data collected through the user's mobile phone is encrypted and saved outside the blockchain. In the public chain, only data hashes are saved. Both users and services can query the data in Tdata transactions. In 2016, to solve the problems of slow medical record information access, data fragmentation, and user privacy preservation, Azaria et al. [10] completed a medical data sharing platform MedRec based on Ethereum. Peterson et al. proposed a blockchain-based participant in advance. A medical data sharing plan with a well-defined rule structure is agreed. Although this solution realizes the sharing of medical data, it lacks a universal access control strategy.

In 2017, Omar et al. [11] proposed data management system for patient healthcare. By adopting blockchain to protect privacy storage, it solves the problem of losing control when storing encrypted data in the system. In addition, by using encryption on the blockchain, the framework will not be affected by data preservation vulnerabilities. Do and Ng [12] proposed a system that uses blockchain technology to provide secure distributed data storage with keyword search services.

In 2018, Magyar [13] designed an integrated health information model that builds a decentralized and openly scalable network based on the blockchain operating environment, making access to data more secure. In order to handle the protected health information (PHI) generated by these devices, Griggs et al. [14] proposed utilizing blockchain-based smart contracts to facilitate secure analysis and management of medical sensors. Using a private blockchain based on the Ethereum protocol, they created a system where the sensors communicate with a smart device that calls smart contracts and writes records of all events on the blockchain. This smart contract system would support real-time patient monitoring and medical interventions by sending notifications to patients and medical professionals, while also maintaining a secure record of who has initiated these activities. This would resolve many security vulnerabilities associated with remote patient monitoring and automate the delivery of notifications to all involved parties in a HIPAA compliant manner. Liang et al. [15] proposed an innovative user-centric health data sharing solution, which uses the blockchain mechanism to protect privacy, strengthen identity management, and collect data in conjunction with mobile applications. Zhang and Lin [16] proposed a personal health record sharing scheme based on blockchain. This solution builds two different blockchains to realize the safe sharing of medical data. The plan separately builds a private chain and a consortium chain. The private chain realizes the encrypted storage of personal medical data. The consortium chain saves the security index corresponding to the personal medical data and secures the data sharing by verifying the doctor's identity token, which protects the medical data. However, using two types of blockchains will not only increase costs, but also reduce their execution efficiency. Ji et al. [17] investigated the location sharing based on blockchains for telecare medical information system. Firstly, they define the basic requirements of blockchain-based location sharing, including

decentralization, unforgeability, confidentiality, multilevel privacy preservation, retrievability, and verifiability. Then, using order-preserving encryption and Merkle tree, they proposed a blockchain-based multilevel location sharing scheme.

In 2019, Wang et al. [18] combined homomorphic encryption and proxy reencrytion technology to implement outsourcing computing solutions in healthcare systems. In this solution, there are several clients with different public keys, an electronic medical cloud platform, and an auxiliary cloud server. The electronic medical cloud platform can provide services to patients and regularly analyze data to provide better services. The HGD architecture based on blockchain proposed by Yue et al. [19] enables patients to safely control and share medical data. Aiming at the privacy of medical data, Tian et al. [20] proposed to establish a shared key that can be reconstructed by legitimate parties before the diagnosis and treatment process begins.

At present, a large number of excellent schemes [21–23] have emerged in mobile medical, and their security and flexibility have been continuously enriched. The characteristics of activity and diversification can better meet the needs of practical application, but there are still some deficiencies. Some schemes encrypt the patient information and store it on the blockchain, and some schemes use anonymous certificates to protect user information. But the doctor cannot read the relevant information. Therefore, it is necessary to design a scheme that can authenticate the device.

## 3. Scheme

*3.1. Structure.* As shown in Figure 1, the local computer of the mobile medical model generates the relevant parameters and sends them to the smart wearable device to start the authentication scheme. After a series of simple calculations, the smart wearable device feeds back the relevant parameters to the local computer. The local computer and the local blockchain node undergo a similar calculation process, and the blockchain node obtains the relevant parameters and sends them to the local computer; the local computer forwards the parameters to the smart wearable device. The smart wearable device performs decryption calculation and passes the verification, and the identity authentication ends smoothly. There are many kinds of mobile medical devices, including bracelets, watches, mobile phones, portable computers, etc. These devices can collect a variety of physiological signals of users, such as blood pressure, blood glucose, blood oxygen, body temperature, etc. After the authentication, the intelligent devices will upload those collected information to the blockchain.

The alliance chain is a blockchain that is jointly managed by multiple institutions, and the joining of network nodes requires the approval of the organization. It completes mutual authentication of the internal membership of the system through the PKI system. The user binds his real identity with the self-signed certificate issued by the CA in the PKI system. We divide the authority of CA into TCA and regulator, and TCA and regulator jointly issue anonymous certificates. After the anonymous certificate is generated, the local device successfully joins the blockchain network.

In order to ensure the privacy of users' medical and health data, the data on the chain is encrypted. For users who need to perform operations such as searching encrypted data, we adopt searchable encryption technology. It can support users to carry out keyword retrieval in ciphertext and realize keyword based secure search. It enables users to store encrypted data in the blockchain, perform keyword search through the ciphertext domain, and selectively retrieve relevant documents from it, so as to ensure the security of data.

### 3.2. Module

*3.2.1. Anonymous Certificate Generation.* A user submits the real-name certificate application and his real identity information to the *CA*. After the *CA* verifies, the real-name certificate Ecert will be issued by the user and saved in the *CA* database U. Then he generates his own anonymous identity AID, public and private key pair (APK, SPK), and random numbers $p$, $r_1$ and calculates the serial number of the anonymous certificate: $\mathrm{SN} = H(\mathrm{APK}, p)$. Then anonymous certificate header $b = (\mathrm{AID}, \mathrm{SN}, \mathrm{APK})$ and content $M = (b, h(\mathrm{Ecert}))$ are generated. After calculating the formula $u = g^{r_1}$, the user sends $u$ and the real-name public key signature $\mathrm{SigPK}(u)$ to the supervisor Admin. Verifying the signature information sent by the user, Admin calculates the formula $w = u_{d_1}$ and sends $w$ to the user, which will be saved in the supervisor database in the form of key-value pairs $<E_{d_1}(u)$: $ID>$. After the user accepts $w$, he uses *ASK* to perform signature calculation on $M$ which is $\mathrm{Sig}_{\mathrm{ASK}}(M)$ and send random numbers $r_1$ and $w$ to *TCA*. Then the *TCA* verifies the parameters sent by the user and, after the verification passes, calculates the formula $z = w_{d_2}$ and judges whether $Q = z{r_1}^{-1}$ is true. If $Q = z{r_1}^{-1}$, save <SN: $E_{d_2}(z)$>. in the database in the form of key-value pairs. Then it generates a random number $r_2$, calculates the joint signature: $Usigd = (g^{r_2}, (h^{-1}(M) + g^{r_2 * d_1 * d_2}) \cdot {r_2}^{-1})$, and sends it to the user. Then the user gets the anonymous certificate $(M, \mathrm{Usigd})$.

*3.2.2. Lightweight Authentication.* Relevant parameters in this section are shown in Table 1.

First the local computer generates a random number $x$ and a timestamp $t_R$ and sends them to the smart wearable device. After receiving the parameters, the device calculates whether $|t_R - {t_R}^*| \le \Delta T$ is true. If not, the communication delay is greater than the maximum delay allowed by the system, so the authentication stops. If $|t_R - t_R^*| \le \Delta T$, the smart wearable device generates a random number $y$ and a timestamp $t_T$ and performs the following calculations based on ID and $K$:

$$N_1 = ROL(K \oplus y, x), \tag{1}$$

$$N_2 = ROL(ID \oplus y, x). \tag{2}$$

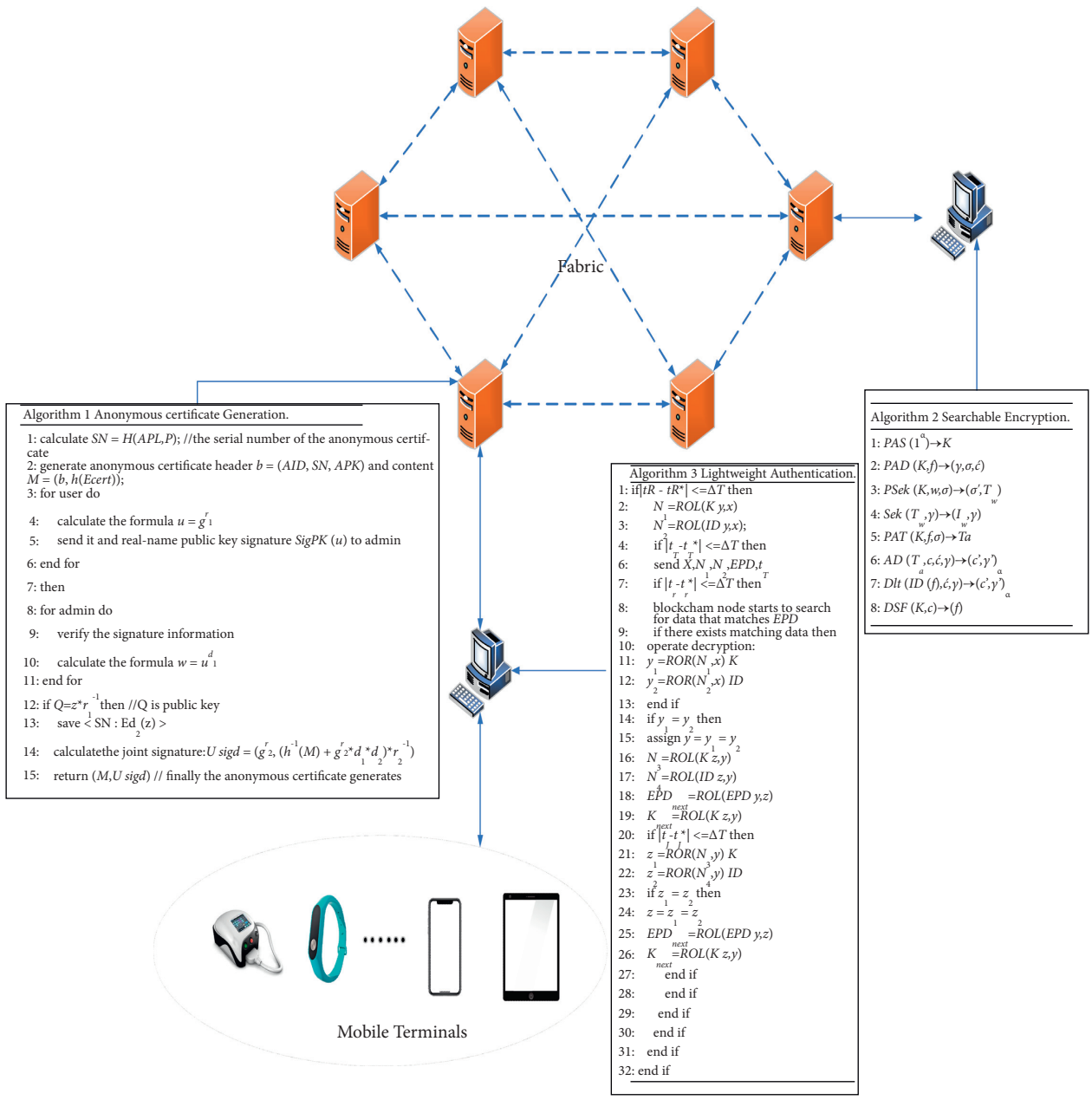


Figure 1: The system structure.

The smart wearable device feeds $N_1$, $N_2$, EPD, $t_T$, $x$ to the local computer. When receiving those parameters, the local computer calculates whether $|t_T - t_T^*| \le \Delta T$ is true. If true, the local computer generates a timestamp $t_r$ and sends $N_1$, $N_2$, $t_r$, $x$, and EPD to the blockchain node. If not, the authentication stops.

When $|t_T - t_T^*| \le \Delta T$ and the blockchain node receives the parameters, the node calculates whether $|t_T - t_T^*| \le \Delta T$ is true. If $|t_T - t_T^*| \le \Delta T$, the blockchain node starts to search for data that matches EPD; else the authentication stops. If there is no matching data, we can obtain the matching ID and $K$ for decryption operation. Perform the following calculations $y_1 = \mathrm{ROR}(N_1, x) \oplus K$ and $y_2 = \mathrm{ROR}(N_2, x) \oplus \mathrm{ID}$. Then judge whether $y_1$ and $y_2$ $X$ are equal. If $y_1 \ne y_2$, it indicates that the data is not credible, and the authentication stops. If $y_1 = y_2$, the blockchain node authentication continues and assigns $y = y_1 = y_2$. The blockchain node generates a random number $z$ and a timestamp $t_J$ to perform the following calculations: $N_3 = \mathrm{ROL}(K \oplus z, y)$ and $N_4 = \mathrm{ROL}(ID \oplus z, y)$. After that, the following operation formulas $\mathrm{EPD}_{\mathrm{next}} = \mathrm{ROL}(\mathrm{EPD} \oplus y, z)$ and $K_{\mathrm{next}} = \mathrm{ROL}(K \oplus z, y)$ can be obtained.

The blockchain node sends $N_3$, $N_4$, $t_T$ to the local computer. After the local computer receives the parameters, it first calculates whether $|t_J - t_J{}^*| \le \Delta T$ is true. If not, the communication delay is greater than the maximum delay allowed by the system, and the authentication fails. Otherwise, the local computer will send $N_3$, $N_4$ to the smart wearable device. After receiving the parameters, the smart wearable device decrypts $N_3$ and $N_4$. Then, it is judged

Table 1: Parameters of the lightweight authentication.

| Symbol | Explanation |
|---|---|
| $t^*_R$ | The time when the smart wearable device first received a local computer message |
| $\Delta T$ | Maximum transmission delay allowed in the system |
| $t^*_T$ | The time when the local computer first received the smart wearable device |
| $t^*_r$ | The time when the blockchain node first received a local computer message |
| EPD | Pseudonyms for smart wearable devices |
| $\mathrm{hm}(X)$ | Represent the Hamming weight of binary string $X$ |
| $\mathrm{ROR}(X, Y)$ | $X$ and $Y$ are binary strings with a length of $L$ bits. Circulate the binary string $Y$ to the right to move $\mathrm{hm}(X)$ bits of the binary string $X$, then get the result of ROL ($X$, $Y$) |
| $ID$ | Identifier of smart wearable device |
| $K$ | Shared key value between smart wearable device and blockchain node |
| $\mathrm{hm}(Y)$ | Represent the Hamming weight of binary string $Y$ |
| $\mathrm{ROL}(X, Y)$ | $X$ and $Y$ are binary strings with a length of $L$ bits. Circulate the binary string $X$ to the right to move $\mathrm{hm}(Y)$ bits of the binary string $Y$, then get the result of ROL ($X$, $Y$) |

whether $z_1 = z_2$ is true while $z_1 = \mathrm{ROR}(N_3, y) \oplus K$, and $z_2 = \mathrm{ROR}(N_4, y) \oplus \mathrm{ID}$. If not, it indicates that the data is not credible, and the authentication stops. If $z_1 = z_2$, the smart wearable device authentication is passed, and the value $z = z_1$ or $z = z_2$ is assigned. Perform the following calculations: $\mathrm{EPD}_{\mathrm{next}} = \mathrm{ROL}(\mathrm{EPD} \oplus y, z)$ and $K_{\mathrm{next}} = \mathrm{ROL}(K \oplus z, y)$. Finally, the update and the identity authentication are finished.

*3.2.3. Searchable Encryption.* Relevant parameters in the section are shown in Table 2.

We first perform the formula $PAS(1^\alpha)$ which is just a probabilistic algorithm, and then we can get the key $K = (k_1, k_2)$ while $k_1 = \{0, 1\}^\alpha$ and $k_2 = \mathrm{PAS}(1^\alpha)$. If we want to query the search index $\gamma$ and search history $\sigma$, we need to create three empty hash linked lists $\gamma_f$, $\gamma_w$, $\gamma_d$ and an empty set $\sigma$ firstly. For any file $f \in \mathrm{f}$, the unique keyword set of $f$ is $\overline{f}$ and $f \supseteq \overline{f} = (w_1, \ldots\ldots, w_{\mathrm{lenth}(\overrightarrow{f})})$. Generate a string of pseudorandom sequences $s_1, \ldots\ldots, s_{\mathrm{lenth}(\overrightarrow{f})}$ through the pseudorandom number generator. Set $\tau_{w_i} = F_{k_1}(w_i)$ and $\widetilde{c_i} = H_{\tau_{w_i}}(s_i) \| s_i$ if $w_i \in \overline{f}$ and $1 \le \mathrm{i} \le \mathrm{lenth}(\overline{f})$. $\overline{c} = (\widetilde{c_1}, \ldots\ldots, \widetilde{c}_{\mathrm{lenth}(\overline{f})})$ is sorted by dictionary order and saved in $\gamma_f$. Then set $\gamma_f[\mathrm{ID}(f)] = \overline{c}$. Calculate the formula: $c = \mathrm{SKE.PAD}_{k_2}(f)$. For the keyword $w$ to be searched, calculate the search label: $\tau_w = F_{k_1}(w)$ and $\sigma' = \sigma \cup \{\tau_w\}$. Then, output the updated search history $\sigma'$ and search credentials $\tau_w$. First set $\gamma = (\gamma_f, \gamma_w, \gamma_d)$. Then figure out whether there is a key value related to $\tau_w$ in hash list $\gamma_w$, and whether there is key value related to $\tau_w$ in the hash chain table $\gamma_w$. If a key value is related to $\tau_w$ in the hash chain table $\gamma_w$, set $I_w = \gamma_w[\tau_w]$ and $\gamma_w^{'} = \gamma_w$. If not, generate an empty list $I_w$ for any $\overline{c} \in \gamma_w$.

For any $\widetilde{c_i} \in \overline{c}$, $1 \le i \le \mathrm{lenth}(\overline{c})$, set $\widetilde{c_i} = l_i \| r_i$, and verify whether $H_{\tau_w}(r_i) = l_i$ is true. If true, insert the file identifier $\mathrm{ID}(f)$ which is corresponding to $\overline{c}$ into $I_w$, and add $\tau_w$ to $\gamma_d[\mathrm{ID}(f)]$. Update $\gamma_w[\tau_w] = I_w$, and set updated indexes as $\gamma\prime_w$ and $\gamma\prime_d$. We get $I_w$ and $\gamma' = (\gamma_f, \gamma'_w, \gamma'_d)$ at last. For the file $f$ to be added and its unique keyword set $\overline{f}$, a series of pseudorandom sequences $\mathrm{s}_1, \ldots\ldots, s_{\mathrm{lenth}(\overline{f})}$ is generated by the pseudorandom number generator. Create an empty list $X$, for any $w_i \in \overline{f}$, $1 \le i \le \mathrm{lenth}(\overline{f})$. Calculate the formula below.

$$\tau_{w_i} = F_k(w_i). \tag{3}$$

If $\tau_{w_i} \in \sigma$, it means this keyword has been searched. Insert $\tau_{w_i}$ into list $X$, and its formula can be expressed as follows:

$$\widetilde{c}_i = H\tau_{w_i}(s_i) \| s_i, \tag{4}$$

$\overline{c} = (\widetilde{c_1}, \ldots\ldots, \widetilde{c}_{\mathrm{lenth}(\overline{f})})$ is sorted by dictionary order which means $\overline{c} = \mathrm{SKE.Enc}_{k_2}(f)$. While $\tau_\alpha = (\mathrm{ID}(f), \overline{c}, c, X)$ and $\gamma = (\gamma_f, \gamma_w, \gamma_d)$, add $\gamma_f[\mathrm{ID}(f)] = \overline{c}$ to the index $\gamma_f$, for any $x_i \in X$, and $ID(f)$ is added to $\gamma_w[x_i]$. Then set $\gamma_d[\mathrm{ID}(f)] = X$. The updated index is $\gamma'_f, \gamma'_w, \gamma'_d$. Add $c$ to c. The updated ciphertext collection is marked as $c'$ and then $(c', \gamma')$ will be output where $\gamma' = (\gamma_f, \gamma'_w, \gamma'_d)$. When we want to decrypt the file ciphertext $c$, we input the key, and then we get the decrypted file; the formula can be expressed as follows: $f = \mathrm{SKE.DSF}_{k_2}(c)$.

## 4. Experiment and Analysis

In this section, we discussed the performance of our scheme and analyzed the results of simulated experiments. We tested and compared the performance efficiency and storage cost of the lightweight authentication with others. We also compared our lightweight searchable encryption with others.

We compared Fabric with Corda, FISCO BCOS, and Quorum. The result is shown in Table 3. Considering that our scheme is oriented to mobile medical, we chose "Fabric" as our blockchain framework in the end.

Hyperledger Fabric is managed by the Linux Foundation, hoping to change the single common network mode of the public chain. By establishing multiple interconnected blockchain networks to cover all kinds of different business scenarios, it realizes the flexibility of design, meets the diversified requirements, and realizes the interaction between networks. This idea is reflected in its unique channel mechanism design. Hyperledger Fabric aims to build an open source framework for general blockchain regardless of industry and has the largest consensus in the consortium chain. FISCO BCOS originates from the enterprise blockchain platform BCOS. As a branch of the financial version, it pays more attention to the financial industry while retaining its universality and takes more account of the particularity of regulators. It is applicable to a wide range of distributed

Table 2: Parameters of the searchable encryption.

| Symbol | Explanation |
|---|---|
| $\{0,1\}$ | Binary sequence with length $n$ |
| $\{0,1\}$ | Binary sequence of arbitrary length |
| $\text{len}(u)$ | Bit length of binary sequence $u$ |
| $u\|\|v$ | Connection of binary sequences $u$ and $v$ |
| $z \leftarrow A$ | $Z$ is the output of probabilistic algorithm $A$ |
| $\alpha$ | Security parameters |
| SKE (PAS, PAD, DSF) | Symmetric encryption scheme against indistinguishable selective plaintext attack |

Table 3: Comparison of blockchain platform.

| Name | Data model | Consensus mechanism | Smart contract | Database |
|---|---|---|---|---|
| Fabric | Account based | Solo/Kafka/PBFT | Go/Node.js/Java | LevelDB/CouchDB |
| BCOS | Account based | Raft/PBFT | Solidity | Level DB |
| Corda | Transaction based | Notary | Java/Kotlin | Relational database |
| Quorum | Account based | Raft/PBFT | Solidity | Level DB |

business scenarios. Corda is aimed at the financial industry and clearly stated that it will not consider other industries for at least a certain period of time. Corda hopes to provide a global logical account with uniqueness and authority that can record all the agreements between enterprises. The core is to achieve a noncentral database with the minimum trust mechanism between nodes. Corda advocates fully considering the combination with the existing business system rather than dismantling the existing business system. Quorum is an alliance chain scheme, an enterprise-level distributed ledger, and intelligent contract platform developed by JPMorgan. It is developed on the basis of Ethereum, providing private intelligent contract execution scheme and meeting the performance requirements of the enterprise, applicable to scenarios requiring high-speed transactions and private transactions between high-throughput processing alliances, designed primarily to address the special challenges of blockchain applications in finance and other industries.

In the current medical industry, we need to build licensed blockchains, such as hospitals, which need to operate under strict regulatory requirements, and cannot let unknown users view transaction data. In addition, medical information is very important, so unauthorized viewing will leak patient information in the future. At the same time, Fabric is a framework that requires prior permission. All participants have known identities and are verified according to the organization's identity management system. There are no anonymous or pseudonymous users.

As a result, we chose Fabric finally.

We analyzed the security and privacy of our proposed scheme. The details are as follows. The specific experimental environment is shown in Table 4.

### 4.1. Test

*4.1.1. Lightweight Authentication.* In this section, the performances of mobile medical devices are compared with classical authentication schemes.

Table 4: The experimental environment.

| CPU | AMD Ryzen 5900x |
|---|---|
| GPU | NVIDIA GeForce GTX 2080Ti |
| Memory of single pc | 16G |
| Blockchain architecture | Fabric 2.0 |
| System version | Ubuntu 18.04 |
| Database | MySQL 8.0 |

Assume that the length of communication, traffic, and storage parameters are the same. There are four kinds of information, that is, IDS, ID, K, and $\Delta$K saved in mobile terminal devices in the medical system. In our scheme, there are 14 session messages in a complete session. At the same time, there are 14 session messages in [24] and 10 session messages in [25]. Reference [26] has 16 session messages. Reference [27] and reference [28] have 10 messages. Therefore, the communication traffic size is 14 in our scheme. It can be seen from Figure 2 that our scheme can reduce the computing burden.

From the point of view of the computing burden, our scheme and the scheme in [28] are both ultralightweight. The algorithms used in other comparative references are all lightweight, so the scheme in this paper has great advantages in reducing the calculation time. The result is shown in Table 5.

In the scheme of [28], the computation of shared secret key and pseudonym updating is more complex, which increases the number of CMO operations, so the overall calculation cost is higher than our scheme. In our scheme, the steps of calculation are as follows. Firstly, we generate a random number $x\,(\Delta y/\Delta x)$ to operate RAN. Secondly, in the process of calculating messages $N_1$ and $N_2$, we perform CMO operations on $N_1$ and $N_2$, respectively. Thirdly, the third and fourth CMO operations and the first and second DIG operations are needed to decrypt messages $N_3$ and $N_4$. Lastly, we perform the last two CMO operations to update the shared secret values and pseudonyms. Therefore, the total computing burden in our scheme is 6CMO + 2DIG + 1RAN.

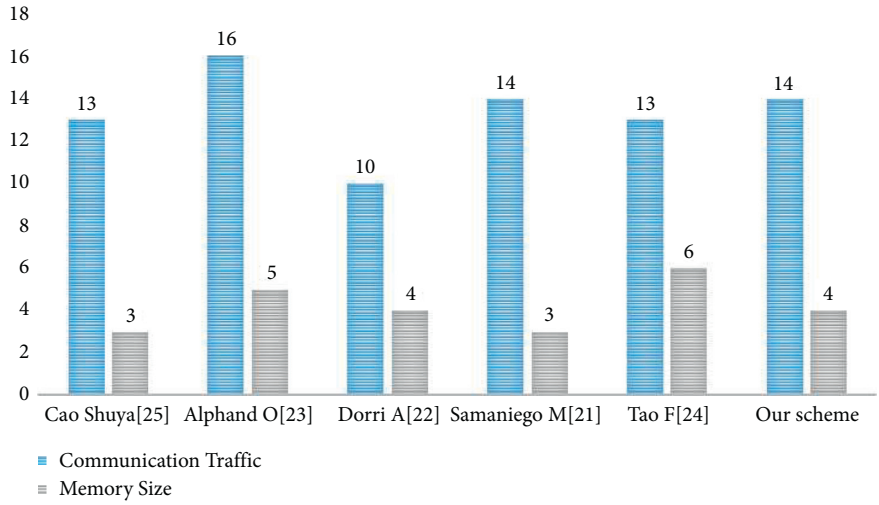


Figure 2: Comparison of communication.

Table 5: Performance comparison of different schemes.

| Symbol | Explanation |
|---|---|
| Reference [24] | 5PUF + 5DIG + 1RAN |
| Reference [25] | 7MOD + 2DIG + 2RAN |
| Reference [26] | 6HASH + 3DIG + 1RAN |
| Reference [27] | 7PRNF + 4DIG + 2RAN |
| Reference [28] | 11CMO + 4DIG + 1RAN |
| Our scheme | 6CMO + 2DIG + 1RAN |

Symbols of lightweight authentication are shown in Table 6.

*4.1.2. Searchable Encryption.* The performances of our scheme are compared with other references, and the results are shown in Table 7.

Our scheme gradually builds indexes in the search process. At the beginning, maintain a regular index $\gamma_f$ and store the encrypted keywords for each file. Once a keyword $w$ is retrieved, the identifier of all the files containing the keyword is moved into a reverse index $\gamma_w$, and a delete index $\gamma_d$ is constructed to store the keywords that have been searched for in the files appearing in $\gamma_w$. A search history is maintained at the client to record which keywords have been searched. The searched keywords can directly query the index $\gamma_w$ to obtain the search results. This disperses the time and storage cost of building index tables into each search process, saving search time.

Descriptions of the relevant symbols are as shown in Table 8.

The biggest improvement of our scheme compared with scheme [33] is the deletion of index $\gamma_d$, which reduces the execution time of deletion operation to a certain extent. We mainly compare the deletion operations of the two schemes.

For each file deleted in the scheme of [33], traverse each item in $\gamma_w$ and find each node in $\gamma_w[\tau_{w_i}]$ one by one until the identifier of the deleted file is found or the end node is reached. In this scheme, delete index $\gamma_d$ is used. When deleting a file, read $\gamma_d[\mathrm{ID}(f)]$ directly. For any $x_i$ in $\gamma_d[\mathrm{ID}(f)]$, only find each node in the list of $\gamma_w[x_i]$ in $\gamma_w$ until finding the identifier of the deleted file.

We select 51 English documents. First, we convert all uppercase to lowercase, remove all punctuation, and separate words only with space. According to statistics, there are 3711262 words in 51 documents, removing duplicate words in each document, leaving a total of 373221 unique words. We search for 5000 words; that is, there are 5000 input items in the search index $\gamma_w$, 51 documents are searched, and 51 input items in the index $\gamma_d$ are deleted. We delete five files, respectively, and give the traversal times and time consumption of the two schemes when deleting files, as shown in Table 9. The traversal times are the comparison times of nodes in the list in tables $\gamma_w$ and $\gamma_d$ when deleting files. The result is shown in the following table.

*4.1.3. Blockchain.* Due to the dependence and mobility on massive data, the performance index of blockchain is quite important, which includes latency, energy consumption, throughput, and scalability.

In our experiment, we used the Caliper to test the performance. Caliper is a blockchain performance testing framework that currently supports testing for processing traffic (TPS), latency, and resource utilization. After each round of test, users can obtain a series of test results and reports by Caliper. The result is shown in Figure 3.

As shown in Figure 4, the throughout increased steadily with the increase of transaction times. It reached the peak when the transaction times reached 5000, the throughput is

Table 6: Parameter values.

| Symbol | Explanation |
|---|---|
| PUF | Computation amount of physical unclonable function |
| DIG | Computation amount of physical unclonable function |
| RAN | The amount of calculation to generate random numbers |
| MOD | Modular calculation amount |
| HASH | Calculation amount of hash function |
| PRNF | The amount of calculation to generate a pseudorandom function |
| CMO | Calculation amount of circular movement operation |

Table 7: Parameter values.

| Literature | Search time | Index space | Update leak | Update cost |
|---|---|---|---|---|
| Literature [29] | $O(m/n)$ | $O(m+n)$ | $ID(w)$ | $O(m+n)$ |
| Literature [30] | $O(\log\|f\|\bullet m/n)$ | $O(\|f\|\bullet n)$ | | $O(\log\|f\|\bullet m/n)$ |
| Literature [31] | $O(m/n)$ | $O(m+n)$ | | $O(m+n)$ |
| Literature [32] | $O(m/n)$ | $O(m+n)$ | $ID(w)$ | $O(m+n)$ |
| Literature [33] | $O(m/n)$ | $O(m+n)$ | | $O(m+n)$ |
| Our scheme | $O(m/n)$ | $O(m+n)$ | | $O(m+n)$ |

Table 8: Parameter values.

| Symbol | Explanation |
|---|---|
| $n$ | The total number of unique keywords |
| $m$ | The total number of all keywords |
| $ID(w)$ | Fixed identifier for the keyword |
| $\|f\|$ | Total number of files |

Table 9: Comparison of our scheme and scheme of [33].

| Document | | $f_1$ | $f_2$ | $f_{20}$ | $f_{40}$ | $f_{51}$ |
|---|---|---|---|---|---|---|
| Scheme [33] | Number of traversals | 34656 | 32474 | 39447 | 32495 | 47693 |
| | Time (ms) | 4.7 | 2.8 | 1.9 | 5.1 | 1.1 |
| Our scheme | Number of traversals | 25160 | 17919 | 15734 | 11353 | 7 |
| | Time (ms) | 3.2 | 1.8 | 1.7 | 1.9 | 0.01 |

296.4TPS, and the average latency is 215.4 ms. Then it began to decline slowly when the transactions times exceed 5000. At present, there is no national standard for blockchain performance indicators, and China Institute of Information and Communications is actively formulating it. According to the existing blockchain industry standards (Table 10), the performance of our system meets the requirements.

### 4.2. Security

(1) In design of the authentication scheme, the pseudonym of a smart wearable device is introduced, which is transferred during each communication, and the pseudonym is updated after each communication, so that the pseudonym of each round is different. Additionally, other private information that needs to be sent is encrypted before it can be sent, which makes it impossible for attackers to obtain useful and valid information. Therefore, attackers cannot learn the real identity information of a smart wearable device user. Hence, this scheme can provide the anonymity of entities. At the same time, our scheme uses the method of mixing random numbers in the message encryption. The random number is randomly generated by the system, and it is unpredictable and inconsistent. Therefore, the attacker cannot analyze the value of the next round of communication messages by intercepting the current message or deduce the user's privacy information in the previous round of communication messages, which makes the scheme more secure.

(2) In process of anonymous certificate generation, TCA is visible to the content of the certificate but invisible to the user's identity, while regulators are visible to the user's identity but invisible to the content of the certificate, which enhances the anonymity of the user. In addition, in the process of tracking the user's real identity, TCA and regulators need to provide their own key information, which reduce the threat of unilateral dishonesty and single point attack on the security of anonymous certificates. In our scheme, we disclose specific information to the server during the operations of query and update. Next, we use the following leak functions $L_{\text{search}}$, $L_{\text{add}}$, $L_{\text{delete}}$, $L_{\text{encrypt}}$ to give the leaked information.

In our scheme,

$$L_{\text{search}}(f,w) = \left(ACCP_t(w), ID(w)\right), \tag{5}$$

$$L_{\text{delete}}(f,w) = \left(\text{ID}(f), \text{SRCH\_HIS}(\overline{f})\right), \tag{6}$$

$$L_{\text{encrpt}(f)} = \text{length}(f), \tag{7}$$

$$L_{\text{add}}(f,f) = \left(\text{ID}(f), \text{lenth}(\overline{f}), \text{SRCH\_HIS}(\overline{f})\right). \tag{8}$$

According to the above leak functions, except the access model, our scheme does not disclose more information to the server. The relevant parameters are shown in Table 11.

###test result:###

| Name | Succ | Fail | Send Rate (TPS) | Max Latency (s) | Min Latency (s) | Avg Latency (s) | Throughput (TPS) | Avg Response (s) |
|---|---|---|---|---|---|---|---|---|
| writeAsset | 11719 | 0 | 275.3 | 2.11 | 0.06 | 0.48 | 256.1 | 0.48 |

### resource stats ###

| Name | CPU% (max) | CPU% (avg) | Memory (max) [MB] | Memory (avg) [MB] | Traffic In [MB] | Traffic Out [MB] | Disc Write [MB] | Disc Read [MB] |
|---|---|---|---|---|---|---|---|---|
| dev-peer1.org2.fabComm... | 2.55 | 1.89 | 9.13 | 9.11 | 8.91 | 2.63 | 0.00 | 0.00 |
| dev-peer0.org1.fabComm... | 2.95 | 1.93 | 11.2 | 11.2 | 9.02 | 2.66 | 0.00 | 0.00 |
| dev-peer0.org2.fabComm... | 0.00 | 0.00 | 10.1 | 10.1 | 0.000479 | 0.000542 | 0.00 | 0.00 |
| cli | 0.00 | 0.00 | 7.35 | 7.35 | 0.00 | 0.00 | 0.00 | 0.00 |
| peer0.org2.fabComm.com | 14.23 | 7.93 | 342 | 315 | 34.2 | 0.484 | 102 | 0.00 |
| orderer.fabComm.com | 10.19 | 7.44 | 120 | 104 | 36.6 | 69.9 | 70.2 | 0.00 |
| peer0.org1.fabComm.com | 21.10 | 16.10 | 332 | 312 | 45.1 | 20.2 | 102 | 0.00 |
| peer1.org2.fabComm.com | 20.30 | 15.29 | 321 | 295 | 44.8 | 50.3 | 102 | 0.00 |
| peer1.org1.fabComm.com | 12.76 | 9.02 | 334 | 311 | 34.4 | 37.9 | 102 | 0.00 |

Figure 3: One round of test.

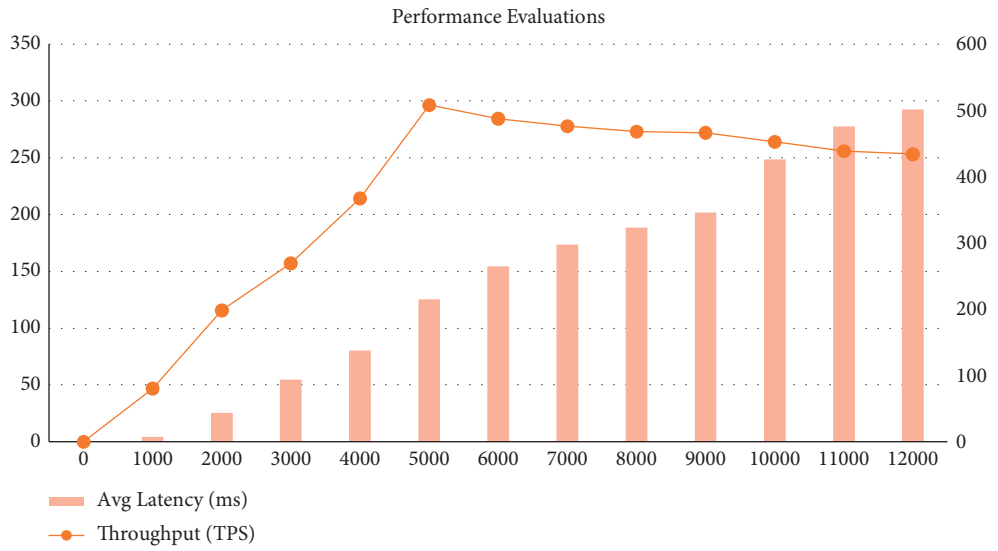


Figure 4: Performance evaluations.

Table 10: Blockchain industry standards.

| Name | Requirement cost |
|---|---|
| Success | Rate >95% |
| Average | Response time <0.5 s |
| Average latency | <1 s |
| Throughput (TPS) | 200–300 |
| Success rate | >95% |

Table 11: Symbols of leak functions.

| Symbol | Explanation |
|---|---|
| $\mathrm{ACCP}_t(w)$ | Access pattern, the file identifier of the file in $f_w$ when the keyword $w$ is queried at time $t$, that is, the set $\{ID(f_i)\colon w \in f_i, f_i \in f\}$ |
| $\overline{f}$ | Unique keyword set of files $f$ |
| $\mathrm{SRCH\_HIS}(\overline{f})$ | The set of identifier $ID(w)$ of keywords that have been searched in time $t$ file $f$, that is, the set $\mathrm{SRCH\_HIS}(\overline{f}) = \{\mathrm{ID}(w_i)\colon w_i \in f, \tau_{w_i} \in \sigma\}$ |

## 5. Conclusion

As an intelligent product at this stage, mobile intelligent terminal integrates the existing information system of the hospital through mobile Internet technology, shares and exchanges clinical business data, and provides a new way of diagnosis and treatment for the hospital. To solve the problem of privacy leakage of medical patients, we design a privacy preservation scheme based on mobile terminals in Internet medical by combining privilege separation, authentication scheme, lightweight loop operation, and improved searchable encryption algorithm in the model system, and we conducted a comparative experiment on data from different systems. Compared with the original anonymous authentication system, we separate the regulator and TCA authority and improve the efficiency of certificate generation by 34.8% compared with the scheme. The results show that the model trained by our scheme has less calculation burden, better stability, and higher security. Further works are as follows.

(1) To improve the efficiency of searchable encryption.

(2) To expand the diversified search functions. Except the basic search function, we also need to support some special functions, such as approximate search, wildcard search, fuzzy search, multikeyword search, and so on. Increasing the diversity of search functions is an important research direction in the future.

## Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## References

[1] D. M. West, *Improving health care through mobile medical devices and sensors*, Brookings Institution Policy Report, vol. 10, , pp. 1–13, 2013.

[2] Y. Huang, H. Xue, H. Gao, X. Ma, and W. Hussain, "SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.

[3] H. Gao, W. Huang, and Y. Duan, "The cloud-edge-based dynamic reconfiguration to service workflow for mobile ecommerce environments," *ACM Transactions on Internet Technology*, vol. 21, no. 1, pp. 1–23, 2021.

[4] X. Yang, S. Zhou, M. Cao, and Applications, "An approach to alleviate the Sparsity problem of hybrid collaborative filtering based recommendations: the product-attribute perspective from user reviews," *Mobile Networks and Applications*, vol. 25, no. 2, 2020.

[5] S. Deng, Z. Xiang, J. Taheri et al., "Optimal Application Deployment in Resource Constrained Distributed Edges," *IEEE Transactions on Mobile Computing*, vol. 99, p. 11, 2020.

[6] J. Xiao, H. Xu, H. Gao, M. Bian, and Y. Li, "A weakly supervised Semantic Segmentation network by aggregating seed cues: the multi-object proposal generation perspective," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 1s, pp. 1–19, 2021.

[7] M. R. Patra, R. K. Das, and R. P. Padhy, "CRHIS: cloud based rural healthcare information system," in *Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance*, pp. 402–405, New York, NY, United States, 2012.

[8] N. Ye, Y. Zhu, R.-c. Wang, R. Malekian, and Q.-m. Lin, "An efficient authentication and access control scheme for perception layer of internet of things," *Applied Mathematics & Information Sciences*, vol. 8, no. 4, 2014.

[9] G. Zyskind, O. Nathan, and A. S. Pentland, "privacy: using blockchain to protect personal data," in *Proceedings of the EEE Security & Privacy Workshops*, p. 180 184, San Jose, CA, USA, May 2015.

[10] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: using blockchain for medical data access and permission management," in *Proceedings of the International Conference on Open & Big Data*, Vienna, Austria, August 2016.

[11] A. A. Omar, M. S. Rahman, A. Basu, and S. K. MediBchain, "A blockchain based privacy preserving platform for healthcare data," in *Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, Zhangjiajie, China, November 2017.

[12] H. G. Do and W. K. Ng, "Blockchain-based system for secure data storage with private keyword search," in *Proceedings of the IEEE World Congress on Services (SERVICES)*, pp. 90–93, Honolulu, HI, USA, May 2017.

[13] G. B. Magyar, "Solving the Privacy and Research Availability Tradeoff for EHR Data," in *Proceedings of the A New Disruptive Technology in Health Data Management*, pp. 000135–000140, IEEE 30th Neumann Colloquium, Budapest, Hungary.

[14] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 7, pp. 130–137, 2018.

[15] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *Proceedings of theThe 28th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1–5, IEEE PIMRC, Montreal QC Canada, June 2017.

[16] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of Medical Systems*, vol. 42, no. 8, p. 140, 2018.

[17] Y. Ji, J. Zhang, J. Ma, C. Yang, and X. Yao, "BMPLS: blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–13, 2018.

[18] Q. Wang, D. Zhou, S. Yang, P. Li, and Q. Guan, "Privacy preserving computations over healthcare data," in *Proceedings of the International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data*, pp. 635–64, SmartData, Atlanta, GA, USA, July 2019.

[19] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, pp. 218–8, 2016.

[20] H. Tian, J. He, and Y. Ding, "Medical data management on blockchain with privacy," *Journal of Medical Systems*, vol. 43, no. 2, p. 26, 2019.

[21] S. Gao, Q. Wang, Y. Liu, Z. Liu, W Ou, and W. Han, "A Privacy-Preservation Scheme Based on Mobile Terminals in Internet Medical," *ResearchGate. Preprint*, 2021.

[22] S. A. Chaudhry, A. Irshad, J. Nebhen et al., "An anonymous device to device access control based on secure certificate for internet of medical things systems," *Sustainable Cities and Society*, vol. 75, no. 1, Article ID 103322, 2021.

[23] A. Arasan, R. Sadaiyandi, F. Al-Turjman, A. k. Rajasekaran, and K. S. Karuppuswamy, "Computationally efficient and secure anonymous authentication scheme for cloud users," *Personal and Ubiquitous Computing*, pp. 1–11, 2021.

[24] M. Samaniego, R. Deters, and U Jamsrandorj, "Blockchain as a Service for IoT," in *Proceedings of the Blockchain as a service for IoT. in IEEE International*, pp. 433–436, Chengdu, China, December 2016.

[25] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized BlockChain for IoT," in *Proceedings of the The Second IEEE/ACM Conference on Internet of Things Design and Implementation*, pp. 173–178, Pittsburgh, PA, USA, April 2017.

[26] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, and F. Z. IoTChain, "A blockchain security architecture for the internet of things," in *Proceedings of the IEEE Wireless Communications and Networking Conference*, pp. 1–6, WCNC, Barcelona, Spain, April 2018.

[27] F. Tao, D. Zhao, Y. Hu, and Z. Zhou, "Resource service composition and its optimal-selection based on particle swarm optimization in manufacturing grid system," *IEEE Transactions on Industrial Informatics*, vol. 4, no. 4, pp. 315–327, 2008.

[28] Y. Y. Cao Shuya, "Chang Xiaolin, Lightweight secure authentication scheme using blockchain for RFID system in smart factory," *Cyberspace Security*, vol. 11, no. 9, p. 10, 2020.

[29] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic Searchable Symmetric Encryption," in *Proceedings of the ACM Transactions on Internet Technology*, p. 965, Raleigh North Carolina USA, October 2012.

[30] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable Symmetric encryption," in *Proceedings of the International Conference on Financial Cryptograph & Data Security*, pp. 258–274, Okinawa, Japan, April 2013.

[31] D. Cash, J. Jaeger, S. Jarecki et al., "Dynamic searchable encryption in very-large databases: data structures and implementation," *Network & Distributed System Security Symposium*, 2014.

[32] M. Naveed, M. Prabhakaran, and C. A. Gunter, "Dynamic searchable encryption via blind storage," in *Proceedings of the IEEE Symposium on Security & Privacy*, pp. 639–654, Berkeley, CA, USA, May 2014.

[33] F. Hahn and F. Kerschbaum, "Searchable Encryption with Secure and Efficient Updates," in *Proceedings of the ACM Transactions on Internet Technology*, pp. 310–320, Raleigh North Carolina USA, October 2014.