A Privacy-Preservation Scheme based on Mobile Terminals in Internet Medical

Shuo Gao

Hainan University

Qichao Wang

Hainan University

Yihan Liu

Hainan University

Zekai Liu

Hainan University

Wei Ou (✉ ouwei@hainanu.edu.cn)

Hainan University

Wenbao Han

Hainan University

Research Article

Keywords: Internet Medical, Mobile Terminal, Privacy Preservation, Lightweight Authentication, Blockchain, Searchable Encryption

Posted Date: March 15th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-288792/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

A Privacy-Preservation Scheme based on Mobile Terminals in Internet Medical

Shuo Gao¹, Qichao Wang¹, Yihan Liu¹, Zekai Liu¹, Wei Ou^{1*}, and Wenbao Han¹

¹ School of Computer Science and Cyberspace Security, Hainan University, 570228, Haikou, China

*Correspondence should be addressed to Wei Ou: ouwei@hainanu.edu.cn

Abstract

Since the 21st century, Internet technologies have entered a stage of rapid developments, and gradually been widely used in various industries. Internet Medical is gradually matured and used widely. Aiming at the problems such as the easy leakage of privacy in mobile medical equipment and untrustworthy data, we make use of a role-separated mechanism to generate trusted anonymous certificates and propose a lightweight identity authentication scheme to protect the medical data security. It reduces the calculation cost. Meanwhile, in view of problems of transparency and visibility of blockchain information, we adapt searchable encryption algorithm to realize ciphertext processing in the whole life cycle. Experiments show that our scheme can reduce the cost of computation on basis of ensuring traffic. In process of dynamic updating of ciphertext keywords, except the keyword identifier, less information is leaked to the server, which protect users' privacy.

Keywords: Internet Medical, Mobile Terminal, Privacy Preservation, Lightweight Authentication, Blockchain, Searchable Encryption

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 population. 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.

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 medical 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) are 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 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. 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 and other private information.

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 scheme 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.

Related Works

For the storage and transmission of medical data, scholars around the world have conducted a lot of researches. In 2012, Patra [2] et al. 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 2015, Guy Zyskind [3] et al. 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: T_{data} for data storage and recovery and access time T_{access} 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 T_{data} transactions. Witchey N proposed the use of a medical transaction ticket to

verify the medical blockchain system, but there is still a problem of privacy leakage.

In 2016, to solve the problems of slow medical record information access, data fragmentation, and user privacy-preservation, Azaria [4] et al. 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. Though this solution realizes the sharing of medical data, it lacks a universal access control strategy.

In 2017, Al Omar et al. [5] proposed a data management system for patient health care. By adopting blockchain to protect privacy storage, it solved 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.

In 2018, Gabor Magyar [6] 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, Kristen N. Griggs [7] et al. 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.

In 2014, Ye [8] et al. proposed a well-organized authentication and access control scheme based on the attributes of the perceived IoT access control layer.

In 2017, Hoang Giang Do [9] et al. proposed a system that uses blockchain technology to provide secure distributed data storage with keyword search services.

In 2018, Liang [10] et al. 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 [11] et al. 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 well. Privacy. However, using two types of blockchains will not only increase costs, but also reduce their execution efficiency. Yaxian Ji [12] et al. investigated the location sharing based on blockchains for telecare medical information systems. Firstly, they define the basic requirements of blockchain-based location sharing including decentralization, unforgeability, confidentiality, multi-level privacy preservation, retrievability and verifiability. Then, using order-preserving encryption and Merkle tree, they proposed a blockchain-based multi-level location sharing scheme, i.e. BMPLS.

In 2019, Qi Wang [13] et al. combined homomorphic encryption and proxy re-encryption 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 analyse data to provide better services. The HGD architecture based on blockchain proposed by Yue [14] et al. enables patients to safely control and share medical data. Aiming at the privacy of medical data, Tian [15]

et al. proposed to establish a shared key that can be reconstructed by legitimate parties before the diagnosis and treatment process begins.

Scheme

Structure

Fig.1 The System Structure

In our system, the local computer of the mobile medical model generates 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 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.

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. Complete the 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.

To ensure the privacy of users' medical and health data, the data on the chain is encrypted. To solve operations such as searching for encrypted data, we use searchable encryption technology. If other users need to encrypt data, they can query the data through the blockchain network.

Module

Anonymous Certificate Generation

The steps to generate an anonymous certificate are as follows.

Step 1: A user submits the real-name certificate application and his real identity information to the CA. After the CA verifies, the real-name certificate E_{cert}

will be issued for the user and saved in the CA database.

Step 2: User U generates his own anonymous identity AID , public and private key pair (APK, ASK) , random numbers p , r_1 , and calculates the serial number of the anonymous certificate: $SN = H(APK, p)$; generate anonymous certificate header $b = (AID, SN, APK)$; Anonymous certificate content $M = (b, h(E_{cert}))$; Calculate the formula $u = g^{r_1}$. Then, the user sends u and the real-name public key signature $Sig_{PK}(u)$ to the supervisor Admin.

Step 3: Admin verifies the signature information sent by the user. After the verification is passed, calculate the formula $w = u^{d_1}$ and send w to user U , which will be saved in the supervisor database in the form of key-value pairs $\langle E_{d_1}(u) : ID \rangle$.

Step 4: After the user accepts w , he uses ASK to perform signature calculation on M which is $Sig_{ASK}(M)$, and send random numbers r_1 and w to TCA .

Step 5: TCA verifies the parameters sent by the user, and after the verification passes, calculate the formula below $z = w^{d_2}$. Then judge whether $Q = z g_1^{-1}$ is true, if $Q = z g_1^{-1}$, save $\langle SN : E_{d_2}(z) \rangle$ in the TCA

database in the form of key-value pairs. Then generate a random number r_2 , calculate the joint signature:

$$U_{Sigd} = (g^{r_2}, (h^{-1}(M) + g^{r_2 * d_1 * d_2}) g_2^{-1}) \quad (13)$$

and send it to the user, User U gets the anonymous certificate (M, U_{Sigd}) in the end.

Lightweight Authentication

Table.1 Symbols of Lightweight Authentication.

Symbol	Explanation
t_R^*	The time when the smart wearable device first received a local computer message.
t_T^*	The time when the local computer first received the smart wearable device.
t_J^*	The time when the local computer first received the blockchain node message.
t_r^*	The time when the blockchain node first received a local computer message.
ΔTY	Maximum transmission delay allowed in the system.
EPD	Pseudonyms for smart wearable devices.
EPD_{next}	Next-round communication pseudonyms for smart wearable devices.
ID	Identifier of smart wearable device.
K	Shared key value between smart wearable device and blockchain node.
K_{next}	The next round of communication between the smart wearable device and the blockchain node shares the key value.
$ROL(X, Y)$	X and Y are binary strings with a length of L bits, hm(X) and hm(Y) respectively represent binary strings X, hamming weight of binary string Y, circulate the binary string X to the right to move the Hamming weight hm(Y) bits of the binary string Y, you can get the result of ROL (X, Y).
$ROR(X, Y)$	X and Y are binary strings with a length of L bits, hm(X) and hm(Y) respectively represent binary strings X, hamming weight of binary string Y, circulate the binary string Y to the right to move the Hamming weight hm(X) bits of the binary string X, you can get the result of ROL (X, Y).

The steps required for lightweight authentication are as follows.

Step 1: The local computer generates a random number x and a timestamp t_R , and sends x and t_R to the smart wearable device. After the smart wearable device receives the parameters, it first calculates whether $|t_R - t_R^*| \leq \Delta T$ is true. If $|t_R - t_R^*| > \Delta T$, it means that the communication delay is greater than the maximum delay allowed by the system, and the authentication stops. If $|t_R - t_R^*| \leq \Delta T$, the smart wearable device generates a random number y and a

timestamp t_T , and performs the following calculations based on the devices ID and K :

$$N_1 = ROL(K \oplus y, x) \quad (1)$$

$$N_2 = ROL(ID \oplus y, x) \quad (2)$$

Step 2: The smart wearable device feeds N_1, N_2, EPD, t_r, x to the local computer. After the local computer receives the parameters, it first calculates whether $|t_T - t_T^*| \leq \Delta T$ is true. If $|t_T - t_T^*| > \Delta T$, it means that the communication delay is greater than the maximum delay allowed by the system, and the authentication stops. If $|t_T - t_T^*| \leq \Delta T$, the local

computer generates a timestamp and sends N_1, N_2, EPD, t_r and x to the blockchain node.

Step 3: After the blockchain node receives the parameters, it first calculates whether $|t_r - t_r^*| \leq \Delta T$ is true. If $|t_r - t_r^*| > \Delta T$, it means that the communication delay is greater than the maximum delay allowed by the system, and the authentication stops. If $|t_r - t_r^*| \leq \Delta T$, the blockchain node starts to search for data that matches EPD . If there is no matching data, it indicates that the data is not credible, and the authentication stops. If there is matching data, then obtain the matching ID and K for decryption Operation:

$$y_1 = \text{ROR}(N_1, x) \oplus K \quad (3)$$

$$y_2 = \text{ROR}(N_2, x) \oplus ID \quad (4)$$

Then, it is judged whether $y_1 = y_2$ or not. If $y_1 \neq y_2$, it indicates that the data is not credible, and the authentication is stopped. If $y_1 = y_2$, pass the blockchain node authentication and assign $y = y_1 = y_2$.

Step 4: The blockchain node generates a random number z and a timestamp t_J to perform the following calculations:

$$N_3 = \text{ROL}(K \oplus z, y) \quad (5)$$

$$N_4 = \text{ROL}(ID \oplus z, y) \quad (6)$$

Then, perform the following calculation:

$$EPD_{\text{next}} = \text{ROL}(EPD \oplus y, z) \quad (7)$$

$$K_{\text{next}} = \text{ROL}(K \oplus z, y) \quad (8)$$

Step 5: The blockchain node sends N_3, N_4, t_J to the local computer. After the local computer receives the parameters, it first calculates whether $|t_J - t_J^*| \leq \Delta T$ is true. If $|t_J - t_J^*| > \Delta T$, it means that the communication delay is greater than the maximum delay allowed by the system, and the authentication stops. If $|t_J - t_J^*| \leq \Delta T$, 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 .

$$z_1 = \text{ROR}(N_3, y) \oplus K \quad (9)$$

$$z_2 = \text{ROR}(N_4, y) \oplus ID \quad (10)$$

Then, it is judged whether $z_1 = z_2$ is true. If $z_1 \neq z_2$, it indicates that the data is not credible, and the authentication is stopped. If $z_1 = z_2$, the smart wearable device authentication is passed, and the value $z = z_1$ or $z = z_2$ is assigned.

Then, perform the following calculation:

$$EPD_{\text{next}} = \text{ROL}(EPD \oplus y, z) \quad (11)$$

$$K_{\text{next}} = \text{ROL}(K \oplus z, y) \quad (12)$$

Finally, the update and the identity authentication are finished.

Searchable Encryption

Table. 2 Symbols of Searchable Encryption

Symbol	Explanation
$PAS(1^\alpha) \rightarrow K$	A probability algorithm, input security parameter λ , output key K .
$PAD(K, f) \rightarrow (\gamma, \sigma, \bar{c})$	A probability algorithm, input key K and file set f , output encrypted file set c , search index γ and search history σ .
$PSek(K, w, \sigma) \rightarrow (\sigma', \tau_w)$	A possible probability algorithm, input key K , keyword w and search history σ , output updated search history σ' and search credentials τ_w .
$Sek(\tau_w) \rightarrow (I_w, \gamma')$	A certain algorithm, input search credentials τ_w , file ciphertext collection c and search index γ , output file identifier set I_w and updated search index γ' .
$PAT(K, f, \sigma) \rightarrow \tau_a$	A possible probability algorithm, input key K , file f and search history σ , output add credentials.
$AD(\tau_a, c, \bar{c}, \gamma) \rightarrow (\bar{c}', \gamma')$	A certain algorithm enters an add credential, an encrypted file c , encrypt the file set c and the search index γ , and output the updated ciphertext set c' and the updated search index γ' .
$Dlt(ID(f), \bar{c}, \gamma) \rightarrow (\bar{c}', \gamma')$	A certain algorithm input a file identifier $ID(f)$, encrypted file set c and search index γ , output the updated ciphertext set c' and the updated search index γ' .
$DSF(K, c) \rightarrow f$	A certain algorithm, input key K and a file ciphertext c , output the decrypted file f .

Steps of the searchable encryption scheme are as follows.

Step 1: $PAS(1^\alpha) \rightarrow K$: Generate two α -bit binary strings: $k_1 = \{0,1\}^\alpha$, $k_2 = PAS(1^\alpha)$, and we get the key $K = (k_1, k_2)$.

Step 2: $PAD(K, f) \rightarrow (\gamma, \sigma, \bar{c})$: Create three empty hash linked lists $\gamma_f, \gamma_w, \gamma_d$ and an empty set σ . For any file $f \in f$, the unique keyword set of f is $\bar{f}$, $f \supseteq \bar{f} = (w_1, \dots, w_{lenth(\bar{f})})$.

Generate a string of pseudo-random sequences $s_1, \dots, s_{lenth(\bar{f})}$ through the pseudo-random number generator. Perform a cyclic computation for $w_i \in \bar{f}$,

$1 \leq i \leq lenth(\bar{f})$, $\tau_{w_i} = F_{k_1}(w_i)$, $\mathcal{E}_i = H_{\tau_{w_i}}(s_i) \parallel s_i$;
 $\bar{c} = (\mathcal{E}_1, \dots, \mathcal{E}_{lenth(\bar{f})})$ is sorted by dictionary order and save it in γ_f , set $\gamma_f[ID(f)] = \bar{c}$; Calculate the formula below:

$$c = SKE.PAD_{k_2}(f) \quad (13)$$

We get (γ, σ, c) , where $\gamma = (\gamma_f, \gamma_w, \gamma_d)$, $c = (c_1, \dots, c_{lenth(\bar{f})})$, γ_w , γ_d and σ are empty sets at this time.

Step 3: $PSek(K, w, \sigma) \rightarrow (\sigma', \tau_w)$: Set $K = (k_1, k_2)$, for the keyword w to be searched, calculate the search label:

$$\tau_w = F_{k_1}(w), \sigma' = \sigma \cup \{\tau_w\} \quad (14)$$

and the formula can be expressed as follows: (τ_w, σ') .

Step 4: $Sek(\tau_w, \gamma) \rightarrow (I_w, \gamma')$: set $\gamma = (\gamma_f, \gamma_w, \gamma_d)$.

Find out whether there is a key value related to τ_w in hash list γ_w . Find whether there is a key value related to τ_w in the hash chain table γ_w . If a key value is related to τ_w in the hash chain table γ_w , set $I_w = \gamma_w[\tau_w]$, $\gamma_w' = \gamma_w$. If not, generate an empty list I_w for any $\bar{c} \in \gamma_f$,

For any $\mathcal{E}_i \in \bar{c}$, $1 \leq i \leq lenth(\bar{c})$, set $\mathcal{E}_i = l_i \parallel r_i$, verify whether $H_{\tau_w}(r_i) = l_i$ is true, if it is true, then insert the file identifier $ID(f)$ corresponding to $\bar{c}$ into I_w , add τ_w to $\gamma_d[ID(f)]$. Update

$\gamma_w[\tau_w] = I_w$, and set the updated indexes as γ_w' , γ_d' . We get I_w and $\gamma' = (\gamma_f', \gamma_w', \gamma_d')$.

Step 5: $PAT(K, f, \sigma) \rightarrow \tau_a$: set $K = (k_1, k_2)$, for the file f to be added and its unique keyword set f , a series of pseudo-random sequences $s_1, \dots, s_{len(\bar{f})}$ are generated by the pseudo-random number generator. Create an empty list X , for any $w_i \in \bar{f}$, $1 \leq i \leq len(\bar{f})$, calculate the formula below:

$$\tau_{w_i} = F_{k_1}(w_i) \quad (15)$$

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

$$\mathcal{E}_f = H_{\tau_{w_i}}(s_i) \parallel s_i \quad (16)$$

$\bar{c} = (\mathcal{E}_1, \dots, \mathcal{E}_{len(\bar{f})})$ is sorted by dictionary order,

and its formula can be expressed as follows:

$$c = SKE.Enck2(f) \quad (17)$$

Then, and the formula can be expressed as follows:

$$\tau_a = (ID(f), \bar{c}, c, X) \quad (18)$$

Step 6: $AD(\tau_a, c, c', \gamma) \rightarrow (c', \gamma')$:

$\tau_a = (ID(f), \bar{c}, c, X)$, $\gamma = (\gamma_f, \gamma_w, \gamma_d)$. Add $\gamma_f[ID(f)] = \bar{c}$ to the index γ_f , for any $x_i \in X$, add $ID(f)$ to $\gamma_w[x_i]$, set $\gamma_d[ID(f)] = X$. The updated index is γ_f' , γ_w' , γ_d' . Add c to c . The updated ciphertext collection is marked as c' . Output (c', γ') , where $\gamma' = (\gamma_f', \gamma_w', \gamma_d')$.

Step 7: $Dlt(ID(f), c', \gamma) \rightarrow (c', \gamma')$:

$\gamma = (\gamma_f, \gamma_w, \gamma_d)$, $\gamma_w[Y_i]$, Create a list Y , $Y = \gamma_d[ID(f)]$. For any $Y_i \in Y$, delete $ID(f)$ from, delete $\gamma_f[ID(f)]$ from γ_f , delete $\gamma_d[ID(f)]$ from γ_d . The updated index is γ_f' , γ_w' , γ_d' . Delete c corresponding to $ID(f)$ from c , and write it as c' after the update. Then, output (c', γ') , $\gamma' = (\gamma_f', \gamma_w', \gamma_d')$.

Step 8: $DSF(K, c) \rightarrow f$: Set $K = (k_1, k_2)$, and its formula can be expressed as follows:

$$f = SKE.DSFk2(c) \quad (19)$$

Analysis

Performance

Analysis of Lightweight Authentication

Table. 3 Symbols of Lightweight Authentication

Symbol	Explanation
PUF	Computation amount of physical unclonable function.
DIG	Calculation amount of bitwise operation.
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 pseudo-random function.
CMO	Calculation amount of circular movement operation.

In this paper, performances of mobile medical devices are compared with some classic

authentication schemes. Comparisons of calculation cost are shown in Fig. 2.

Fig. 2 Comparison of Communication

Assumed that the length of communication traffic and storage parameters are the same. And there are four kinds of information, that are IDS , ID , K and Δk saved in mobile terminal devices in medical system. In our scheme, there are 14 session

messages in a complete session. So, the communication traffic size is 14. It can be seen from the Fig. 2 that our scheme can reduce the computing burden.

Table. 4 Comparison of Calculation Cost of Each Scheme.

Scheme	Computing Burden
Reference [28]	5PUF+5DIG+1RAN
Reference [27]	7MOD+2DIG+2RAN
Reference [26]	6HASH+3DIG+1RAN
Reference [30]	7PRNF+4DIG+2RAN
Reference [25]	11CMO+4DIG+1RAN
Our scheme	6CMO+2DIG+1RAN

From the point of view of the computing burden, our scheme and the scheme in reference [25] are both ultra-lightweight. The algorithms used in other comparative references are all lightweight, so the scheme in this paper has great advantages in reducing calculation time.

In the scheme of reference [25], 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, steps of calculation are as follows. Firstly, we generate a random number

$x \frac{\Delta y}{\Delta x}$ to operate RAN. Secondly, in the process of

Table. 5 Symbols of Searchable Encryption

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

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 message N_3 and N_4 . Lastly, we perform the last two CMO operations to update the shared secret values and pseudonyms. So, the total computing burden in our scheme is $6CMO + 2DIG + 1RAN$.

Analysis of Searchable Encryption

Description of relevant symbols are as shown in Table 5.

The performances of our scheme are compared with other references, and the results are shown in Table 6.

Table. 6 Comparison of Time Complexity

Program	Search Time	Index Space	Update Leak	Update Cost
literature [20]	$O(m/n)$	$O(m+n)$	$ID(w)$	$O(m/n)$
literature [21]	$O(\log f \cdot m/n)$	$O(f \cdot n)$	—	$O(\log f \cdot n)$
literature [16]	$O(m/n)$	$O(m+n)$	—	$O(m/n)$
literature [17]	$O(m/n)$	$O(m+n)$	$ID(w)$	$O(m/n)$
literature [18]	$O(m/n)$	$O(m+n)$	—	$O(m/n)$
Our work	$O(m/n)$	$O(m+n)$	—	$O(m/n)$

Security

(1) In design of the authentication scheme, the pseudonym of 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 number 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 message from

intercepting the current message or deduce the user's privacy information in the previous round of communication message, 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 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 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_{search} , L_{add} , L_{delete} , $L_{encrypt}$ to give the leaked information. Relevant parameters are shown in Table 5.

Table. 7 Symbols of Leak Functions

Symbol	Explanation
$ACCP_t(w)$	Access pattern, the file identifier of the file in f_w when the keyword w is queried at time t , that is, the set $\{ID(fi) : w \in fi, fi \in f\}$.
$\bar{f}$	Unique keyword set of files f .
$SRCH_HIS(\bar{f})$	The set of identifier $ID(w)$ of keywords that have been searched in time t File f , that is, the set $SRCH_HIS(\bar{f}) = \{ID(wi) : wi \in f, \tau_{wi} \in \sigma\}$.

In our scheme,

$$L_{search}(f, w) = (ACCP_t(w), ID(w)) \quad (20)$$

$$L_{delete}(f, f) = (ID(f), SRCH_HIS(\bar{f})) \quad (21)$$

$$L_{encrypt}(f) = lenth(f) \quad (22)$$

According to the above leak functions, except access models, our scheme doesn't disclose more information to the server.

Conclusions

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. In order 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, 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 diversified search functions. Except the basic search function, we also need to support some special functions, such as approximate search, wildcard search, fuzzy search, multi-keyword search and so on.

Acknowledgments

We sincerely thank the Reviewers and the Editor for their valuable suggestions.

Authors' contributions

Shuo Gao and Zekai Liu designed the framework of this scheme. Yihan Liu and Qichao Wang designed the core algorithm and performed the experiments. Wei Ou provided technical supports. All authors reviewed and approved final manuscript.

Authors' information

Shuo Gao is a student of Hainan University. His research interests include information security and cyber security.

Qichao Wang is a student of Hainan University. His research interests include information security and cyber security.

Yihan Liu is a student of Hainan University. His research interests include information security and cyber security.

Zekai Liu is a student of Hainan University. His research interests include information security and cyber security.

Wei Ou received the B.S. degree from the Air Force Engineering University, in 2000, and the M.S. degree in the National University of Defense Technology in 2005, and the Ph.D. degree in the National University of Defense Technology, in 2013. He is

an associate professor in Hainan University. His research interests include cryptography, cyber security, AI security and Blockchain technology.

Wenbao Han received his M.S. degree at Sichuan University in 1988 and the Ph.D. degree at Sichuan University in 1994. He is currently a professor in Hainan University. His research interests include cryptography, cyber security, AI security and Brain-like computing.

Funding

Not applicable.

Availability of data and materials

There is no supporting data available.

Competing Interests

The authors declare that they have no competing interests.

References

- [1] West D M. Improving health care through mobile medical devices and sensors. Brookings Institution Policy Report, 2013, vol. 10, pp. 1-13.
- [2] Patra, Manas Ranjan, Rama Krushna Das, and Rabi. Prasad Padhy CRHIS: cloud based rural healthcare information system. In: Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance, 2012, pp. 402-405.
- [3] Zyskind, Guy, and Oz Nathan. Decentralizing privacy: Using blockchain to protect personal data. IEEE Security and Privacy Workshop, 2015, pp. 180-184.
- [4] Azaria, Asaph. Medrec: Using blockchain for medical data access and permission management. IEEE International Conference on Open and Big Data (OBD), 2016, pp. 25-30.
- [5] Al Omar, Abdullah. Medibchain: A blockchain based privacy preserving platform for healthcare data. Springer, Cham International conference on security, privacy and anonymity in computation, communication and storage, 2017, pp. 534-543.
- [6] Magyar, Gábor. Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. IEEE 30th Neumann Colloquium (NC), 2017, pp. 135-140.
- [7] Griggs K N, Ossipova O, Kohlios C P, Baccarini A N, Howson E A, and Hayajneh T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of medical systems, 2018, 42(7): 1-7.

- [8] Ye N, Zhu Y, Wang R, Malekian R, and Lin Q M. An efficient authentication and access control scheme for perception layer of internet of things, 2014, pp. 1617-1624.
- [9] Do, Hoang Giang, and Wee Keong Ng. Blockchain-based system for secure data storage with private keyword search. IEEE World Congress on Services (SERVICES), 2017, pp 90-93.
- [10] Liang X, Zhao J, Shetty S, Liu J, and Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), 2017, pp. 1-5.
- [11] Zhang A, and Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of medical systems, 2018, 42(8): 1-18.
- [12] Ji Y, Zhang J, Ma J, et al. BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems. Journal of Medical Systems, 2018, vol. 42, no.8, pp 147.
- [13] Wang Q, Zhou D, Yang S, Li P, Wang C, and Guan Q. Privacy preserving computations over healthcare data. 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 (SmartData), 2019, pp 635-640.
- [14] Yue X, Wang H, Jin D, Li M, and Jiang W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 2016, 40(10): 1-8.
- [15] Tian H, He J, and Ding Y. Medical data management on blockchain with privacy. Journal of medical systems, 2019, 43(2): 26.
- [16] Cash D, Jaeger J, Jarecki S, Jutla C S, Krawczyk H, Rosu M C, and Steiner M. Dynamic searchable encryption in very-large databases: data structures and implementation. NDSS, 2014, pp 23-26.
- [17] Naveed M, Prabhakaran M, and Gunter C A. Dynamic searchable encryption via blind storage. IEEE Symposium on Security and Privacy, 2014, pp 639-654.
- [18] Hahn F, and Kerschbaum F. Searchable encryption with secure and efficient updates. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014, pp 310-320.
- [19] Chen L, Lee W K, Chang C C, et al. Blockchain based searchable encryption for electronic health record sharing[J]. Future Generation Computer Systems, 2019, 95: 420-429.
- [20] Kamara S, Papamanthou C, Roeder T. Dynamic searchable symmetric encryption. Proceedings of the 2012 ACM conference on Computer and communications security, 2012, pp 965-976.
- [21] Kamara S, Papamanthou C. Parallel and dynamic searchable symmetric encryption. International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2013, pp. 258-274.
- [22] R Wang, J He, C Liu, Q Li, W Tsai and E Deng. A Privacy-Aware PKI System Based on Permissioned Blockchains. IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), 2018, pp 928-931
- [23] Zhong H, Li Z, Cui J, Sun Y, and Liu L. Efficient dynamic multi-keyword fuzzy search over encrypted cloud data. Journal of Network and Computer Applications, 2020, 149: 102469.
- [24] Eslami Z, Noroozi M, and Baek J. On the Security of a Privacy-Preserving Ranked Multi-Keyword Search Scheme. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 2019, 10(1): 75-85.
- [25] Cao Shuya, Yao Yingying, Chang xiaolin. Lightweight A port-based forwarding load-balancing scheduling approach for cloud datacentre networkssecure authentication scheme using blockchain for RFID system in smart factory. Cyberspace Secumity, 2020, vol.11, no. 9, pp. 70-77.
- [26] Alphand O, Amoretti M, Claeys T, et al. IoTChain: A blockchain security architecture for the Internet of Things[C]. IEEE wireless communications and networking conference (WCNC), 2018, pp. 1-6.
- [27] Dorri A, Kanhere S S, Jurdak R. Towards an optimized blockchain for IoT[C]. IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, 2017, pp. 173-178.
- [28] Samaniego M, Jamsrandorj U, Deters R. Blockchain as a Service for IoT[C] IEEE 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 (SmartData). IEEE, 2016, pp. 433-436.
- [29] Ma X, Gao H, Xu H, and Bian M. An IoT-based task scheduling optimization scheme considering the deadline and cost-aware

scientific workflow for cloud computing. EURASIP Journal on Wireless Communications and Networking, 2019, pp. 1-19.

- [30] Tao F, Zhao D, Hu Y, et al. Resource service composition and its optimal-selection based on particle swarm optimization in manufacturing grid system[J]. IEEE Transactions on industrial informatics, 2008, 4(4): 315-327.

Figures

Figure 1

The System Structure

Figure 2

Comparison of Communication