World Wide Web (2018) 21:33–57
DOI 10.1007/s11280-017-0455-z

An infrastructure framework for privacy protection of community medical internet of things

Transmission protection, storage protection and access control

Fulong Chen[1,2] · Yonglong Luo[1,2] · Ji Zhang[3] ·
Junru Zhu[2] · Ziyang Zhang[2] · Chuanxin Zhao[2] ·
Taochun Wang[2]

Received: 5 October 2016 / Revised: 24 January 2017 /
Accepted: 27 March 2017 / Published online: 6 April 2017

Abstract As a kind of medical service around people, community health care is closely related to peoples lives, and thus it has also been placed higher requirements. In the face of growing community medical needs, the construction and development of community medical Internet of things is imminent. Subsequently, massive multi-type of medical data which

This article belongs to the Topical Collection: *Special Issue on Security and Privacy of IoT*
Guest Editors: Tarik Taleb, Zonghua Zhang, and Hua Wang

✉ Fulong Chen
long005@ahnu.edu.cn

Yonglong Luo
ylluo@ustc.edu.cn

Ji Zhang
ji.zhang@usq.edu.au

Junru Zhu
jrzhu_study@163.com

Ziyang Zhang
zzy000@ahnu.edu.cn

Chuanxin Zhao
zhaocx@mail.ahnu.edu.cn

Taochun Wang
wangtc@ahnu.edu.cn

[1] Department of Computer Science and Technology, Anhui Normal University, Wuhu, China

[2] Engineering Technology Research Center of Network and Information Security,
Anhui Normal University, Wuhu, China

[3] Faculty of Health, Engineering and Sciences, University of Southern Queensland,
Toowoomba, Australia

contain all kinds of user identity data, various types of vital signs data and other sensitive information are generated. Such a large scale of data in the transmission, storage and access process is facing the risk of data leakage. To effectively protect the privacy information of patients, an infrastructure framework for privacy protection of community medical Internet of things is proposed. It includes transmission protection based on multi-path asymmetric encryption fragment transmission mechanism, storage protection using distributed symmetric encryption cloud storage scheme and access control with identity authentication and dynamic access authorization. Through theoretical analysis and simulation experiments, it is proved that the community medical data can be effectively protected.

Keywords Internet of things · Privacy protection · Encryption · Health care · Authentication

1 Introduction

As one of the most booming technologies, the Internet of things (IoT) was gradually applied to various fields, especially in the field of health care. The rapid economic development has led to the deterioration of the natural environment upon the survival of people's health under unprecedented threat. Various non-predictability of diseases have sprung up on the patients so that patients' illness makes it painful bring the demand for medical services growing. However limited traditional medical service resources and uncertainty treatment time urge people to start to look for better health services to make up for the lacking of available resources.

Medical Internet of things (MIoT) is a specific "smart health care" implementation, more simple to say, is a kind of applications of Internet of things technology in medical field. In MIoT, due to the huge amount of heterogeneous medical data, extensive medical data sources, and various identification information which involve user privacy, once medical data loses or tampers, some privacy leakages resulting in catastrophic loss will occur. The open nature of wireless medium may expose some privacies to a variety of unauthorized users, and will result in insecure transmission, storage and access [37, 38]. As IoT is built on the basis of the Internet [4, 13], security problems of the Internet will also show up in MIoT.

How to ensure the security of such data has been always the focus of academic research. Therefore, we propose an infrastructure framework for privacy protection of community medical Internet of things (CMIoT). Our contributions are to provide CMIoT with privacy protection in three aspects such as transmission protection based on multi-path asymmetric encryption fragment transmission mechanism, storage protection using distributed symmetric encryption cloud storage scheme and access control with identity authentication and dynamic access authorization.

The rest of this paper is organized as follows. Section 2 discusses some related works. Section 3 describes the architecture of CMIoT. Transmission protection, storage protection and access control in CMIoT are introduced in Sections 4, 5, and 6. Section 7 presents some experimental and simulation results. The last section concludes the paper and lays out future research issues.

2 Related works

Since the concept of IoT was proposed, some scholars have tried to design its security privacy protection methods. Encryption including symmetric and asymmetric encryption is a common way of privacy protection. Popular encryption methods, e.g., DES (Data Encryption Standard), RSA (Ron Rivest, Adi Shamir, and Leonard Adleman), et al, are used in many information systems and also can be used in CMIoT. However, we must consider that there are many low speed, small capacity transmission nodes in CMIoT. Ning [20] considered a variety of secure factors of IoT, and believed that there would be a tradeoff between privacy strength and specific business needs. Namely, it needs to custom privacy policy moderately on the basis of business needs as much as possible to protect users' privacy. Therefore, some methods of data disorder with low configuration requirements are also preferentially used to encrypt sensitive data.

2.1 General methods

Lamport [16] first proposed the safe way Hash function encryption to users. Ding [5] proposed a kind of authentication protocol based on Hash function. Maeda [18] proposed two schemes based on re-encryption in which one is to use the re-encryption authentication to prevent location privacy leaks, and another is to use a one-time re-encryption to make RFID tags anonymous. Wu [30] introduced the data protection methods using lightweight cryptographic algorithms and a kind of ONS query mechanism under the condition of encrypted search query in most IoT applications. Du [6] proposed a probabilistic key sharing scheme suitable for WSNS to share. The same communication key exists between any two nodes is P and security is not guaranteed. Song [23] studied the secure and reliable transmission scheme SPS based on Internet of Things. He presented a cooperative transmission mechanism and the rate selection algorithm based on the channel state in order to transmit data effectively and reliably. Kothmayr [15] proposed an end-and-end mutual authentication mechanism of IoT based on DTLS protocol. The mechanism is based on the existing Public-key encryption algorithm, which is vulnerable to suffer from middle attack because of no three session process. Groce [8] introduced a provably secure PAKE protocol standard model. However there is no trusted third party so as to result in non-universal about the presented protocol.

Ma proposed a point-to-point authentication and secure transmission protocol [17] based on Hash functions and block cipher. A secure transmission method which may be fit on the IoT has been mentioned in [31]. The trusted third party would be adopted while two parties would be authenticating, and therefore the scheme would be not universal in terms of the complex Web environment. In secure model of IoT, there is a common problem in the application, and there involves a variety of mixed-format electronic medical records and other patient data in MIoT. However, those methods which we have discussed above cannot fit the field. When data are transferred, stored or accessed, data attacking and data leaking will cause our privacy information to be illegally obtained.

Taking into account the special nature of CMIoT, in [32], privacy data is divided into two categories such as enforcing data privacy and user privacy over outsourced database service so as to achieve the classified protection of user privacy information. In a large number of electronic archives security and privacy protection schemes, Hong [9] proposed a very effective protection scheme for electronic health records based on SOA with SSL, WS-Security, and personal access control technology. Venkatasubramanian [24] proposed a key agreement PSKA based on physiological signal information, providing guarantee for secure communication between nodes in wireless body area network.

2.2 Transmission protection

In CMIoT, data is mostly transmitted through wireless communication, easier to be intercepted. In view of the limited capacity of the sensor or communication system, the method of privacy protection of data is mostly based on the lightweight encryption algorithm [29]. Du [6] proposed a probabilistic key sharing scheme suitable for WSNS, and however if the probability of the same communication key between any two nodes was P, the security would be not guaranteed. Song et al [23] designed the rate selection algorithm based on the current channel state and the mechanism of multi-party cooperative data transmission.

About authentication before transmission, some schemes, e.g., Hwang's [12] two-way authentication scheme between nodes, Peyravian's [21] authentication scheme based on Hash function, Wang's [27] two way anonymous password authentication scheme, and Kothmayr's [15] end to end two-way authentication mechanism for IoT based on DTLS protocol using the existing public key encryption algorithm, have been proposed. However in these methods, there were no three session process and vulnerable to the middle attack. Groce [8] studied and proposed a protocol that could be proved secure in the general model, and however there was no assumption of a trusted third party and the protocol was not universal. Forsstrom [7] studied the security issues of intelligent terminals in the Internet of things through a variety of heterogeneous network architecture, and a distributed verification system based on MediaSense platform was proposed to ensure the security of the communication between smart terminals. We had also proposed a disturbing data transmission mode [36] for privacy protection on massive streaming categorical information.

Unfortunately, for all these IoT security transmission models, there are some problems in their application, e.g., many kinds of mixed format data including patient's electronic medical record and so on in MIoT.

2.3 Storage protection

Data storage faces a paradox: encryption data cannot be efficiently processed, and the security and privacy of non encrypted data can not be guaranteed. Therefore, it is urgent to need a kind of effective privacy protection method to ensure the safety of medical data storage in the controllable range. Ateniese [1] proposed a distributed data secure storage scheme in which data is encrypted using the symmetric keys, and the symmetric keys are encrypted using public key. However, there exists the risk of collusion between the malicious server and malicious users, leading to the disclosure of the file encryption key. Vimercati [25] proposed a method for secure storage of data by a non trusted server key derivation method, in which each file is encrypted with a symmetric key, each user has a private key, and in order to authorize, data owners create public tokens for users so that authorized users can use their private key to derive the decryption key of the specified file from the tokens. The key number of the scheme is too large and the complexity of the operation is linear with the number of users so as unable to effectively extend. Kamara [14] studied a kind of abstract public cloud storage encryption framework composed of data processing module, data verification module, token generation module and credential generation module, in which the storage data controlled by the owner is authorized to be accessed via token token generated by the token generator and to be decrypted through credentials generated by credential generator, and their security is controlled by the password mechanism. The data protection technology based on VMM is proposed in [10] where the operating system and the distributed file system are isolated to protect data security by using the Daoli virtual security monitoring system and the SSL secure transmission module. A kind of homomorphic encryption algorithm [11] is designed to realize data encryption and decryption with mixed operations of cector and matrix operation, supports for fuzzy retrieval of encrypted data, and can be better to perform the homomorphic addition and subtraction operation. The downside of this approach is the low efficiency in cipher text retrieval and homomorphic multiplication/division.

Wang [28] studied and proposed a secure storage of outsourced data in the cloud environment. In the method, the storage efficiency is improved by dividing the file into blocks and the data security is ensured for each data block using a different key encryption. Because of the need to spend a lot of cost data encryption and key management, the scheme has a lot of problems. A reliable data protection and destruction method with the help of a trusted platform was proposed by Zhang [35]. He designed a virtual monitor as the trusted third party responsible for monitoring and protecting the user's privacy data, and destroying user data in accordance with user requirements, even if the cloud server's super administrator can not bypass the protection of user privacy data. It is obvious that the method is too high requirements for the reliability of the hardware and software, and the actual situation is difficult to meet. A storage model of cloud computing was designed in [19] where the trusted third party server is responsible for the isolation of user privacy data and general data, and thereby realizes the protection of user's privacy information. However, in this scheme, when the data is stored, the two times of data partitions and matrix operation make the storage efficiency low so that it is difficult to use and expand on a large scale.

2.4 Access control

As a kind of storage media which can not controlled by users, cloud storage needs to be ensured to access legally. In MIoT, a large number of diagnostic data of patients are generated each day and stored in the cloud server so that access control faces new challenges. Users such as patients, doctors, and nurses can use mobile terminals for personal medical data query including query for privacy data. Most of the data in the server are not encrypted. We need to ensure that users access to the medical data storage server without disclosing patient privacy data. Access control mechanism can authorize legitimate users to access specific resources while denying access to illegal users. Authorization method is generally divided into two categories including access control model and encryption mechanism. In the access control model, different roles are divided according to the specific access policies. When data is accessed, the system can be controlled to be accessed or not through the role of the visitor. The encryption data in the cipher mechanism can only be encrypted by the authorized person having the corresponding key. Pirretti [22] put forward that in the encryption scheme based on attributes, the user attribute and the time stamp for this attribute were added. The disadvantage of the scheme is that users need to regularly apply to the Certification Center for the reuse of private keys, and before the end of time, user rights can not be revoked. On the basis of the attribute-based scheme, Bethencourt [3] put forward the cipher text strategy in which the identity of a user is represented as a collection of attributes, related to the access control structure of encrypted data, so that users can decrypt them according to attribute set related to user's identity. ABE cipher text access control was addressed in [33] using dynamic changed strategies, but the execution efficiency is not high and the cost of a single execution is very large. Yuen [34] proposed the identity as the encryption base for encrypting users to resist information leakage, and Beato [2] proposed a user identity Username as the identity of the public key for encrypting the user's privacy information stored in the OSN network or shared with other users. All of them need to be improved in terms of efficiency and security.

3 Community medical internet of things

The CMIoT is achieved in one community, as shown in Figure 1. In the CMIoT, using ZigBee, blue-tooth or infrared communication technology, data from a sensor is sent toward the nearest gateway belong to some place such as home, community public area, community health center or hospital, and then the data is transmitted to the nearest community router using WiFi or Ethernet communication technology. Through various routers, the communication link is built between the gateway and the cloud storage server in the community health center through wireless and wired network. In the end, the cloud storage server provides the resolved data to users with mobile terminals or PC terminals.

As shown in Figure 2, the CMIoT is mainly composed of three different sub-systems as follows.

- **Home subsystem**.
  It includes a sink gateway supporting ZigBee, blue-tooth, infrared and WiFi communication, some medical sensors such as blood pressure, blood oxygen, blood glucose, heart rate, and ECG sensor, some actuators such as buzzer, indicator, DC motor, stepping motor, etc. used for alarm, display and control, and mobile terminals. These sensors can collect users' physical sign data and send them to the gateway so that latter can take some measures and send them to the cloud storage server through the communication link. Those data also can be sent to mobile terminals so that users can view

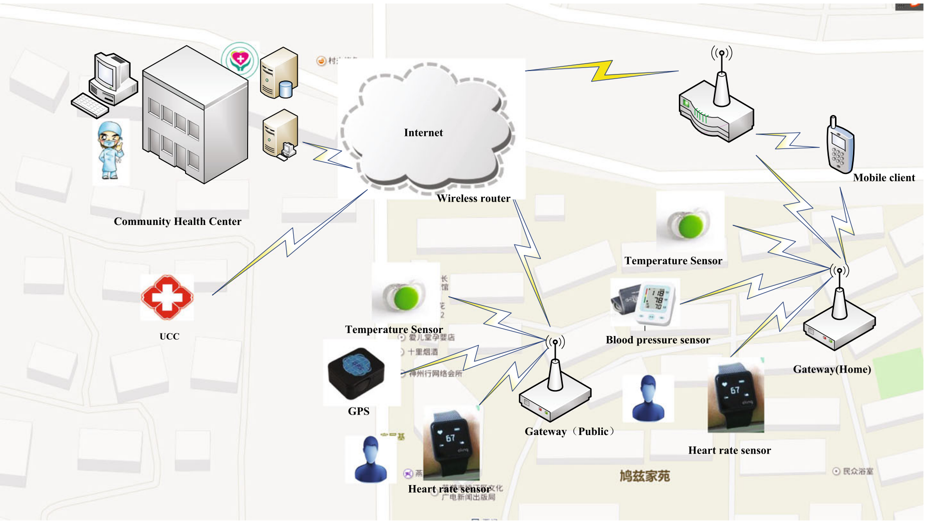

Figure 1 Deployment structure of community medical Internet of things

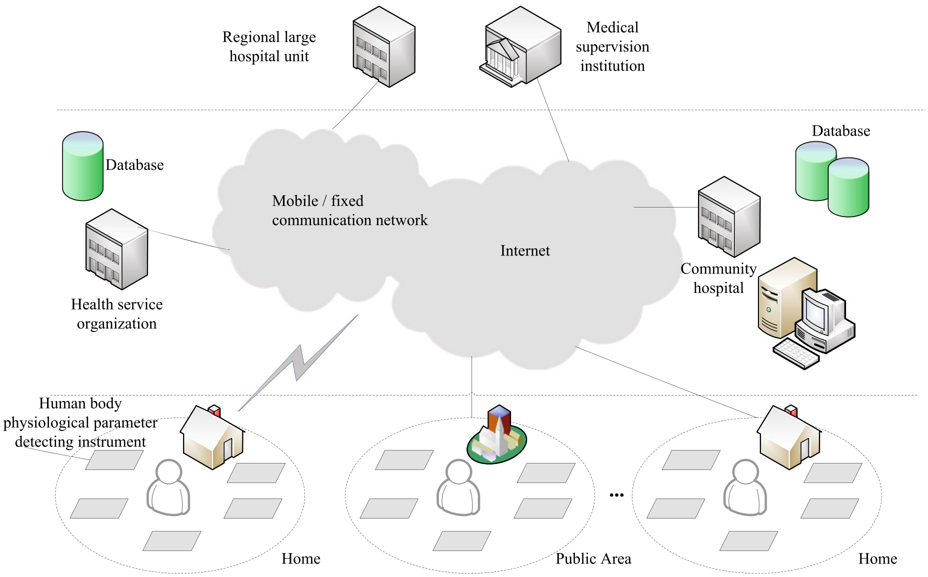
Regional large hospital unit
Medical supervision institution
Database
Database
Mobile / fixed communication network
Internet
Health service organization
Community hospital
Human body physiological parameter detecting instrument
...
Home
Public Area
Home

Figure 2 Abstract structure diagram of community medical Internet of things

them or control some actuators. Of course, mobile terminals can also be used to access the data stored on the cloud storage server. In a community, there are various of home systems.

- **Public area subsystem**.

  Besides the sink gateway, some sensors and actuators similar to the home subsystem, some rehabilitation and fitness equipments connected with the sink gateway are deployed in the public area subsystem. In a community, there are various of public area systems.
- **Community hospital subsystem**.

  There are some sink gate way, some medical sensors and actuators, some mobile terminals and computers for doctors or nurses, some storage servers for cloud storage, a management system in the CMIoT server, and some special medical instrument and equipments. In this system, the main functions are storage management and access control management.

4 Multi-path asymmetric encryption fragment transmission mechanism

4.1 Multi-path fragment transmission model

After collecting a set of medical data from medical sensors, the sink gateway will package those data into a packet and then divide it into a group of split fragments using slice model so that they can be transferred in split fragments through multiple paths built of routers as shown in Figure 3. Assuming that the user's information in a packet is M, and the number of paths is n, the packet M composed of various medical information is divided into n independent and interrelated numbered data fragments M_1, M_2, ..., M_n by the sink gateway. After those data fragments are processed in a certain processing method, e.g., encryption,

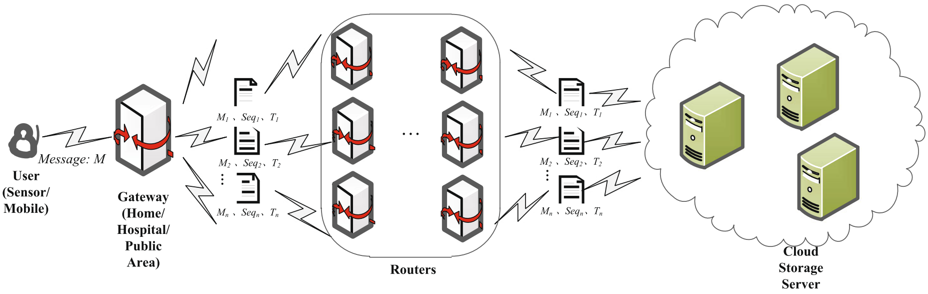

Figure 3 Multi-path transmission model

they are sent from the sink gateway. Each fragment which contains certain user information is transmitted to the cloud storage server through respective communication links.

4.2 Gateway node registration and bi-directional authentication

In the multi-path asymmetric encryption fragment transmission mechanism, some data transmission symbols are defined as shown Table 1.

4.2.1 Registration process

Before the normal data transmission is carried out, it needs to complete some initial operations including gateway node registration and three-party bi-directional authentication. The gateway node G registers itself in the third party authentication server S_A and set up the authentication key in the cloud storage server S_S as shown in Figure 4.

Table 1 The definitions of data transmission symbols

No.	Symbol	Definition
1	S	Server node, e.g., authentication server S_A and storage server S_S
2	G	Gateway node
3	ID_G	Gateway node identification
4	PW_G	Gateway node Password
5	$H(x)$, $H_K(x)$	Strongly non-collision Hash function, and Hash function with key
6	R_G	Random number of gateway node
7	R_S	Random number of server node
8	SK_G	Private key of gateway node
9	PK_G	Public key of gateway node
10	SK_S	Private key of server node
11	PK_S	Public key of server node
12	$e_K(M)$	Encrypt M with K with some symmetric encryption algorithm
13	$d_K(M)$	Decrypt M with K with some symmetric decryption algorithm
14	$E_{SK}(M)$	Encrypt M with SK with some asymmetric encryption algorithm
15	$D_{PK}(M)$	Decrypt M with PK with some asymmetric decryption algorithm
16	K_{G-S}	Shared key between G and S

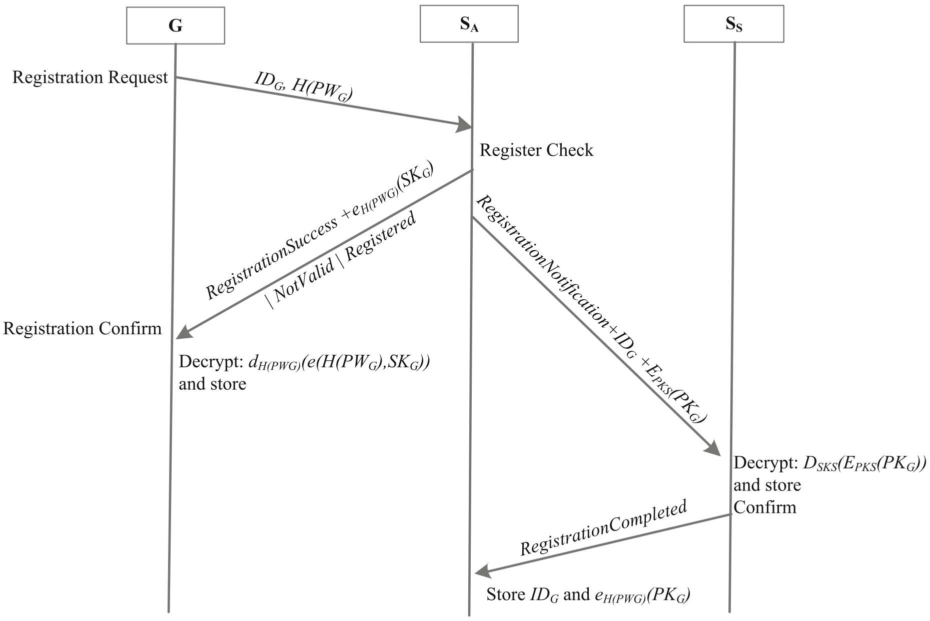
G
S_A
S_S
Registration Request
ID_G, H(PW_G)
Register Check
RegistrationSuccess +e_H(PWG)(SK_G)
\ NotValid \ Registered
RegistrationNotification+ID_G +E_PKS(PK_G)
Registration Confirm
Decrypt: d_H(PWG)(e(H(PW_G),SK_G)) and store
Decrypt: D_SKS(E_PKS(PK_G)) and store
Confirm
RegistrationCompleted
Store ID_G and e_H(PWG)(PK_G)

Figure 4 Registration process

4.2.2 Gateway node

For the gateway node G, it runs as the following process.

Step 1: G delivers its identification code ID_G and the Hash value of password PW_G to S_A. To be clear, PW_G is distributed to G by the administrator of S_A in advance. It continues to ***Step 2***.

Step 2: After receive some feedback messages from S_A, G will check its registration. If the message is $NotValid$, it needs to modify its password so as to send the registration request again or drops its registration. If the message is $RegistrationSuccess$, it decrypts

$$x = e_{H(PW_G)}(SK_G) \tag{1}$$

gets

$$SK_G = d_{(H(PW_G)}(x) \tag{2}$$

stores SK_G in its non volatile memory so as to make sure that this time of authentication is completed. If the message is $Registered$, it needs to modify its identification code so as to send the registration request again or drops its registration.

4.2.3 Authentication server

For the third party authentication server S_A, it runs as the following process.

Step 1: S_A searches ID_G in its registration dictionary, and contrasts $H(PW_G)$ to validate ID_G and PW_G. If S_A confirms the legitimacy of G, it will go to ***Step 2***. Otherwise, it will send a message $NotValid$ to informing of G that the registration fails.

Step 2: If S_A checks the registration flag of G in its registration dictionary and finds that G is not registered, i.e. the flag is $NotRegistered$, it will modify the flag to be $Registered$, generate a pair of asymmetric keys $\langle SK_G, PK_G\rangle$ for G, securely send a message $RegistrationSuccess$ and $e_{H(PW_G)}(SK_G)$ to G , securely send a message $RegistrationNotification$, ID_G and $E_{PK_S}(PK_G)$ to the cloud storage server S_S, and go to . Otherwise, it will only send a message $Registered$ to G.

Step 3: If a message $RegistrationCompleted$ is received from S_S, it stores ID_G and $e_{H(PW_G)}(PK_G)$ in S_A and this time of authentication is completed.

For the cloud storage server S_S, it runs as the following process.

Step 1: If it receives a message $RegistrationNotification$, ID_G and

$$x = E_{PK_S}(PK_G) \tag{3}$$

it decrypts x and gets

$$PK_G = D_{SK_S}(x) \tag{4}$$

and stores ID_G and PK_G in its public key table of gateway nodes. Then it goes to ***Step 2***.

Step 2: It sends a message $RegistratiionCompleted$ to S_A and this time of authentication is completed.

4.3 Improved Diffie-Hellman key agreement mechanism

After completing the three party bi-directional authentication among G, S_A and S_S, G obtains its private authentication key SK_G, and S_S obtains G's public authentication key PK_G. For traditional Diffie-Hellman key agreement mechanism, when two parties involved in key agreement are exchanging data, if the exchanged data are intercepted and captured, the key negotiated by them may be guessed. Therefore making use of the two keys SK_G and PK_G, G and S_S can exchange encrypted data. Using the improved Diffie-Hellman key agreement mechanism, G and S_S will negotiate the transmission keys, which generation and distribution process are elaborated as follows.

Step 1: A large prime number p is selected by G and S_S, and g is selected as a generator for the multiplicative group Z_p^*;

Step 2: G selects a secret integer x:

$$1 \leq x \leq p - 1 \tag{5}$$

and calculates $g_x = g^x \; mod \; P$, and sends $E_{SK_G}(g_x)$ to S_S;

Step 3: S_S selects a secret integer y:

$$1 \leq y \leq p - 1 \tag{6}$$

and calculates $g_y = g^y \; mod \; P$, and sends $E_{PK_G}(g_y)$ to G;

Step 4: G decrypts

$$g_y = D_{SK_G}(E_{PK_G}(g_y)) \tag{7}$$

calculates

$$K_{G-S} = g_y^x \; mod \; p \tag{8}$$

Step 5: S_S decrypts

$$g_x = D_{PK_G}(E_{SK_G}(g_x)) \tag{9}$$

calculates

$$K_{G-S} = g_x^y \, mod \, p \tag{10}$$

Step 6: G and S_S share the same key K_{S-G}, which is used to complete the key sharing and ensure the uniqueness of the key for the data transmission.

4.4 Fragmented multi-path data transmission

According to the mentioned above, G and S_S have accomplished their bi-directional authentication and key agreement, and finally they can commonly share the session key K_{S-G}. To ensure the security of the data transmission process, G encrypts the the data M to be transmitted with the key K_{S-G}, and divides cipher-text into fragments to transfer through multiple different paths. Multi-path data encryption and cipher-text transmission are described as follows.

Step 1: Assuming that the data packet to be transmitted is M, G uses the key K_{S-G} to encrypt M, and gets the cipher-text

$$C = e_{K_{S-G}}(M) \tag{11}$$

Step 2: G divides C into sub data packets

$$C = \biguplus_{i=1}^{n} C_i \tag{12}$$

For every one of the sub data packets, G adds a session number Seq, sub-packet identification i and time stamp T_i to them, and get the sub data packets as follows:

$$m_i = \langle C_i, Seq, i, T_i \rangle (1 \le i \le n) \tag{13}$$

Where Seq and i are used to restore the data by S_S, and T_i is used to prevent replay attacks. Then G calculates the message authentication code $H_{K_{S-G}}(C_i, Seq, i, T_i)$ using the Hash function $H(x)$ with keys, so that S_S can verify the message. Finally on each selected path, G sends the message

$$S_i = \langle C_i, Seq, i, T_i, H_{K_{S_G}}(C_i, Seq, i, T_i) \rangle \tag{14}$$

Step 3: For each sub data packet S_i received

$$S_i = \langle C_i, Seq, i, T_i, A \rangle \tag{15}$$

S_S will extract the received authentication code A from S_i, and also calculate the authentication code

$$A' = H_{K_{S-G}}(C_i, Seq, i, T_i) \tag{16}$$

If $A = A'$, then accept S_i.

Step 4: After S_S receives all of sub data packets $S_1, S_2, ..., S_n$, which are sent from G, S_S will reorganize the sub data packets and get the full cipher-text message

$$\biguplus_{i=1}^{n} C_i = C \tag{17}$$

decrypt C and recover the data packet M

$$M = d_{K_{S-G}}(C) \tag{18}$$

Table 2 Authentication security analysis

Security condition	[12]	[21]	[27]	[17]	Multi-path
Prevent DoS attacking	–	Yes	–	Yes	Yes
Prevent replay attacking	–	Yes	Yes	Yes	Yes
Prevent dictionary attacking	Yes	Yes	Yes	–	Yes
Prevent server forging	Yes	Yes	Yes	Yes	Yes
Prevent gateway-node forging	Yes	–	Yes	Yes	Yes
No public key mechanism	Yes	Yes	–	Yes	Yes
Hash function	Yes	Yes	Yes	Yes	Yes
MAC function	–	–	–	Yes	Yes

4.5 Transmission security analysis

For the data transmission protection in CMIoT, its security includes authentication security, key agreement security and multi-path transmission security.

4.5.1 Authentication security

Before data transmitting, G has an authentication with S_S and S_A. If the two-party bi-directional authentication do not entirely pass, S_S will refuse to receive data so as to prevent fake gateway nodes from forging transmission data, and G will refused send data so as to avoid the phishing of the pseudo server node. Even if attackers steal the password table of S_A, they cannot crack the password because of the unidirectional characteristic of Hash function. Therefore, it can effectively ensure the identity authentication for S_A and G.

As shown in Table 2 where ”Yes” represents that the security condition is met, from the implementation process, the above protocol takes advantage of Hash function and MAC to become more efficient than Wang’s public key algorithm. MAC function is not referred in Peyravian’s research, therefore Peyravian’s protocol cannot prevent gateway nodes forging. Ma’s protocol cannot prevent dictionary attacking due to the data characteristic despite of various means of attacking.

4.5.2 Key agreement security

In order to prevent the attacker intercepting a party data and forging new data for transmission when the two parties exchange data, the three-way handshake is brought into the key agreement process for ensuring the correctness of the final key-agreement. In Table 3, “Yes” represents that the security condition is met.

Table 3 Key agreement security analysis

Security condition	*Diffie-Hellman*	[31]	Multi-path
Prevent replay attacking	Yes	Yes	Yes
Forward security	Yes	Yes	Yes
Integrity attacking	Yes	Yes	Yes
Known key security	Yes	Yes	Yes
Prevent wiretap attacking	Yes	Yes	Yes
Prevent MITM attacking	–	Yes	Yes
Three-way handshake	–	–	Yes

4.5.3 Multi-path transmission security

Compared to single path transmission mechanism, multi-path transmission can effectively increase the difficulty of the attacker to obtain the complete data. After the server receives the data, the data packet can be compared with the message authentication code. If they are the same one, then the data will be added in the reorganization data packet, otherwise discarded , so as to ensure the correctness and security of the data received. Assuming the attacker has the ability to fake packets and the probability of intercepting a single packet is $P(0 < P < 1)$, for the single path mechanism and multi-path (n) mechanism, the probability of the loss and forgery of data packet is P and P^n, obviously $P^n < P$, and the security of multiplex transmission is ensured much more.

5 Distributed symmetric encryption cloud storage scheme

5.1 Distributed symmetric encryption cloud storage model

The Cloud storage server S_S is composed of the storage control center and the file system. After medical data generated by different systems and modules in CMIoT are transmitted to the server node, they firstly enter the storage buffer for unified processing of the control area in the storage module. The control center and the file system with a message queue exchange information through a message channel. If they communicate successfully and the current file system is free, the server can store the current data stream. Each file system independently enjoys and controls the communication link in order to achieve the purpose of distributed data storage.

As shown in Figure 5, at some point, there may be a large number of medical data to enter the storage server so that the control area can not handle them immediately. At this time, the server sends the data to the buffer storage buffer, and after the completion of the current data processing tasks in the control area, the data is extracted from the buffer and processed into the storage link. The control area immediately detects the current file system, and once the idle file system is detected, the control area will store in order the buffer data into the free file system through the message channel.

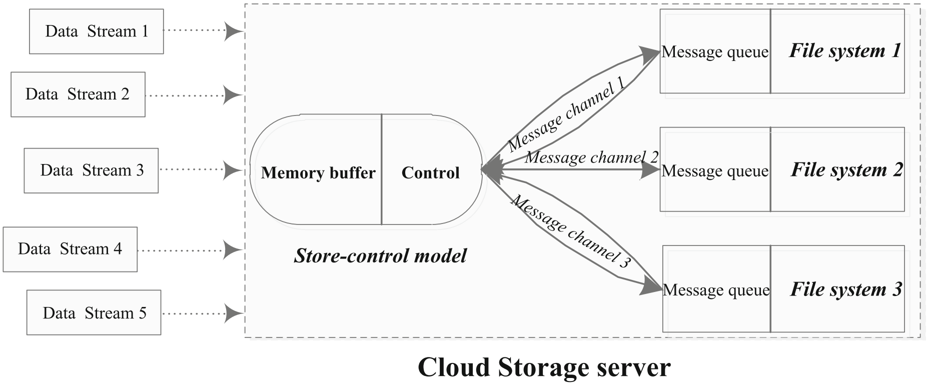

Figure 5 Storage server model

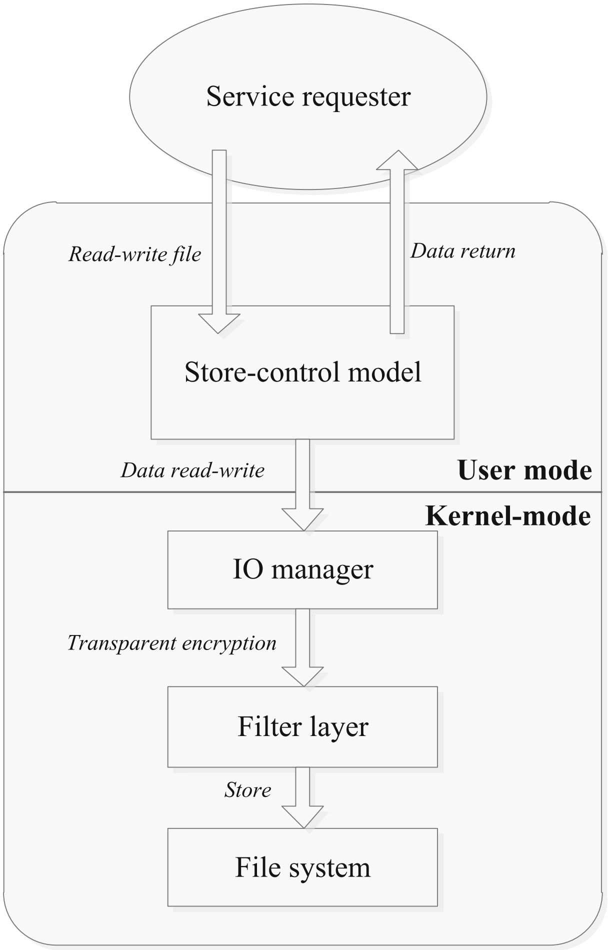

Figure 6 Server security storage model

For each data stream, that is a message M, before coming to the storage server, it is encrypted by the data source sender with the key K_{G-S}, and then the control area decrypts it. If the data stream after decryption is detected without finding illegal operations, the storage control area uses its own symmetric key to encrypt the data stream, and store it to the file system. The storage control area has a specific process to process data streams so that the data stream is stored safely to the specified file system. Figure 6 is the server security storage model.

5.2 Distributed symmetric encryption cloud storage scheme

After the storage server control area gets the data stream from the buffer, the server encrypts the data stream with some key, and then generates a new encrypted data packet. Using polling mode, the server queries whether the file system is idle or not, and stores the buffer data to the idle file system step by step.

Table 4 The symbol definitions of data package

No.	Name	Definition
1	Header	Header of data file
	$Data\_Sequence$	Sequence No. of data stream
	$Data\_FileNo$	File system No. of data stream
	$Data\_type$	Type of data stream
2	Body	Body of data file
	$Data_1$	Data body 1 of data stream
	$Data_2$	Data body 2 of data stream
	$Data_3$	Data body 3 of data stream
3	Remark	Remark
	$Data\_Length$	Length of data stream
	$Data\_En\_Alg$	Encryption algorithm

After the data stream enters the storage server, the control area of the storage server will decrypt the data packet for distributed storage. The data packet includes three parts such as $Header$, $Body$ and $Remark$ as shown in Table 4. Afterwards, the control area encrypt the packaged data with some key, and through the data channel established between the control area and the file system, using the data transmission mechanism based on transmission response, in other words, once the data transmission is interrupted, the data packet will be retransmitted, the control area stores all the data streams into distributed file systems as shown in Figure 7.

5.3 Storage security analysis

5.3.1 Data integrity

The scheme is provided with a control area module and a memory module in the storage server. The control area module is composed of a memory buffer and a control area. When

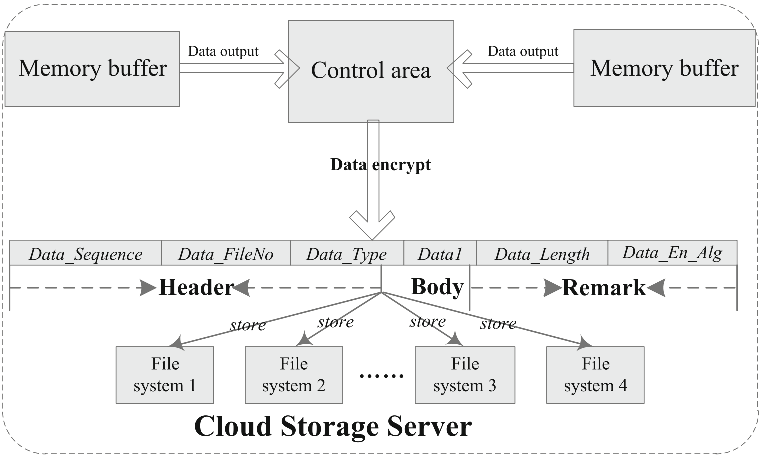

Figure 7 Process of server storage

data flows into a storage server, if the control area is processing some previous storage tasks, and unable to process incoming data stream in time, at this time the data stream will be stored in the memory buffer, so that the control area can complete the current tasks and turn to process current data storage. This ensures that a large amount of data can enter the storage server at the same time without being lost.

When the control area processes the new coming data streams, it will detect whether the storage modules of the file systems are idle or not, and once it finds a file system idle, it will transfer the data stream in a timely manner through the dedicated message channel.This avoids the situation that data can not be stored and may be lost due to unknowing whether the file system is busy or not, and the data integrity is guaranteed.

When the control area detects whether the file systems are idle or not, it will communicate with the file system in the form of a message queue. The communication channel between the control area and the file systems will not be blocked due to a lot of communication in a short time. It is very good to ensure the timely arrival of the feedback message and the integrity of the feedback information.

5.3.2 Data security

Before entering the storage server, the data stream is encrypted by the sender, and then the control area uses K_{G-S} to decrypt the data and verifies its integrity. After that, the data is encrypted with a symmetric key and stored into the corresponding file system. This ensures the security of data in the process of arriving at the server and the file systems.

When a data stream is stored in some distributed file systems, it is interacted between the user state and the kernel state. Therefore, data storage is completed with to I/O manager and processed by a transparent encryption method. Once the data in the user state is requested to access, the kernel will receive that request, conduct an access request processing by verifying the role properties and finally complete data transmission in a transparent decryption method. The whole data request and feedback process is transmitted through the data encryption method. This avoids data concentration and also can protect the security of data.

6 Access control with identity authentication and dynamic access authorization

In addition to the transmission encryption and fragmentation mechanism addressed in Section 4, in order to protect the security and integrity of the patient's medical privacy data storage, and share those data conveniently, it needs to dynamically manage the corresponding access to medical privacy data using hierarchical and dynamic authorization.In the open network environment, the access control of medical data mainly includes:

- Allow legitimate users (patients, doctors and nurses) to access their own data information;
- Prevent illegal users from illegally accessing to medical privacy data files;
- Prevent legitimate users from unauthorized access to other user's medical privacy data information;
- Share locally the medical privacy data, allow patients to understand their health status in a timely manner, allow health care workers to follow up the patient's condition, so as to promote the health and rapid development of the medical field.

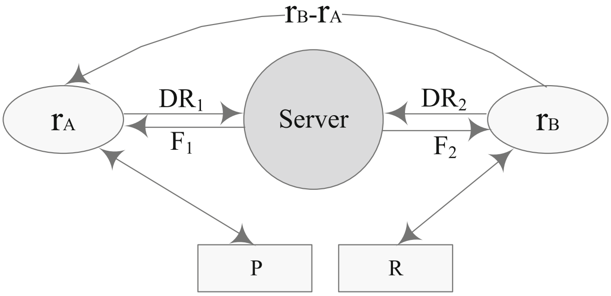

Figure 8 Abstract access control model

6.1 Fine grained access control model

By setting the user's security access policy for the medical privacy data, using the security and anti leak system in the open CMIoT Environment, the relationships among users, sensitive data and permissions can be customized flexibly, and the access authority to sensitive data can be managed dynamically. This involves several different types of access, e.g., normal access to medical privacy data by legitimate users, failure to access to sensitive data by illegal users, and limited access to subset of data by semi legal users authorized by legitimate users.

Figure 8 shows an abstract access control model for CMIoT, and some symbols are defined in Table 5, where medical data include text data of diagnosis and treatment , pathological documents, image files, etc., $r_i \rightarrow r_j$ represents that between two different users u_i and u_j, u_i in r_i authorizes u_j to access to the data which u_i can access, $t_i \rightsquigarrow t_j$ represents that between two different users u_i and u_j, u_i authorize u_j a time period from t_i to t_j to access to the data where u_i can access, and DR represents that when a user request to access to the data in the storage server, according to the set of user's roles and the set of access permissions, the server will determine whether the user data request is reasonable and whether or not to return the user data. Similar to [26], each user may be assigned one or more roles, and each role can be assigned one or more privileges that are permitted to users in the specified role.

In practical applications, the difference of users and the actual operating environment needs to be taken into account. Assuming that there are two patients, e.g. P_A and P_B, two doctors or nurses, e.g. D_A and D_B, P_a and P_B are treated in the medical institution where

Table 5 The symbol definitions of access model

No.	Symbol	Definition
1	$U = \{u_i \mid i = 1, 2, ..., m\}$	Set of users that can access to medical data
2	$R = \{r_j \mid j = 1, 2, ..., n\}$	Set of roles that can access to medical data
3	$F = \{f_i \mid i = 1, 2, ...n\}$	Set of types of data in the storage server
4	$P = \{p_i \mid i = 1, 2, ..., n\}$	Set of access permissions owned by a role
5	$A = \{r_i \rightarrow r_j \mid i, j = 1, 2, ...m\}$	Set of access authorizations between users
6	$T = \{t_i \rightsquigarrow t_j \mid i, j = 1, 2, ..., m\}$	Set of authorized time between users
7	$DR = \{dr_i \mid i = 1, 2, ..., n\}$	Set of data requests

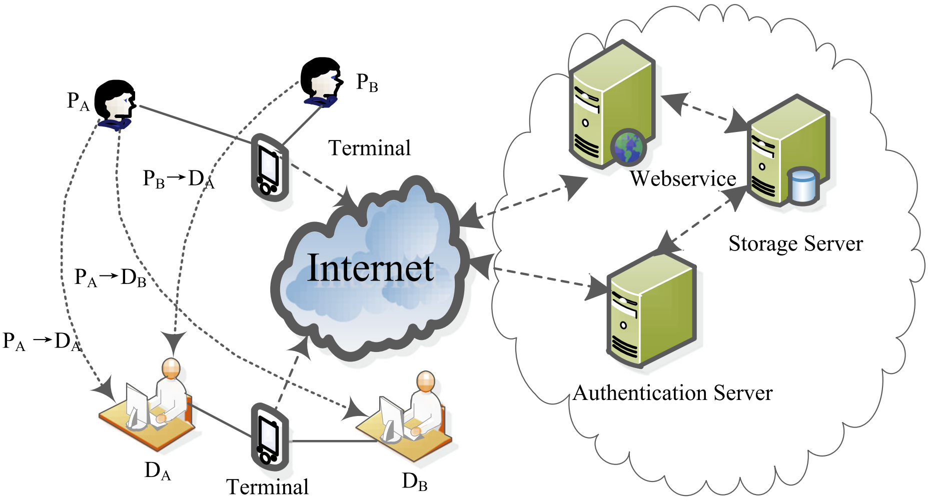

Figure 9 Fine grained access control model

D_A and D_B works, and D_A and D_B are responsible for the two patients' condition tracking and nursing. As users in CMIoT, patients, doctors and nurses send their data access request of medical data to the storage server with mobile terminals or PC terminals, and the storage server verifies the legitimacy of request and return data if legal. Figure 9 shows the data access methods and authorizations of patients, doctors and nurses. P_A sends his or her data request to the storage server with terminals so as to access personal basic information and medical data from the storage server. P_A can also authorize D_A and D_B to the medical data of P_A. The authorization between patients and doctors is a multi to multi mode. A patient may authorize a number of doctors or nurses for medical data access and disease tracking, and a doctor or nurse can also accept more than one patient's authorization at the same time. The authorization has an authorization cycle. Once the authorization expires, the doctor or nurse will not be able to view the patient's medical data.

6.2 Access control scheme

In the cloud storage environment of CMIoT, the access control policy of medical privacy data mainly includes

- After a patient logins the cloud storage server, he or she may view his or her own medical data , i.e. personal information, medical data, electronic medical record, PACS image information.
- After a doctor or nurse logins the cloud server, he or she can view their own account information and track the patient's medical data. Under normal circumstances, he or she can only can manage his or her own personal data without no right to access a patient's medical data. Once the patient authorizes an access permission to a doctor or nurse by the authorization code, the doctor or nurse can view and track the medical data of the patient through his or her own account in a certain authorization period.

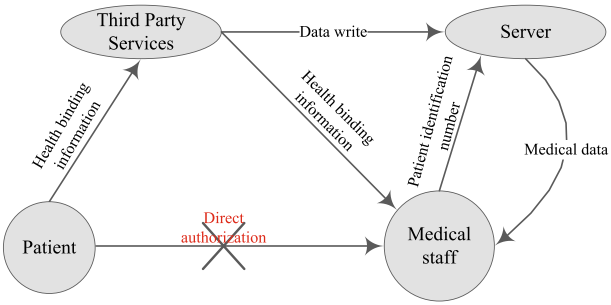

Figure 10 Dynamic authorization

When medical data is accessed by different users, the cloud storage server will verify the user's permissions according to the user's role and return the corresponding data to the user according to the data request. This can be implemented through dynamic authorization as shown in Figure 10. At the authorization stage, in order to ensure safety, patients are not allowed to directly authorize the access permission to medical staff. Role and permission are bound as the patient authorization data to be written to the server through the third party data platform, and is sent to medical staff so that he or she can access to the cloud storage server according to the role and permission.

During medical data access, different roles have different access permissions. However, a role can provide other role the access permission through dynamic authorization. Assuming that a patient has a role 1, a nurse has a role 2, a doctor has a role 3, the patient in role 1 has the permission of direct access to his or her own medical data and the nurse can not access directly to those data. That means that the nurse need an authorization. Likewise, the doctor also needs to be authorized. Therefore, the patient can authorize the role 1 to the role 2 and the role 3 so that the nurse and the doctor has the same permissions as the patient as shown in Figure 11.

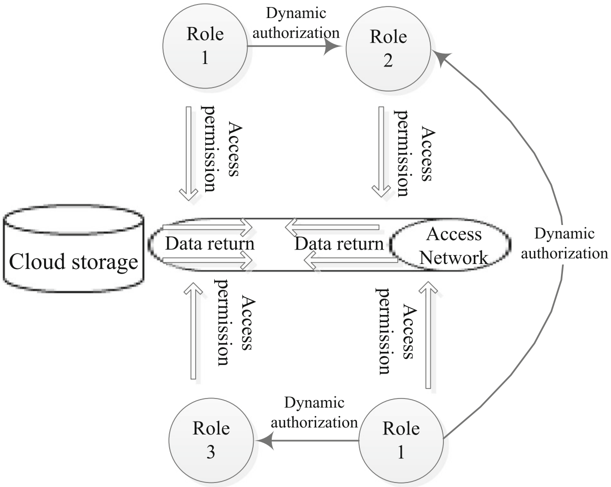

Figure 11 Access control process

The mechanism provides convenience for medical staff in a certain period of time, and makes the unauthorized medical staff can not view the patient data so as to avoid the risk of patient medical data theft. This greatly protect the privacy of the patient's medical data in two aspects. one is operation permission control of medical privacy data file. Different levels of users have different permissions for different sensitive data files. another one is dynamic management of user access permissions. In case that a doctor is authorized by a patient, he or she can access the patient's electronic medical record, the history of medical information and image information, etc.

6.3 Access control security analysis

The above access control scheme reaches the following effects:

- Users can access to the cloud storage server and query personal information through their own user name and password. This can prevent illegal users from entering the server to steal data.
- Legitimate users can log on the cloud server to view personal information and cannot access non self data. This can prevent illegal users from abnormal access.
- Through the dynamic authorization mechanism, patients can register an authorization code on the medical data so that once some medical staff has the same authorization code, he or she can access those data within the effective time limit.

7 Experiment and simulation

In CMIoT, some medical sensors and devices are deployed indoors at home, and some ones are deployed public area such as community public area, community health center or hospital. In our test, they gather some information about people's medical data including blood pressure, blood oxygen, blood glucose, heart rate ,ECG (Electrocardiograph) data and so on $n \geq 10$ times each day. After packaging those data, the gateway will split them into some fragments and send them to different wireless routers so that the latter can transmit them father to the cloud storage server in the community health center with the wireless communication link. In the meantime, users such as patients, doctors, nurses, managers and so on can access to the medical data in the cloud storage server given in a specified role with some specified permissions.

7.1 Security

According to the security analysis, the data packet will be transmitted to the gateway node after authenticating between server node and gateway node. Assuming that the probability of data stolen in single-path transmission is $P(0 < P < 1)$, the probability in multi-path transmission is P^n, where n presents the number of paths. For ease of comparison, we assume that $P \geq 0.7$ and $n \leq 14$, then, the simulation results are shown in in Figures 12 and 13.

Under three different packet loss rates, when there is only one transmission path, the packet loss rate will not change. When the number of paths increases, the total packet loss rate decreases with the increase of the number of paths. This shows that the packets got by attackers account for a smaller proportion of the total data packets, the risk of information leakage caused by data packet loss is much smaller, and the safety factor is much higher.

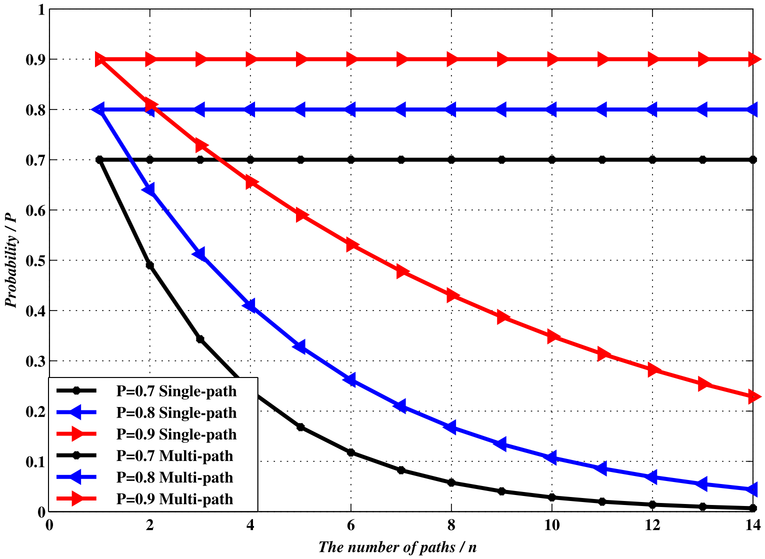

Figure 12 Packet loss rate

7.2 Reliability

Assuming as follows:

- The length of the communication link from the terminal node to the server node is L, and there are k unreliable nodes, then we conclude that the probability of effective node is $P = 1 - k/L$.
- The terminal node and the server node locate in the position 0 and $L + 1$, and the reliability of the information is R.
- $A(1 \leq x \leq L - k)$ represents that the x_{th} node in the communication link is the first unreliable node.
- A' represents that the first unreliable node is the x_{th} node or the former node.
- $P(x)$ represents the probability that the first unreliable node locates at the x_{th} node in the communication link.
- B represents that the identity of the sender is guessed correctly by the first unreliable.
- $P(B \mid A'_B)$ represents the probability that the unreliable node correctly infers the message sender.

According to the assumptions above, the probability that the first unreliable node locates at the x_{th} node in the communication link is

$$P(A_x) = p^{(x-1)}(1 - p) \tag{19}$$

Then the probability that the first unreliable node locates at 1^{st} or latter node is

$$P(A'_1) = (1 - p) \sum_{i=1}^{L-k} p^{i-1} = 1 - p^{L-k} \tag{20}$$

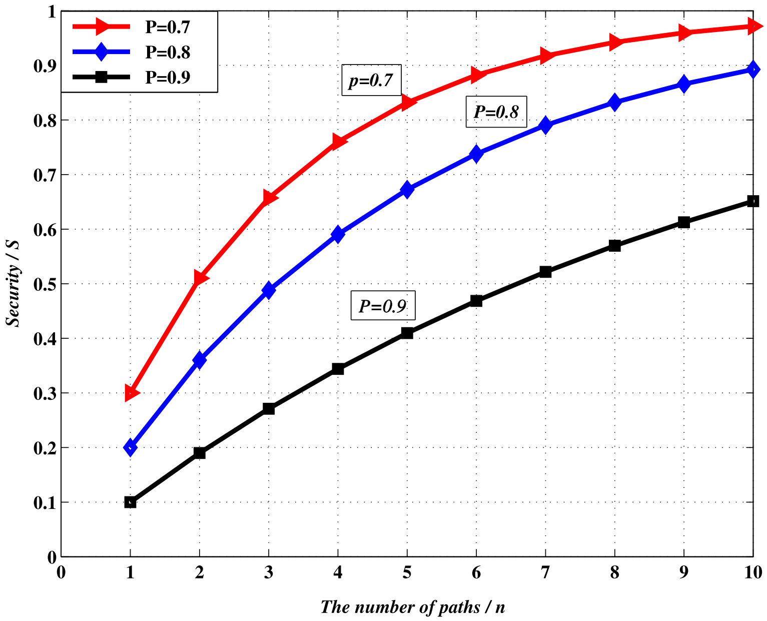

Figure 13 Security of communication link

Therefore we can conclude:

$$P(B \mid A_1') = \frac{1-p}{1-p^{L-k}} \tag{21}$$

We also can assume as follows:

- $LA_x(k \leq x \leq L)$ represents that the last unreliable node locates at the x^{th} node in the communication link.
- LA_x' represents that the last unreliable node locates at the x_{th} node or the latter node.
- $P_{l(x)}$ represents that probability that the last unreliable node locates at the x_{th} node in the communication link.
- B_l represents that the identity of the receiver is inferred correctly by the last unreliable node.
- $P_l(B \mid A_B')$ represents the probability that the unreliable node infers the identity of the receiver correctly.

According to the assumptions above, the probability that the last unreliable node locates at the x_{th} node in the communication link is

$$P(A_x) = (1-p)p^{L-x} \tag{22}$$

The probability that the last unreliable node locates at the n_{th} node or the latter node is

$$P(A_n^i) = (1-p)\sum_{j=k}^{L} p^{L-j} \tag{23}$$

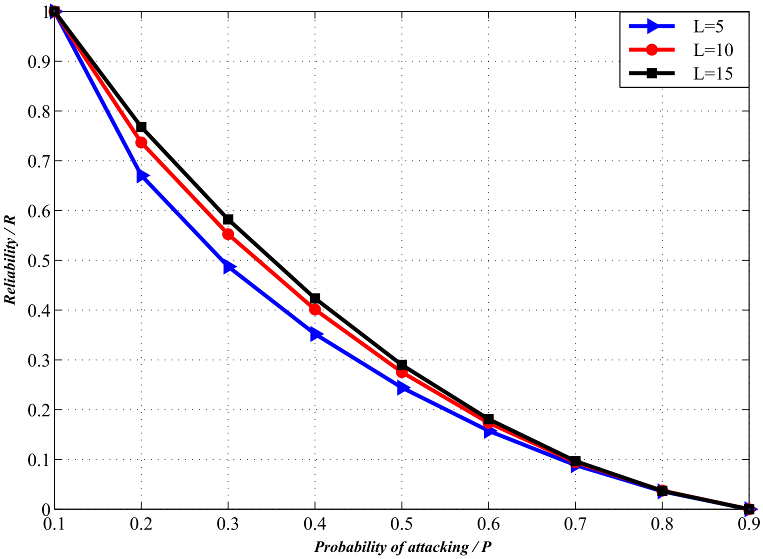

Figure 14 Reliability of communication link

Therefore we can also conclude

$$P(B_l \mid A'_n) = \frac{1-p}{1-p^{L-k+1}} \tag{24}$$

To sum up, we can get that the reliability of the communication link is

$$\begin{aligned} R &= P(B \mid A'_q) \times P(B_l \mid A'_n) \\ &= \frac{(1-p)^2}{(1-p^{L-k})\times(1-p^{L-k+1})} \end{aligned} \tag{25}$$

In order to reflect more directly the influence of the reliability about data transmitting with the impact of the length of the communication link and the probability of the node which is attacked, we have a simulation as shown in Figure 14. It indicates that the reliability decreases with the increase of the probability p of the unreliable nodes and the communication link length L. When p does not change, the greater L, the greater R, and this is in line with the actual situation. Therefore, during data transmission, under the situation that the length of the communication link is as small as possible, the multi-path transmission is more secure.

8 Conclusions and future works

In this paper, we design an infrastructure framework on transmission protection, storage protection, and access control for CMIoT. Firstly we takes the CMIoT as a standpoint, and aims at the privacy data protection. For the transmission protection, we summarize upon three aspects, authentication, communication key agreement and multi-path security transmission. Considering of the security problems that might exist in the communication process, we improve the traditional key agreement algorithm to enhance the key negotiation security. Furthermore, we increase the multi-path transmission mechanism to become more difficult for attacker to obtain complete data without affecting server data receiving. Finally, we analysis the security about the method inferred to the full text. Our second contribution is to present a safe medical data storage model and method in the cloud storage server. The server receives medical data through a server buffer, its control area is responsible for data processing and storage ,then decrypts uploaded medical data, and finally stores the data to the storage database through the key encryption and the transparent encryption method. In order to ensure the security of medical data in the cloud storage server, an access control method with authorization is used. This scheme provides a secure access to the cloud storage server through login authentication and access authorization for protecting the privacy of patients' medical data, isolation of access to patient data of medical staff who does not participate in the diagnosis of disease and controlling the access period of authorized doctor and nurse by the time of authorization. However, we do not consider the multiple identity of medical staff, i.e., if the medical staff also is a real patient, whether it can be as common as the operation of medical privacy data. Another issue is to study the mechanism of efficient key generation, distribution and recovery.

Acknowledgements This work was supported in part by the National Natural Science Foundation of China[No.61572036, No.61672039 and No.61402014], Anhui Province University Outstanding Youth Talent Support Program [No.gxyqZD2016026] and Anhui Provincial Natural Science Foundation [No.1708085MF156].

References

1. Ateniese, G., Fu, K., Green, M., et al.: Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans. Inf. Syst. Secur. **9**(1), 29–43 (2006)
2. Beato, F., Meul, S., Preneel, B.: Practical identity-based private sharing for online social networks. Comput. Commun. **73**, 243–250 (2016)
3. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy (2007)
4. Chen, M., Qian, Y., Mao, S., et al.: Software-defined mobile networks security. Mob. Netw. Appl. **21**(5), 729–743 (2016)
5. Ding, Z., Li, J., Bo, F.: Research on hash-based RFID security authentication protocol. J. Comput. Res. Dev. **46**(4), 583–592 (2009)
6. Du, W., Deng, J., Han, Y.S., et al.: A pairwise key pre-distribution scheme for wireless sensor networks. In: Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 42–51 (2003)
7. Forsstrom, S., Kanter, T., Osterberg, P.: Ubiquitous secure interactions with intelligent artifacts on the internet-of-things. In: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (Trustcom), pp. 1520–1524 (2012)
8. Groce, A., Katz, J.: A new framework for efficient password-based authenticated key exchange. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, pp. 516–525 (2010)
9. Hong, Z.Z.: Research on electronic health records of community residents Fudan University (2008)
10. Hou, Q.H., Wu, Y.W., Zheng, W.M.: A method on protection of user data privacy in cloud storage platform. J. Comput. Res. Dev. **48**(7), 1146–1154 (2011)
11. Huang, R.W., Gui, X.L., Yu, S., et al.: Privacy-preserving computable encryption scheme of cloud computing. Chinese J. Comput. **34**(12), 2391–2402 (2011)
12. Hwang, J.J., Yeh, T.C.: Improvement on Peyravian-Zunics password authentication schemes. IEICE Trans. Commun. **85**(4), 823–825 (2002)

13. Jing, Q., Vasilakos, A., Wan, J., Lu, J., Qiu, D.: Security of the internet of things: perspectives and challenges. Wirel. Netw. **20**(8), 2481–2501 (2014)
14. Kamara, S., Lauter, K.: Cryptographic cloud storage. In: Proceedings of the 14th International Conference on Financial Cryptograpy and Data Security, pp. 136–149 (2010)
15. Kothmayr, T., Schmitt, C., Hu, W., et al.: A DTLS based end-to-end security architecture for the internet of things with two-way authentication. In: IEEE 37th Conference on Local Computer Networks Workshops, pp. 956–963 (2012)
16. Lamport, L.: Password authentication with insecure communication. Commun. ACM **24**(11), 770–772 (1981)
17. Ma, W.J.: Research and application on security authentication technologies in internet of things Shandong University (2011)
18. Maeda, T., Sato, K., Muraoka, Y., et al.: RFID System and RFID tag. U.S. Patent 8274367 (2012)
19. Mao, J., Li, K., Xu, X.: Privacy protection scheme for cloud computing. Journal of Tsinghua University (Sci & Tech) **51**(10), 1357–1362 (2011)
20. Ning, H.S., Xu, Q.Y.: Research on global internet of things developments and its lonstruction in China. Acta Electronica Sinica **38**(11), 2590–2599 (2010)
21. Peyravian, M., Jeffries, C.: Secure remote user access over insecure networks. Comput. Commun. **29**(5), 660C667 (2006)
22. Pirretti, M., Traynor, P., McDaniel, P., et al.: Secure atrributebased systems. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 99–112 (2006)
23. Song, Z., Zhang, Y., Wu, C.: A reliable transmission scheme for security and protection system based on internet of things. In: IET International Conference on Communication Technology & Application, pp. 806–810 (2011)
24. Venkatasubramanian, K.K., Banerjee, A., Gupta, S.K.S.: PSKA: Usable and secure key agreement scheme for body area networks. IEEE Trans. Inf. Technol. Biomed. **14**(1), 60–68 (2010). A Publication of the IEEE Engineering in Medicine & Biology Society
25. Vimercati, S., Foresti, S., Jajodia, S., et al.: Over-encryption: management of access control evolution on outsourced data. In: Proceedings of the 33rd International Conference on Very Large Data Base, pp. 123–134 (2007)
26. Wang, H., Cao, J., Zhang, Y.: A flexible payment scheme and its role-based access control. IEEE Trans. Knowl. Data Eng. **17**(3), 425–436 (2005)
27. Wang, B., Zhang, H., Wang, Z., et al.: A secure mutual password authentication scheme with user anonymity. Geomatics & Information Science of Wuhan University **33**(10), 1073–1075 (2008)
28. Wang, W., Li, Z., Owens, R., et al.: Secure and efficient access to outsourced data. In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, pp. 55–66 (2009)
29. Wu, C.K.: An overview on the security techniques and challenges of the internet of things. Journal of Cryptologic Research **2**(1), 40–53 (2015)
30. Wu, Z.Q., Zhou, Y.W., Ma, J.F.: A secure transmission model for internet of things. Chinese J. Comput. **34**(8), 1351–1364 (2011)
31. Xie, W.J.: A secure communication scheme based on multipath transportation for the internet of things South China University of Technology (2013)
32. Yong-Hong, Y.U., Bai, W.Y.: Enforcing data privacy and user privacy over outsourced database service. Application Research of Computers **6**(3), 404–412 (2011)
33. Yu, S., Wang, C., Ren, K., et al.: Achieving secure, scalable, and fine-grained data access control in cloud computing. Proc. - IEEE INFOCOM **29**(16), 1–9 (2010)
34. Yuen, T.H., Chow, S.S.M., Zhang, Y., et al.: Identity-based encryption resilient to continual auxiliary leakage. In: Proceedings of the 31st Annual International Conference on Theory and Applications of Cryptographic Techniques, pp. 117–134 (2012)
35. Zhang, F.Z., Chen, J., Chen, H.B., et al.: Lifetime privacy and self-destruction of data in the cloud. J. Comput. Res. Dev. **48**(7), 1155–1167 (2011)
36. Zhang, J., Li, H., Liu, X., et al.: On efficient and robust anonymization for privacy protection on massive streaming categorical information. IEEE Trans. Dependable Secure Comput. doi:10.1109/TDSC.2015.2483503 (2015)
37. Zhang, Y., Shen, Y., Wang, H., Zhang, Y., Jiang, X.: On secure wireless communications for service oriented computing. IEEE Trans. Serv. Comput. doi:10.1109/TSC.2015.2478453 (2015)
38. Zhang, Y., Shen, Y., Wang, H., Yong, J., Jiang, X.: On secure wireless communications for IoT under eavesdropper collusion. IEEE Trans. Autom. Sci. Eng. **13**(3), 1281–1293 (2016)