Hindawi
Journal of Sensors
Volume 2017, Article ID 7862842, 14 pages
https://doi.org/10.1155/2017/7862842

Research Article

Data Transmission and Access Protection of Community Medical Internet of Things

Xunbao Wang,[1] Fulong Chen,[2] Heping Ye,[2] Jie Yang,[2] Junru Zhu,[2] Ziyang Zhang,[2] and Yakun Huang[2]

[1] *Department of Information Service, Anhui Institute of International Business, Hefei, Anhui 230000, China*
[2] *Engineering Technology Research Center of Network and Information Security, Anhui Normal University, Wuhu, Anhui 241002, China*

Correspondence should be addressed to Fulong Chen; chenfulong@gmail.com

Received 9 October 2016; Revised 8 January 2017; Accepted 12 February 2017; Published 13 April 2017

Academic Editor: Wei Li

On the basis of Internet of Things (IoT) technologies, Community Medical Internet of Things (CMIoT) is a new medical information system and generates massive multiple types of medical data which contain all kinds of user identity data, various types of medical data, and other sensitive information. To effectively protect users' privacy, we propose a secure privacy data protection scheme including transmission protection and access control. For the uplink transmission data protection, bidirectional identity authentication and fragmented multipath data transmission are used, and for the downlink data protection, fine grained access control and dynamic authorization are used. Through theoretical analysis and experiment evaluation, it is proved that the community medical data can be effectively protected in the transmission and access process without high performance loss.

1. Introduction

The rapid economic development has led to the deterioration of the natural environment upon which the survival of people's health is under unprecedented threat. Various non-predictability diseases have sprung up on patients. Therefore, the demands on medical services are also growing rapidly. However, limited traditional medical service resources and uncertainty treatment time urge people to begin to look for better health services to make up for the lacking of available medical resources.

Paper [1] addressed a cardiac function in real-time monitoring system that can measure heart rate and other vital sign data and serve data to the medical center for treatment via Bluetooth or wireless networking technologies. Zhang et al. mentioned that obtaining data by remote sleeping monitoring could effectively help doctors diagnose disease and adjust the pillow without affecting sleep [2]. Chen et al.'s AIWAC [3], Zhang et al.'s iDoctor [4], and Wan et al.'s Healthcare [5–7] are also some typical application cases of "smart healthcare" using Internet of Things (IoT) technologies. As a specific "smart healthcare" implementation, Community Medical Internet of Things (CMIoT) is a kind of Internet of Things (IoT) application in the medical field.

In CMIoT, due to the huge amount of heterogeneous medical data, extensive medical data sources, and various identification information which involves user privacy, once medical data are lost or tampered, some privacy leakages resulting in catastrophic loss will occur. How to ensure the security of such data has been always the focus of academic research. Mni proposed that today's medical development should take a new information technology way. He pointed out the key technologies in the medical field and analyzed and presented various models about medical data from generation to storage [8]. Chen et al. [9] and Jing et al. [10] also addressed some relevant security threats and their corresponding countermeasures in wireless communication networks.

In the study of the security of IoTs, we must take into account the particularity of CMIoT. In CMIoT, the uplink data transmission occurs between the server and the medical sensors, and the interaction behavior involving the downlink data transmission takes place between the server and the terminals. An important feature is that the data amount is huge and relatively concentrated. And the data are very relevant to users. There is no complete and feasible method to ensure data security of CMIoT. Therefore, in order to protect the uplink and downlink data, we propose a secure privacy data protection method for CMIoT in two ways including transmission protection and access control. The rest of this paper is organized as follows. Section 2 discusses some related works. Section 3 describes the architecture of CMIoT. Data transmission protection and access control in CMIoT are introduced in Sections 4 and 5. Section 6 presents some experimental results. The last section concludes the paper and lays out future research issues.

2. Related Works

Since the concept of IoT is proposed, some scholars have tried to design its security privacy protection methods. Encryption is a common way of privacy protection. Popular encryption methods, for example, DES and RSA, 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 and Xu [15] considered a variety of secure factors of IoT and believed that there would be a trade between privacy strength and specific business needs. Namely, it needs us to customize privacy policies 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 proposes a safe way Hash function. After that, Ding et al. [17] proposed a kind of authentication protocol based on Hash function. Maeda et al. [18] proposed two schemes based on reencryption in which one is to use the reencryption authentication to prevent location privacy from leaks, and another is to use a one-time reencryption to make RFID tags anonymous. Wu et al. [19] 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. Song et al. [20] studied the secure and reliable transmission scheme SPS based on IoT. They presented a cooperative transmission mechanism and the rate selection algorithm based on the channel state in order to transmit data effectively and reliably.

A secure transmission method which would be fit on the IoT has been mentioned in [14]. 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 IoT model, there is a common problem in the application; for example, a variety of mixed-format electronic medical records and other patient data in CMIoT are involved. However, the methods which we have discussed above cannot fit the field. When the data are transferred or accessed, data attacking and data leaking will cause our privacy information to be illegally obtained.

Taking into account the special natures of CMIoT, in [21], the 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 [22] proposed a very effective protection scheme for electronic health records based on SOA with SSL, WS-Security, and personal access control technology. Venkatasubramanian et al. [23] proposed a key agreement PSKA based on physiological signal information and provided a guarantee for secure communication between nodes in wireless body area network.

2.2. Transmission Protection. In CMIoT, data is mostly transmitted through wireless communication and is easier to be intercepted. Both Atzori et al. [24] and Medaglia and Serbanati [25] mentioned that the tag carried by the user is scanned by the reader without being aware of it and extremely easy to cause personal privacy leak. The information is easy to be attacked when it is transferred between the local server and the remote server. In view of the limited capacity of the sensor or communication system, the method of data privacy protection is mostly based on the lightweight encryption algorithm [26]. Du et al. [27] 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. About authentication before transmission, some schemes, for example, Hwang and Yeh's [11] two-way authentication scheme between nodes, Peyravian and Jeffries's [12] authentication scheme based on Hash function, Wang et al.'s [13] two-way anonymous password authentication scheme, and Kothmayr et al.'s [28] 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 they are vulnerable to middle attacks. Groce and Katz [29] studied and proposed a protocol that could be proved to be secure in the general model, and however there was no assumption of a trusted third party and the protocol was not universal. Forsström et al. [30] studied the security issues of intelligent terminals in the IoT through a variety of heterogeneous network architectures, and a distributed verification system based on MediaSense platform was proposed to ensure the security of the communication between smart terminals. Unfortunately, for all these IoT security transmission models, there are some problems in their application, for example, many kinds of mixed-format data including users' electronic medical record and so on in CMIoT. In our previous paper [31], a kind of simple secure fragmented multipath data transmission model was addressed.

2.3. Access Control. As a kind of storage media which cannot be controlled by users, cloud storage access needs to be ensured legally. In CMIoT, a large number of diagnostic data of patients are generated each day and stored in the cloud server so that the access control faces new challenges. Users such as patients, doctors, and nurses can use mobile terminals for personal medical data queries 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 will not disclose patients' privacy data. Access control mechanism can authorize legitimate users to access specific resources while denying access of illegal users. The authorization methods are 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 et al. [32] 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 permissions cannot be revoked. On the basis of the attribute-based scheme, Bethencourt et al. [33] 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 the attribute set related to user's identity. ABE cipher-text access control was addressed in [34] using dynamic changed strategies, and however the execution efficiency is not high and the cost of a single execution is very large. Yuen et al. [35] proposed the identity as the encryption base for encrypting users to resist information leakage, and Beato et al. [36] 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.

In the study of the security of IoTs, we must take into account the particularity of CMIoT. In CMIoT, the uplink data transmission occurs between the server and the medical sensors, and the interaction behavior involving the downlink data transmission takes place between the server and the terminals. An important feature is that the data amount is huge and relatively concentrated. And the data are very relevant to users. There is no complete and feasible method to ensure the data security of CMIoT.

3. Architecture of Community Medical Internet of Things

Similar to general IoT application systems, as shown in Figure 1, the hierarchical structure of CMIot has four layers: sensing/executing layer, data transmission layer, information integration layer, and application system layer.

The CMIoT is achieved in one community, as shown in Figure 2. In the CMIoT, all medical data are collected by the medical sensors, for example, RFID reader, blood pressure sensor, blood oxygen sensor, blood glucose sensor, heart rate sensor, ECG sensor, and camera, which belong to some place such as home, community public area, community health center, or hospital. These sensor nodes and some mesh nodes work in the low-power ZigBee transmission mode and form a wireless sensor network (WSN).

When a person needs to collect his or her sign data, the identity data in the RFID card can be read by the RFID reader, and the medical data can be collected by the medical sensors. These data are sent to the mesh node connected with the RFID read and medical sensors. Then, the mesh node encapsulates them together and, after security processing, sends them toward the nearest other mesh node or gateway. The gateway is network protocol conversion node which can convert ZigBee mode to WiFi mode. It transmits the medical data to the nearest community routers. The communication link is built among the mesh nodes, gateway node, router nodes, and the database server of cloud data center through wireless network. In the end, the application server of data center provides the resolved data to users with mobile terminals or PC terminals. Data transmission integrates a variety of communication means. Sensors in one place establish the local communication via wireless self-organized network, and data in the gateway are transmitted through wireless wide area network or mobile network.

4. Data Transmission Protection

4.1. Symbol Definition and Multipath Transmission Model. Using slice model, medical data are transferred in split fragments through multiple paths as shown in Figure 3. The data transmission from sensors to cloud storage is a complicated process. As shown in Notations, some data transmission symbols are defined and will be used in Figure 3.

4.2. Region Network Initialization. Before the medical data are transmitted, the CMIoT needs to complete some initial operations including networking, registration, and bidirectional authentication.

(i) Networking. It happens in the ZigBee wireless sensor network of one place. According to the mesh network architecture, the sensor nodes and sink nodes form a regional WSN. As shown in Figure 3, the sensor nodes s_1 and s_2 connect with the sink node N_1, and the sink nodes N_1, N_2, N_3 are interconnected. Otherwise, N_2 and N_3 also connect with the gateway node G which is a protocol conversion gateway for converting ZigBee mode to WiFi mode. Therefore, the region network is a regional ZigBee WSN composed of some nodes

$$\mathrm{WSN} = \left\{s_i\right\} \cup \left\{N_j\right\} \cup \{G\}, \tag{1}$$

where $\{s_i\}$ are senor nodes, $\{N_j\}$ are sink nodes, and G is a gateway node.

(ii) Node Registration. When G registers at the server node S, G delivers the Hash value of password PW_G to S, and then S contrasts it to the password dictionary for authentication. Many gateway nodes' passwords constitute a password dictionary.

(iii) Bidirectional Authentication. In order to guarantee the authenticity of the gateway node and server node, the CMIoT

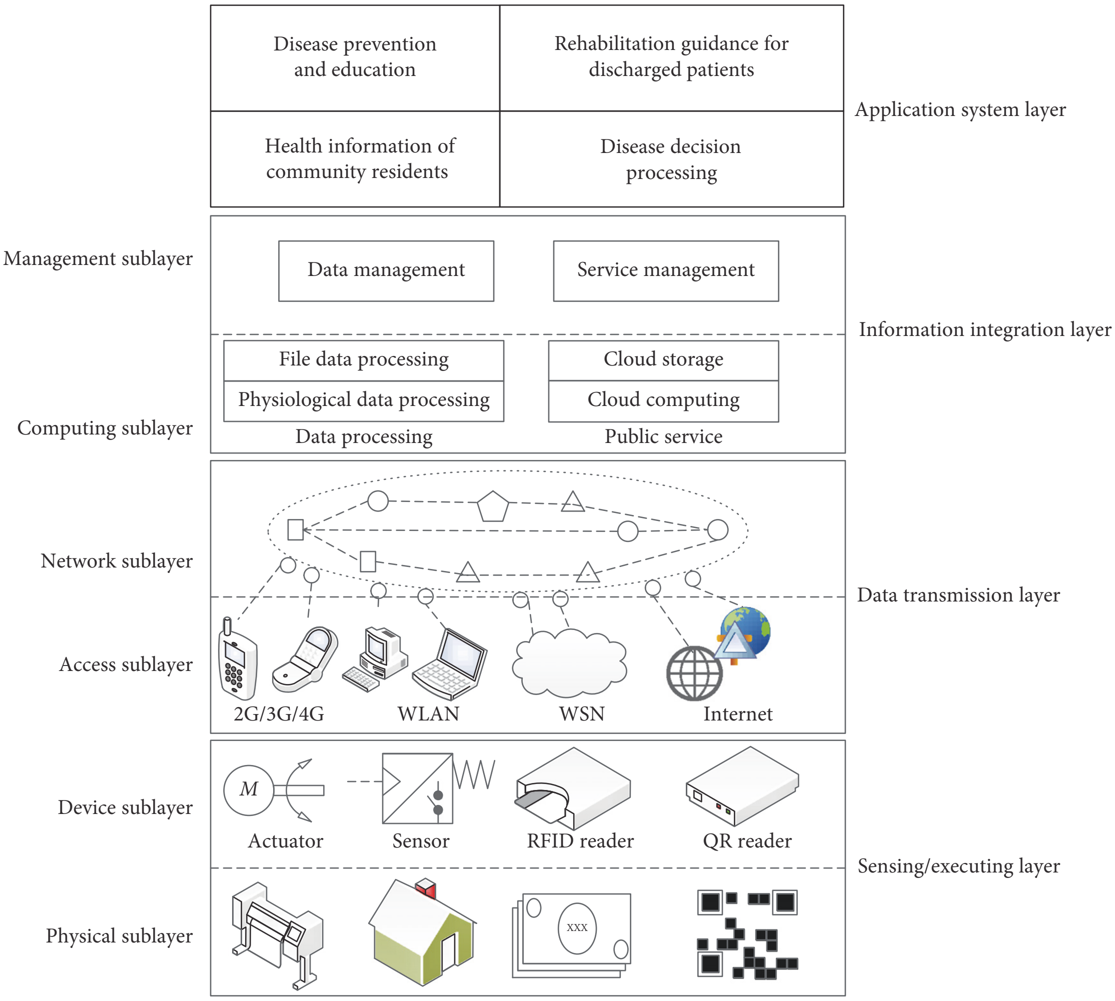


Figure 1: Hierarchical structure of community medical Internet of Things.

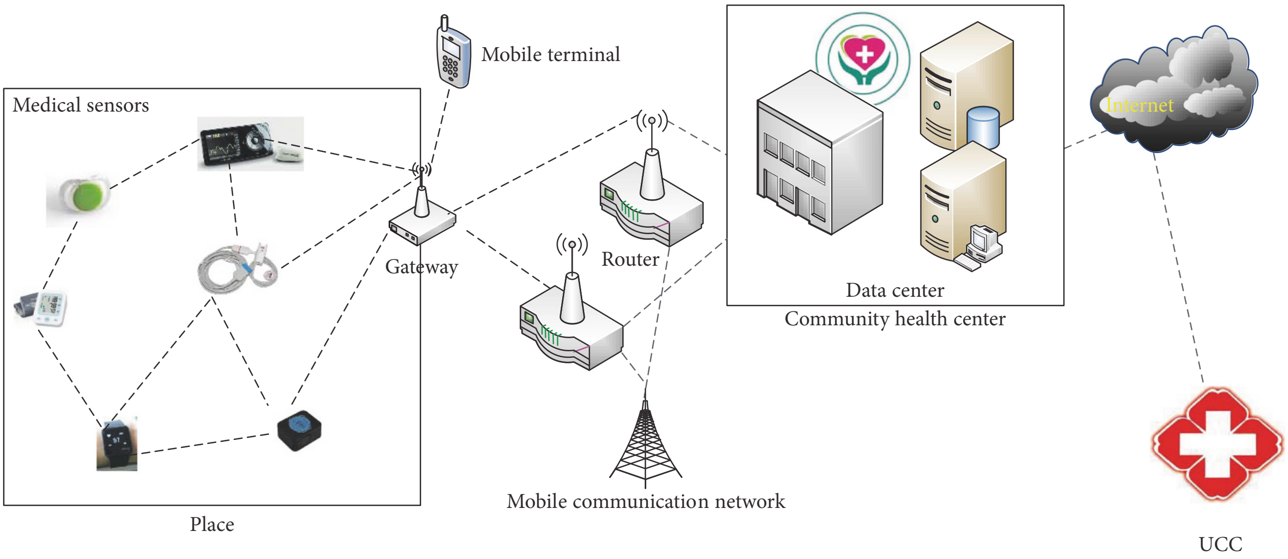


Figure 2: Composition structure of community medical Internet of Things.

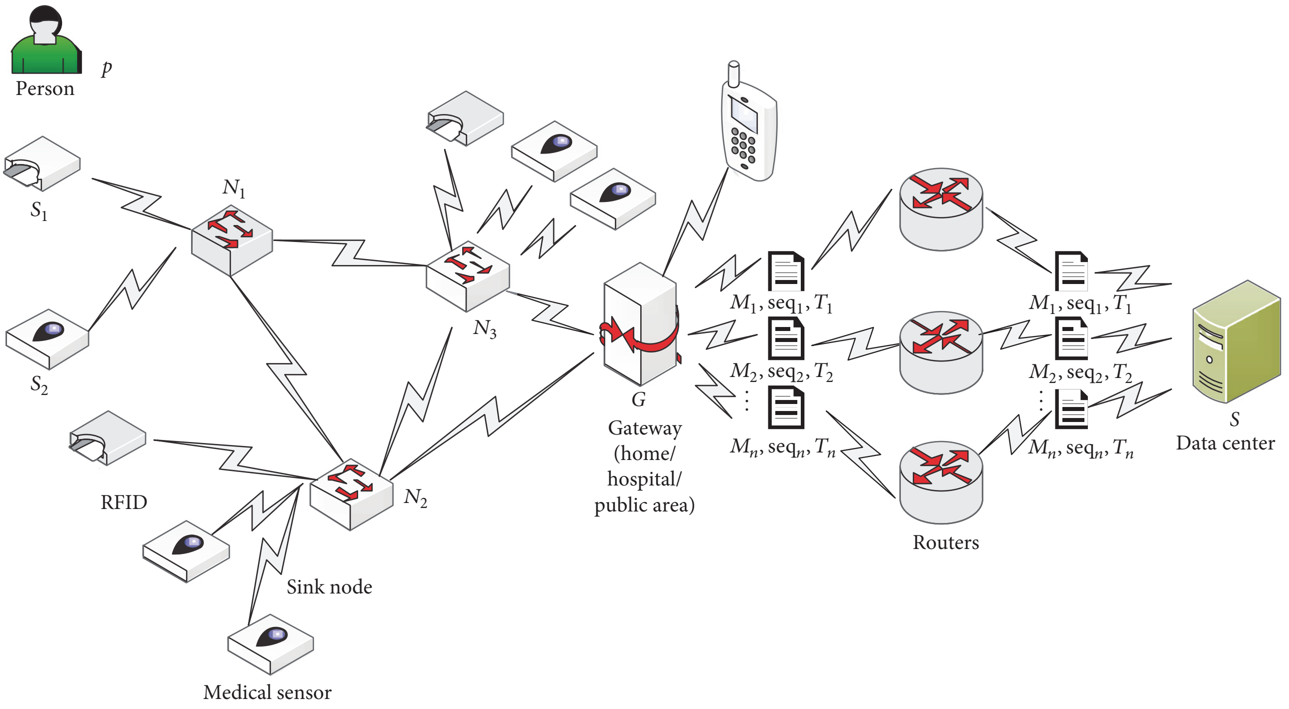


Figure 3: Multipath transmission model of medical data.

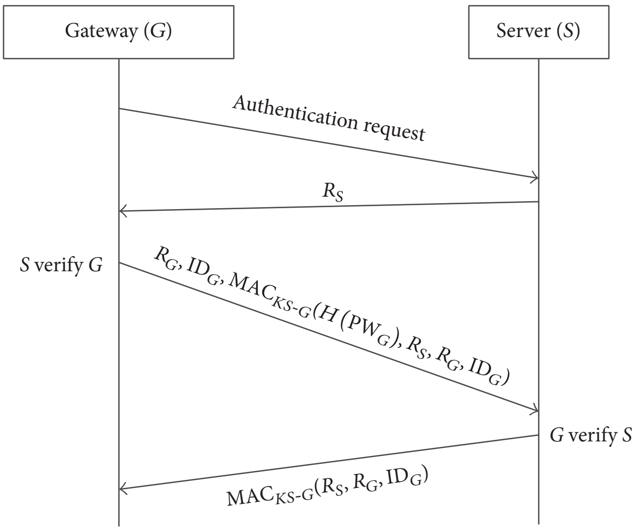

Gateway (G)
Server (S)
Authentication request
R_S
S verify G
R_G, ID_G, $MAC_{KS\text{-}G}(H(PW_G), R_S, R_G, ID_G)$
G verify S
$MAC_{KS\text{-}G}(R_S, R_G, ID_G)$

Figure 4: Authentication process.

needs to set up Bidirectional Authentication (BDA) between G and S, as shown in Figure 4.

(iv) Key Agreement. S and G negotiate and generate a symmetric key $K_{S\text{-}G}$ according to the key agreement mechanism, and both of them securely store $K_{S\text{-}G}$ so that they can encrypt and decrypt the important transmission data later.

4.3. Key Agreement Mechanism.

After completing the bidirectional authentication between G and S, they need to generate a shared key. This happens when the gateway is restarted. The key generation process in the key agreement mechanism (KAM) is elaborated as follows.

Step 1. A large prime number P is selected by G and S, and g is selected as a generator for the multiplicative group Z_P^*.

Step 2. G chooses a secret integer x,

$$1 \leq x \leq P - 2, \tag{2}$$

and calculates

$$X = g^x \bmod P, \tag{3}$$

and sends X to S.

Step 3. S selects a secret integer y,

$$1 \leq y \leq P - 2, \tag{4}$$

and calculates

$$Y = g^y \bmod P, \tag{5}$$

and sends Y to G.

Step 4. G calculates

$$K_G = Y^x \bmod P, \tag{6}$$

generates a random number R_G, and sends $\{E_{K_G}(R_G), R_G\}$ to S.

Step 5. S calculates

$$K_S = X^y \bmod P, \tag{7}$$

encrypts $E_{K_S}(R_S)$ and generates R_S, and then sends $\{E_{K_S}(R_S), R_G, R_S\}$ to G.

Step 6. G receives and decrypts $\{E_{K_S}(R_S), R_G, R_S\}$ and then returns $True$ to S, and the two parties share the same key $K_{S\text{-}G}$, which is used to complete the key sharing.

4.4. Fragmented Multipath Data Transmission. According to the abovementioned, G and S have accomplished their bidirectional authentication and commonly share the session key $K_{G\text{-}S}$. To ensure the security of the data transmission process, G encrypts the the data to be transmitted by a shared key and divides the cipher text into fragments to transfer through selected multiple different paths. The fragmented multipath data transmission (FMPDT) includes multipath data encryption and cipher-text transmission, described as follows.

Step 1. Assuming that the user's medical information is M composed of various identification and sign data sensed by sensors such as s_i $(i = 1, \ldots, m)$, it is received by the sink node N_j and represented as follows:

$$M = \biguplus_{i=1}^{m} \left(\text{type}\left(s_i\right) \oplus \text{value}\left(s_i\right)\right), \tag{8}$$

where one senor is a RFID reader which can get the ID value $\text{ID}(p)$ for a person p and other sensors are medical sensors which can collect the sign data.

Step 2. After being encrypted with the key k which is the data encryption/decryption key shared by all the sensor nodes, all sink nodes, and the gateway node in the regional ZigBee WSN, it becomes

$$c = e_k(M). \tag{9}$$

Step 3. For the cipher-text c of a complete medical information in N_1, it is sent to N_2 or N_3. Then, N_2 or N_3 can transmit it to the gateway node G.

Step 4. After receiving the cipher-text package, G will decrypt it and get the plain-text:

$$M = d_k(c). \tag{10}$$

Step 5. G uses the key $K_{S\text{-}G}$ to encrypt M, and the obtained cipher text is

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

Step 6. C is divided into sub-data packets $C_1, C_2, \ldots, C_n$ by G. For every one of the sub-data packets, G adds a session number Seq and subpacket identification i and gets the sub-data packets as follows:

$$m_i = \left\langle C_i, \text{Seq}, i\right\rangle \quad (1 \leq i \leq n), \tag{12}$$

where Seq and i are used to restore the data by S and are also used to prevent replay attacks. Then, in order to verify the validity of m_i received by the server node S, using the Hash function $H(x)$ with keys, G calculates the message authentication code:

$$h = H_{K_{S\text{-}G}}\left(C_i, \text{Seq}, i\right). \tag{13}$$

Finally, on each selected path, G sends the message

$$S_i = \left\langle C_i, \text{Seq}, i, h\right\rangle. \tag{14}$$

Step 7. For every received sub-data packet $S_i = \langle C_i, \text{Seq}, i, h\rangle$, S will authenticate the message according to the authentication code. In other words, S will determine whether the following condition is established:

$$h == H_{K_{S\text{-}G}}\left(C_i, \text{Seq}, i\right). \tag{15}$$

If that condition is not established, S_i will be discarded. This can ensure the validity of the data packet. Or according to Seq, i, after checking the list of received packets and finding the same one, S will reject S_i in order to avoid the replay attacks.

Step 8. After receiving all of the sub-data packets $\{C_i \mid i = 1, 2, \ldots, n\}$ with the same Seq from the same G, S will reorganize them and get the complete cipher text:

$$C = \biguplus_{i=1}^{n} C_i. \tag{16}$$

Step 9. Then, S decrypts C to recover the data M:

$$M = d_{K_{S\text{-}G}}(C). \tag{17}$$

Eventually, S extracts the medical data from M and stores them in the database according to a certain rule (e.g., encrypted storage, slice storage).

5. Access Control

In order to protect the security and integrity of the patient's medical privacy data storage and share those data conveniently, the corresponding access medical privacy data are needed to be dynamically managed using hierarchical and dynamic authorization. In the open network environment, the access control of medical data mainly includes the following:

(i) Allowing the legitimate users (patients, doctors, and nurses) to access their own data

(ii) Preventing the illegal users from illegally accessing medical privacy data

(iii) Preventing the unauthorized access from legitimate users to other user's medical privacy data

(iv) Sharing locally the medical privacy data, allowing patients to understand their health status in a timely manner, and allowing healthcare workers to follow up the patient's condition, so as to promote the health and rapid development of the medical field.

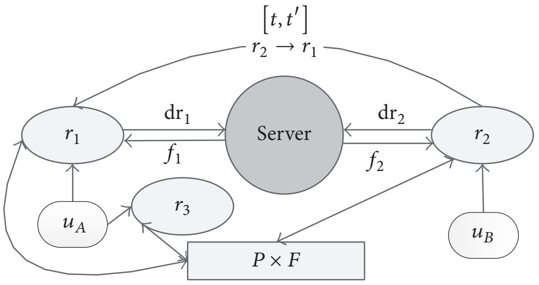


Figure 5: Abstract access control model.

5.1. Fine Grained Access Control. By setting users' security access policy for the medical privacy data, using the security and antileak 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, failed access to sensitive data by illegal users, and limited access to data subset by semilegal users authorized by legitimate users).

Figure 5 shows an abstract access control model for CMIoT, and some symbols are defined in Notations, where

(i) medical data include text data of diagnosis and treatment, pathological documents, image files, etc. and constitute a collection of F;

(ii) $\forall r \in R$, $r = \{\langle f, p, [t, t'] \rangle \mid f \in F,\ p \in P\}$ represents that in this role users can do some specified operations for specified data in the period from t to t';

(iii) $r_i \xrightarrow{[t,t']} r_j$ represents that, between two different roles, for example, a user u_p in $r_i = \langle f, p, [t_i, t_i'] \rangle$ authorizes a role $r_j = \langle f, p, [t, t'] \rangle$ to a user u_q to access the data which u_p can access in the role r_i, and the validity period is from t to t';

(iv) $\forall \mathrm{dr} \in \mathrm{DR}$, $\mathrm{dr} = \langle u, f, p \rangle$, $u \in U$, $f \in F$, $p \in P$. dr represents that when a user request accessing 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.

In practical applications, the difference of users and the actual operating environment need to be taken into account. Assuming that, for the user set U, there are two patients (e.g. $u_{PA} \in U$ and $u_{PB} \in U$) and two doctors or nurses (e.g. $u_{DA} \in U$ and $u_{DB} \in U$), u_{PA} and u_{PB} are treated in the medical institution where u_{DA} and u_{DB} works, and u_{DA} and u_{DB} 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 request legitimacy and return data if legal. Figure 6 shows the data access methods and authorizations of patients, doctors, and nurses. u_{PA} 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. u_{PA} can also authorize u_{DA} and u_{DB} to the medical data of u_{PA}. The authorization between patients and doctors is a many-to-many 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.

5.2. Dynamic Authorization Scheme. In the cloud storage environment of CMIoT, the access control policy of medical privacy data mainly includes the following:

(i) After a patient u_P logs on the cloud storage server, he or she may view his or her own medical data, that is, personal information, medical data, electronic medical record, PACS image information, etc. In other words, u_P has some roles $\{r_i\}$ which u_P owns, and in these roles, u_P can complete some specified operations.

(ii) After a doctor u_D or a nurse u_N logs on the cloud server, u_D or u_N can view their own account information and track the given patients' medical data. Under normal circumstances, u_D or u_N can only manage u_D's or u_N's own personal data without permissions to access a patient's medical data.

(iii) Once the patient u_p authorizes an access permission to u_D or u_N by the authorization code (i.e., u_P selects some $r \in \{r_i\}$ from u_P own roles $\{r_i\}$ and authorizes them to u_D or u_N), u_D or u_N can view and track the medical data of u_P through u_D's or u_N's own account in a certain authorization validity period $[t, t']$.

(iv) In the same way, u_D or u_N can also authorize its own authorized roles to other users.

When the medical data are accessed by different users, as shown in Figure 5, the cloud storage server will verify the user's permissions according to the user's roles $\{r_i\}$ and returns the corresponding data f to the user according to the data request dr. This can be implemented through dynamic authorization as shown in Figure 7. At the authorization stage, in order to ensure the security, patients are not allowed to directly authorize the access permission to medical staff. Roles and permissions are bound as the patient authorization data to be written to the server through the third party data platform and are sent to medical staff so that he or she can access the specified data from the cloud storage server according to the roles and permissions.

During medical data access, different roles have different access permissions. However, a role can provide other roles with access permissions through dynamic authorization. Assuming that the role r_1 is one of the roles which a patient or a designated administrator u_P has been assigned for a validity period $[t_1, t_1']$, and u_P has the permission of direct access to his or her own or manageable medical data, as shown in Figure 8, the nurse u_N and the doctor u_D without the role r_1 cannot directly access those data. That means that u_N and u_D

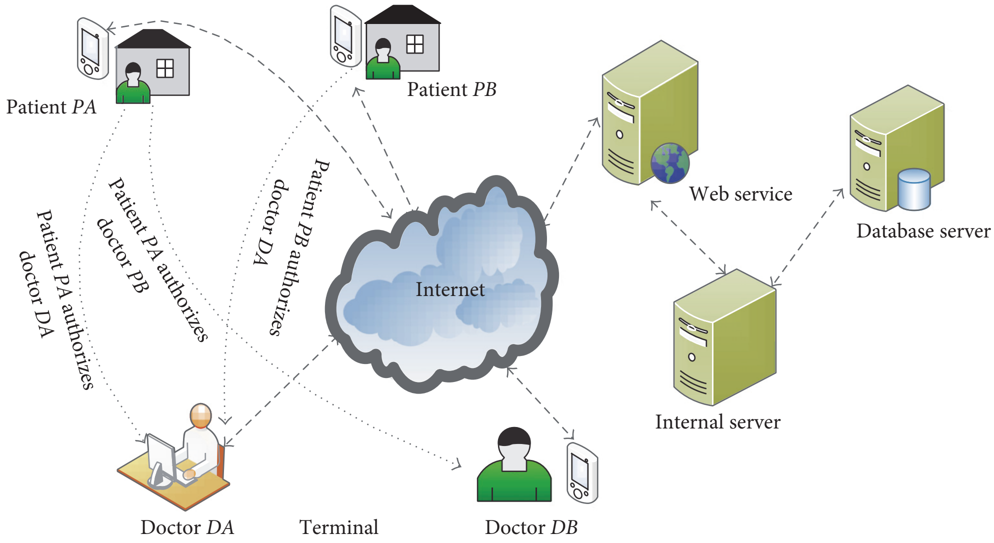


Figure 6: Fine grained access control model.

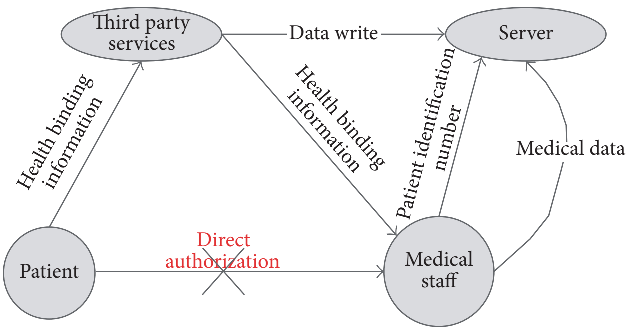


Figure 7: Dynamic authorization.

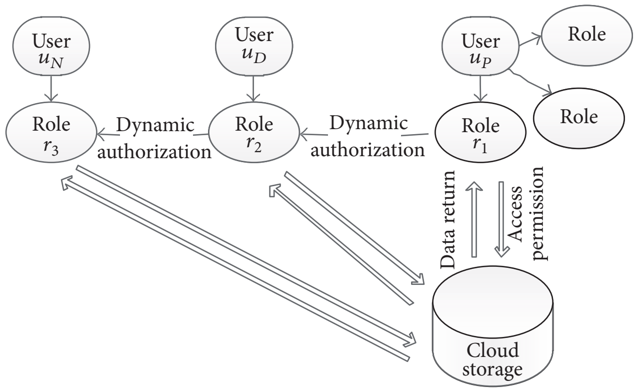


Figure 8: Access control process.

need an authorization. Therefore, u_P can authorize the role r_2 to u_D for a validity period $[t_2, t_2']$ ($r_1 \xrightarrow{[t_2,t_2']} r_2$), and further, u_D can authorize the role r_3 to u_N for a validity period $[t_3, t_3']$ ($r_2 \xrightarrow{[t_3,t_3']} r_3$) so that the nurse has the same permissions. It needs to be explained here: $[t_3, t_3'] \subseteq [t_2, t_2'] \subseteq [t_1, t_1']$.

The mechanism provides a great convenience for medical staffs in a certain period of time and makes the unauthorized medical staffs unable to view the patient data so as to avoid the risk of patient medical data being stolen. This greatly protects the privacy of the patient's medical data in two aspects. One is the operation permission control of medical privacy data. Different levels of users have different permissions for different sensitive data. The other one is the 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. Experiments and Analysis

In CMIoT, some medical sensors and devices are deployed indoors at home, and some ones are deployed in 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, and ECG (electrocardiograph) data $n \geq 10$ 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, and managers can access the medical data in the cloud storage server given in a specified role with some specified permissions.

6.1. Transmission

6.1.1. Security Analysis. For the data transmission protection in CMIoT, its security includes WSN security, authentication security, key agreement security, and fragmented multipath transmission security.

(i) WSN Security. In the WSN, the ZigBee protocol stack defines the security for MAC, network, and application layers and provides a security mechanism of symmetric key; for example, in ZStack-CC2530-2.3.0-1.4.0, AES-128 with a configurable key k, which is an efficient symmetric Rijndael packet encryption/decryption algorithm designed by Daemen and Rijmen, is supported if the Z-stack encryption algorithm is switched on. AES does not use the Feistel structure (as used in DES). Instead, it uses three different reversible uniform transformation layers: linear mixing layer, nonlinear layer, and key addition layer. In the protocol stack, with AES-128, it can avoid the interference of the same device and prevent the other devices from listening. If the AES encryption algorithm is used, all the devices in the network need to open the algorithm, and the key in each device must be the same. This ensures the secure transmission of data in WSN, since the data without encryption, or without encryption using the same key, will not be identified by the WSN nodes.

(ii) Authentication Security. Before the medical data are transmitted, G has an authentication with S. If the bidirectional authentication does not entirely pass, S will refuse to receive data so as to prevent fake gateway nodes from forging transmission data, and equally, G will refuse to send data so as to avoid the phishing of the pseudo-server node. Even if attackers steal the password table in S, they cannot crack the password because of the unidirectional characteristic of Hash function. Therefore, it can effectively ensure the identity authentication for S and G.

As shown in Table 1 where √ 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, and therefore Peyravian's protocol cannot prevent gateway nodes forging. Ma's protocol cannot prevent dictionary attacking due to the data characteristic despite various attacking means.

(iii) Key Agreement Security. In order to prevent the attacker from 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 2, √ represents that the security condition is met. KAM guarantees the security of the key used to encrypt and decrypt the medical data.

(iv) Fragmented Multipath Transmission Security. Compared to any single-path transmission mechanism, the fragmented multipath transmission can effectively increase the difficulty of the attacker to obtain the complete data. It provides security in two ways. On the one hand, the data is encrypted transmission. On the other hand, the data is fragmented transmission. 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 multipath (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.

6.1.2. Performance Impact. The above encrypted fragmented multipath transmission can be used to protect the uplink data. As for the downlink data between access clients and the server S, this method is equally applicable. Of course, the clients also need to complete some initialization processes such as registration, bidirectional authentication, and key agreement, and after that, the server transfers the accessed data to the client by the encrypted fragmented multipath transmission. Whether it is uplink data or downlink data, due to the use of encryption and fragmentation, in the protection of data security at the same time, it is bound to increase the delay of data transmission. The extent of its impact will be discussed as follows.

The encrypted fragmented multipath transmission provides a certain security for CMIoT. In order to test its effectiveness, we designed some experiments as shown in Table 3. In Scheme 1 which is a plain-text transmission without any security protection, no encryption measure is used, and data is transmitted in plain text without fragments in the information integration layer. In Scheme 2 which is a G-S symmetric encrypted nonfragmented transmission, after being encrypted in G using a symmetric cryptography, the data is sent to S as a complete packet in the information integration layer, and in Scheme 3 which is a G-S asymmetric encrypted nonfragmented transmission, an asymmetric cryptography is used. Schemes 4–7 adopt the fragment mechanism for the encrypted message. In Scheme 4, which is a G-S symmetric encrypted fragmented transmission, and Scheme 6, which is an s-N^+-G-S symmetric encrypted fragmented transmission, the symmetric cryptography is put into use in G and S, and they are recommended. On the contrary, in Scheme 5, which is a G-S asymmetric encrypted fragmented transmission, and Scheme 7, which is an s-N^+-G-S asymmetric encrypted fragmented transmission, G and S make use of the asymmetric cryptography. Another difference is that, in Scheme 4 and Scheme 5, for sensor nodes, sink nodes, and G, data transmission between them does not use the symmetric encryption, which is used in Schemes 6 and 7.

Asymmetric cryptography provides higher security (e.g., RSA, EIGamal, LUC, Rabin, and DSA). However, they have lower speed. In our experiments, for the 256-bit key of RSA, the time taken to encrypt and decrypt 128-bit data on a desktop computer (Processor: Intel i5-6200U 2.3 GHz) is, respectively, about 989 ns and 2,971 ns. It should be noted that the 256-bit key of RSA is not the main stream. By comparison, asymmetric cryptography, such as DES, IDEA, GOST, Blowfish, RC-4, RC-5, CAST-128, and AES, has higher speed; for example, for the 128-bit key of AES, the time taken to encrypt and decrypt 128-bit data on a desktop computer is, respectively, about 5 ns and 3 ns. Another significant difference is that the length of the encrypted data changes. The lengths of plain text and cipher text are the same using AES encryption

Table 1: Authentication security analysis.

Security condition	Scheme			
	Hwang and Yeh [11]	Peyravian and Jeffries [12]	Wang et al. [13]	BDA
Prevent DoS attacking	—	√	—	√
Prevent replay attacking	—	√	√	√
Prevent dictionary attacking	√	√	√	√
Prevent server forging	√	√	√	√
Prevent gateway-node forging	√	—	√	√
No public key mechanism	√	√	—	√
Hash function	√	√	√	√
MAC function	—	—	—	√

Table 2: Key agreement security analysis.

Security condition	Scheme		
	Diffie-Hellman	Xie [14]	KAM
Prevent replay attacking	√	√	√
Forward security	√	√	√
Integrity attacking	√	√	√
Known key security	√	√	√
Prevent wiretap attacking	√	√	√
Prevent MITM attacking	—	√	√
Three-way handshake	—	—	√

in CFB mode or OFB mode. However, since the length of cipher text is equal to the length of the key in RSA and the latter is greater than the length of plain text, the length of data after being encrypted with RSA becomes two times the length of the original data if the 256-bit key of RSA is used to encrypt the 128-bit data. The 256-bit key of RSA and 128-bit key of AES are tested in our experiments.

In order to facilitate the test, we select 128 bits as the the fragment length in the fragmented multipath transmission. $n = 1, 2, 4, 8, 16$ are several kinds of fragment numbers. In case that only one sink node N_1 collects sign data from some medical sensors $\{s\}$ and then sends them to the server S through the uplink, which is $s \rightarrow N \rightarrow N \rightarrow \cdots \rightarrow N \rightarrow G \rightarrow R \rightarrow R \rightarrow \cdots \rightarrow R \rightarrow S$, the numbers of sink nodes $\{N\}$ and router nodes $\{R\}$ in the transmission link are fixed; the experimental results are shown in Table 3.

Due to the large delay, Schemes 3, 5, and 7 are not acceptable. As shown in Figure 9, symmetric encryption increases the delay, but it is still acceptable in actual applications. Another important feature is that fragmentation does not result in a significant increase in latency. Therefore, Schemes 4 and 6 are feasible transmission schemes. Of course, if multiple sources in one regional network or multiple regional networks are transmitting data to the server, the delay will increase further.

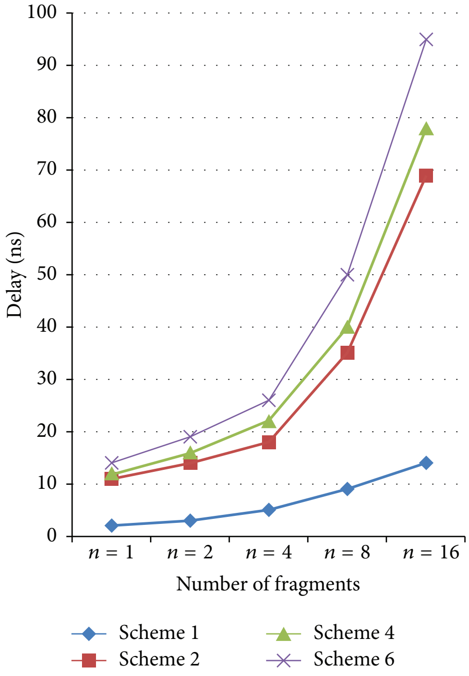


Figure 9: Delay comparison.

6.2. Access

6.2.1. Security Analysis. The above access control scheme reaches the following effects:

(i) Users can access 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.

(ii) Legitimate users can log on the cloud server to view personal information and cannot access nonself data. This can prevent illegal users from abnormal access.

Table 3: Delay of different transmission schemes.

Scheme	Delay (ns) Number of fragments				
	$n = 1$	$n = 2$	$n = 4$	$n = 8$	$n = 16$
Scheme 1	2	3	5	9	14
Scheme 2	11	14	18	35	69
Scheme 3	3,963	7,985	11,979	18,704	33,620
Scheme 4	12	16	22	40	78
Scheme 5	3,965	7,991	11,804	18,716	33,642
Scheme 6	14	19	26	50	95
Scheme 7	3,967	7,994	11,809	18,728	33,665

Table 4: Response time of different grains.

Grain	Response time (ns) Number of accessing users			
	$n = 1$	$n = 10$	$n = 100$	$n = 1{,}000$
User	2	33	5,875	69,568
Type	15	230	40,833	789,865
User, type	6	89	10,988	101,864
Record	78	1,275	204,799	4,756,384
User, type, record	10	125	23,768	351,371

(iii) Through the dynamic authorization mechanism, patients can register an authorization code on the medical data so that once some medical staffs have the same authorization code, they can access those data within the authorized permissions and effective time limitation.

Beyond that, during users' access to medical data, it is also necessary to attach the secure transmission problem of uplink and downlink data to much weight. Any message transmitted on the link also can be protected using the encrypted fragmented multipath transmission mechanism. This will bring a certain degree of delay in the server and clients.

6.2.2. Performance Impact. In one community of 10,000 users, each day there are 100 different types of sign data which need to be collected for 10 times, and in one year, the total amount of collected data is $365 \times 10{,}000 \times 100 \times 10 = 3.65 \times 10^9$. There are also a lot of diagnostic data generated every day. These data will be authorized to users for access operations such as query, modification, and deletion. At the same time of bringing some security, the fine grained access control scheme also increases the response time of users to access data in the server with mobile or PC terminals. Especially in the download link, the CMIoT needs to choose an appropriate access authorization granularity so that the data can be accessed efficiently. In our experiments, the grains could be divided according to user, type of sign data, or record of sign and diagnostic data. In particular, the test involves 100 records per query. As shown in Table 4 and Figure 10, there is a larger difference for the response time of different grains. It can be seen that if the record is taken as a unit of granularity, the response time is very large when the number of accessing users is large. It is not acceptable in actual applications. Even if the type is taken, when the number of users in the operation at the same time is great to a certain extent, the performance of the system will drop a lot.

Therefore, the multidimension grain size needs to be an option. In other words, the data can be authorized by a coarser granularity, and then on another finer granularity, the authorization can be refined. After a series of tests, for the grain divided by user and then divided by type as shown Table 5, the response time is about 0.1 ms for 1,000 accessing users. And for the grain divided by user-type-record which can achieve a more detailed authorization management, it is about 0.4 ms for 1,000 accessing users.

7. Conclusions and Future Works

In this paper, we design the data transmission protection and access control scheme for privacy protection in CMIoT. For the transmission protection, we summarize three aspects such as authentication, communication key agreement, and multipath security transmission. Considering 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 multipath transmission mechanism so that it would become more difficult for the attacker to obtain complete data without affecting server data receiving. Finally, we analyze the security of the method inferred to the full text. In order to ensure the security of medical data in the cloud storage server, an access control method with authorization is used. This scheme

Table 5: Two-dimensional grain in user-type.

Users	Types				
	Hemoglobin	Triglyceride	Glutamic pyruvic transaminase	···	Diagnosis
user_1	151.0 g/L	1.52 mmol/l	40 U/L	···	Mild fatty infiltration of liver
	150.1 g/L	1.66 mmol/l	33 U/L	···	Healthy
	141.0 g/L	0.72 mmol/l	10 U/L	···	Healthy
	139.1 g/L	0.66 mmol/l	11 U/L	···	Healthy
	···	···	···	···	···
user_2	141.0 g/L	0.56 mmoll/l	31 U/L	···	Healthy
	132.6 g/L	0.45 mmol/l	100 U/L	···	Abnormal liver function
	···	···	···	···	···
user_3	···	···	···	···	
···	···	···	···	···	

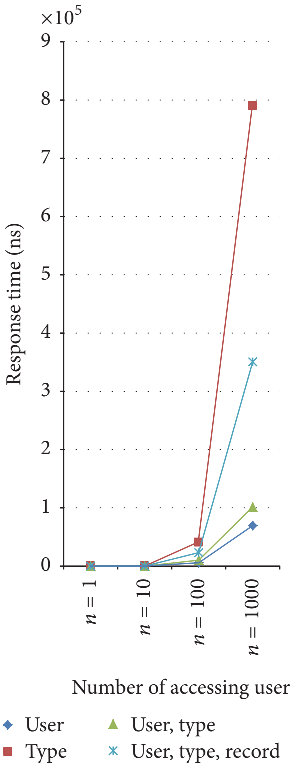


Figure 10: Response time comparison.

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 staffs who do 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 identities of medical staffs, that is, 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.

Notations

The Definitions of Data Transmission Symbols

$p, \text{ID}(p)$:	Person node and the identification number in his or her RFID card
$s_i, \text{type}(s_i), \text{value}(s_i)$:	Sensor node i, type, and sensing value
N_j:	Sink node j
G:	Gateway node
S:	Server node
ID_G:	Gateway node identification
PW_G:	Gateway node password
$H(x), H_k(x)$:	Strongly noncollision Hash function and keyed Hash function
R_G, R_S:	Random number of gateway nodes and server nodes
K_G, K_S:	A pair of asymmetric keys for the gateway node
$K_{S\text{-}G}$:	Symmetric key for gateway node and server node
M, C:	Plain text and cipher text of message
$\text{MAC}_{K_{S\text{-}G}}(M)$:	The MAC value of the message M in the key $K_{S\text{-}G}$
$e_k(x)$:	Symmetric encryption function where k is the key and x is the data
$d_k(x)$:	Symmetric decryption function where k is the key and x is the data
$E_k(x)$:	Asymmetric encryption function where k is the key and x is the data
$D_k(x)$:	Asymmetric decryption function where k is the key and x is the data.

The Symbol Definitions of Access Model

$U = \{u_i \mid i = 1, 2, \ldots\}$:	Set of users that can access medical data
$F = \{f_i \mid i = 1, 2, \ldots\}$:	Set of data in the storage server
$P = \{\text{Read, Append, Delete, Modify}\}$:	Set of access permissions

$R = \{r_i \mid i = 1, 2, \ldots\}$: Set of roles that can access medical data

$A = \{r_i \xrightarrow{[t,t']} r_j \mid i, j = 1, 2, \ldots\}$: Set of access authorizations between roles

$\mathrm{DR} = \{\mathrm{dr}_i \mid i = 1, 2, \ldots\}$: Set of data requests.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported in part by the National Natural Science Foundation of China under Grant no. 61572036, University Natural Science Research Project of Anhui Province under Grant no. KJ2017A863, and Anhui Province University Outstanding Youth Talent Support Program under Grant no. gxyqZD2016026.

References

[1] M. Gao, Q. Zhang, L. Ni, Y. Liu, and X. Tang, "CardioSentinal: a 24-hour heart care and monitoring system," *Journal of Computing Science & Engineering*, vol. 6, no. 1, pp. 67–78, 2012.

[2] J. Zhang, D. Chen, J. Zhao et al., "RASS: a portable real-time automatic sleep scoring system," in *Proceedings of the IEEE 34th Real-Time Systems Symposium*, pp. 105–114, San Juan, Puerto Rico, USA, December 2012.

[3] M. Chen, Y. Zhang, Y. Li, M. M. Hassan, and A. Alamri, "AIWAC: affective interaction through wearable computing and cloud technology," *IEEE Wireless Communications*, vol. 22, no. 1, pp. 20–27, 2015.

[4] Y. Zhang, M. Chen, D. Huang, D. Wu, and Y. Li, "IDoctor: personalized and professionalized medical recommendations based on hybrid matrix factorization," *Future Generation Computer Systems*, vol. 66, pp. 30–35, 2017.

[5] J. Wan, C. Zou, S. Ullah, C.-F. Lai, M. Zhou, and X. Wang, "Cloud-enabled wireless body area networks for pervasive healthcare," *IEEE Network*, vol. 27, no. 5, pp. 56–61, 2013.

[6] Y. Ma, Y. Zhang, J. Wan, D. Zhang, and N. Pan, "Robot and cloud-assisted multi-modal healthcare system," *Cluster Computing*, vol. 18, no. 3, pp. 1295–1306, 2015.

[7] M. M. Hassan, K. Lin, X. Yue, and J. Wan, "A multimedia healthcare data sharing approach through cloud-based body area network," *Future Generation Computer Systems*, vol. 66, pp. 48–58, 2017.

[8] L. Mni, Q. Zhang, H. Y. Tan et al., "Smart healthcare: from IoT to cloud computing," *Scientia Sinica*, vol. 43, no. 4, pp. 515–528, 2013.

[9] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software-defined mobile networks security," *Mobile Networks and Applications*, vol. 21, no. 5, pp. 729–743, 2016.

[10] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[11] J.-J. Hwang and T.-C. Yeh, "Improvement on Peyravian-Zunic's password authentication schemes," *IEICE Transactions on Communications*, vol. 85, no. 4, pp. 823–825, 2002.

[12] M. Peyravian and C. Jeffries, "Secure remote user access over insecure networks," *Computer Communications*, vol. 29, no. 5, pp. 660–667, 2006.

[13] B. Wang, H. Zhang, Z. Wang, and Y. Wang, "Secure mutual password authentication scheme with user anonymity," *Geomatics and Information Science of Wuhan University*, vol. 33, no. 10, pp. 1073–1075, 2008.

[14] W. J. Xie, "A Secure Communication Scheme based on Multipath Transportation for the Internet of Things," South China University of Technology, Guangzhou, China, 2013.

[15] H.-S. Ning and Q.-Y. Xu, "Research on global Internet of Things' developments and it's construction in China," *Acta Electronica Sinica*, vol. 38, no. 11, pp. 2590–2599, 2010.

[16] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[17] Z. Ding, J. Li, and B. Feng, "Research on hash-based RFID security authentication protocol," *Computer Research and Development*, vol. 46, no. 4, pp. 583–592, 2009.

[18] T. Maeda, K. Sato, Y. Muraoka et al., "RFID system and RFID tag," U.S. Patent 8274367, 2012.

[19] Z.-Q. Wu, Y.-W. Zhou, and J.-F. Ma, "A security transmission model for internet of things," *Chinese Journal of Computers*, vol. 34, no. 8, pp. 1351–1364, 2011.

[20] Z. Song, Y. Zhang, and C. Wu, "A reliable transmission scheme for security and protection system based on internet of things," in *Proceedings of the IET International Conference on Communication Technology and Application (ICCTA '11)*, pp. 806–810, October 2011.

[21] Y. U. Yong-Hong and W. Y. Bai, "Enforcing data privacy and user privacy over outsourced database service," *Application Research of Computers*, vol. 6, no. 3, pp. 404–412, 2011.

[22] Z. Hong, *Research on Electronic Health Records of Community Residents*, Fudan University, 2008.

[23] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: usable and secure key agreement scheme for body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 60–68, 2010.

[24] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[25] C. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," in *Proceedings of the 20th Tyrrhenian Workshop on Digital Communications*, pp. 389–395, Sardinia, Italy, September 2009.

[26] C. Wu, "An overview on the security techniques and challenges of the internet of things," *Journal of Cryptologic Research*, vol. 2, no. 1, pp. 40–53, 2015.

[27] W. Du, J. Deng, Y. S. Han et al., "A Pairwise key pre-distribution scheme forwireless sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03)*, pp. 42–51, Washington, DC, USA, 2003.

[28] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication," in *Proceedings of the IEEE 37th Conference on Local Computer Networks Workshops (LCN '12)*, pp. 956–963, October 2012.

[29] A. Groce and J. Katz, "A new framework for efficient password-based authenticated key exchange," in *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10)*, pp. 516–525, ACM, Chicago, Ill, USA, October 2010.

[30] S. Forsström, T. Kanter, and P. Österberg, "Ubiquitous secure interactions with intelligent artifacts on the internet-of-things," in *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom '12)*, pp. 1520–1524, June 2012.

[31] H. Ye, J. Yang, J. Zhu et al., "A secure privacy data transmission method for medical internet of things," in *Proceedings of the Industrial IoT Technologies and Applications*, pp. 144–154, March 2016.

[32] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 99–112, Alexandria, Va, USA, October-November 2006.

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

[34] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proceedings of the 29th conference on Information communications (INFOCOM '10)*, pp. 534–542, San Diego, Calif, USA, March 2010.

[35] T. Yuen, S. M. Chow, Y. Zhang 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, April 2012.

[36] F. Beato, S. Meul, and B. Preneel, "Practical identity-based private sharing for online social networks," *Computer Communications*, vol. 73, pp. 243–250, 2016.

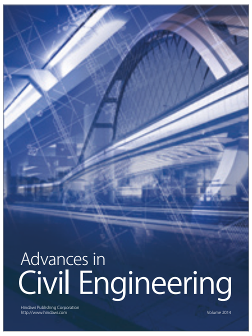
Journal of
Engineering

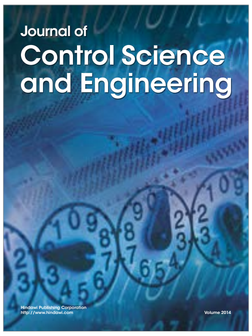
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

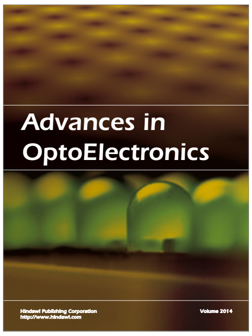
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

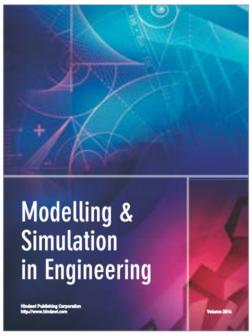
Journal of
Robotics

Journal of
Electrical and Computer Engineering

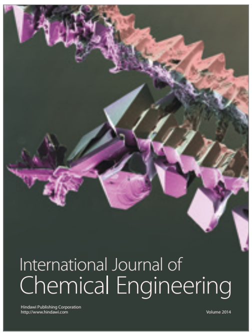

Advances in
OptoElectronics

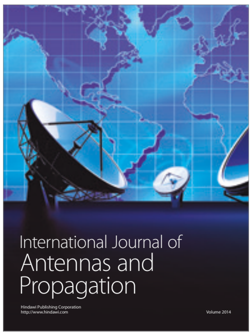
VLSI Design

International Journal of
Navigation and Observation

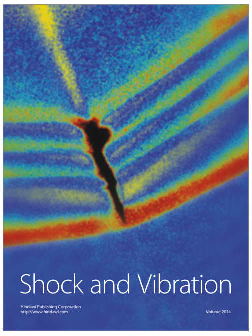

Modelling &
Simulation
in Engineering

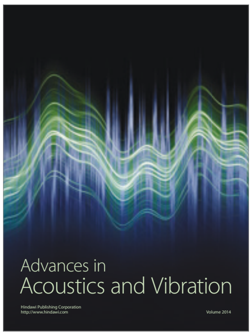
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration