An Advanced Secure Scheme of Domestic E-medical System in Body Area Network

Enjian Bai, Yajie Gao, Xueqin Jiang and Yun Wu

College of Information Science and Technology, Donghua University, Shanghai, China
Email: gggaoyajie@163.com

Abstract. In the context of Body Area Network (BAN), e-medical service is gradually in high demand due to the increasing focus on health care recent years. However, there are still great challenges badly endangering medical information security. Designing for e-medical system, we propose a suit of well-integrated security scheme gathering functions of collecting, processing, diagnosing and querying medical data. Apart from resisting common attacks and eavesdropping from enemies, our proposed scheme borrows idea of dual signature in order to hide partial sensitive information from doctor, server and some other nice identities for privacy protection. In addition, we analyse the security performance of this e-medical system scheme and find it behaves well in resisting privacy disclosure, impersonation attack, replay attack and data falsification.

1. Introduction

Since the rapid development of Internet of Things (IoT) and the expansion of correlative health-care business scope, as a branch of Wireless Sensor Network (WSN) in medical field, Body Area Network (BAN) is gradually coming into view. Generally speaking, a typical BAN system consists of several implantable or wearable sensor nodes used for collecting physiological data and back-end data processing system. Physiological signals such as body temperature, blood pressure, oxygen levels and electrocardiogram (ECG) from the patient is gathered via the wireless sensors and transmitted to a cluster head or a gateway device, which is then possibly relayed to one or more local servers[1-4]. The growth of large-scale information systems is a topical issue in the health-care sector[5]. In addition to ensuring the good device experience, the safe transmission of medical information and privacy protection are also big points in the research of BAN.

In order to solve problems in e-medical system mentioned above, various works have been coming out recent years. Gritzalis and Lambrinoudakis proposed a security architecture which was mainly designed for providing authentication and authorization services in web-based distributed systems[6]. Hsu et al. proposed an integrated Institutional Review Board (IRB) system to connect hospitals, clinics, manufacturers and customers in order to share information, reducing administrative costs, and further improving the quality of intelligent medical devices design[7]. Hu et al. designed a scheme to secure the data communications between implanted/wearable sensors and the data sink/data consumers (doctors or nurse) by employing Ciphertext-Policy Attribute Based Encryption (CP-ABE)[8-10].

However, existing studies mostly focus on resisting the attack of enemies such as eavesdropping and tampering , scarcely considering of covering partial patients' sensitive information under doctors, service supporters and some other legal objects, which can hardly achieve privacy protection in domestic e-medical system. Departed from the issue mentioned above, we proposed an advanced secure scheme of domestic e-medical system (DEMS). DEMS perfectly integrates data collection, diagnosing and some other medical functions as a whole, ensuring transmission security and privacy protection using encryption, digital signature, Hash, etc, which supports a well-integrated suit of e-medical secure scheme.

The rest of paper is organized as follows: Section 2 introduces the system model and related technologies of DEMS and lists all symbols used later. Section 3 specifically illustrates the process of executing DEMS with collecting, encrypting, signing and authenticating included. Section 4 presents the security analysis and section 5 concludes the paper.

2. Preliminaries

DEMS applies to domestic health-care system and it can support more than one person, which distinguishes and serves different users by identifying the flashing ID card on the device.

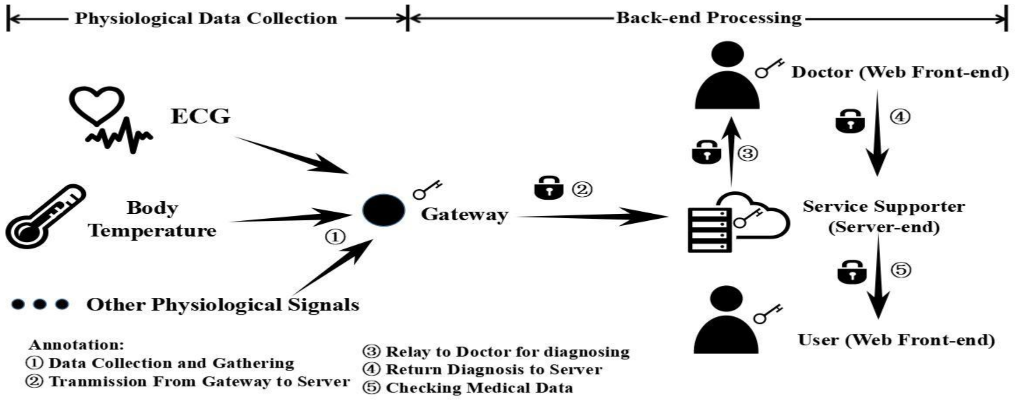
Physiological Data Collection
Back-end Processing
ECG
Body Temperature
Other Physiological Signals
Gateway
①
②
Doctor (Web Front-end)
③
④
Service Supporter (Server-end)
⑤
User (Web Front-end)
Annotation:
① Data Collection and Gathering
② Tranmission From Gateway to Server
③ Relay to Doctor for diagnosing
④ Return Diagnosis to Server
⑤ Checking Medical Data

Figure 1. System model.

Table 1. Declaration of Symbols Used Later

Symbols	Explanation
R	A periodically updated random number generated at server-end
K	Symmetric key used for encrypting physiological data by gateway node
PK , SK	Public key and secret key of gateway
K_0	Symmetric key used for encrypting diagnosis data by doctor
PK_A , SK_A	Public key and secret key of doctor
PK_B , SK_B	Public key and secret key of user
$E_{Ki}(M)$	Ciphertext of message M encrypted using key Ki
$H(M)$	Digest of message M through Hash function

As showed in Figure 1, this e-medical system consists of several sensor nodes, the gateway, the user-end, the server-end and the doctor-end. All physiological data such as body temperature and blood pressure will gather at the gateway after being collected. The gateway will process the received data and send it with its own signature to server through internet. Having received those ciphertext, server will perform identity authentication and relay them to the selected doctor. The doctor will do authentication first as well and return diagnosis in the form of ciphertext with his own signature. Having ensured the data received from doctor believable, server stores all of them in database and waits for request from user.

On the basis of fundamental security measures such as encryption, signature, hash function and so on in this work, note that we bring in the idea of dual signature, a key technology in Secure Electronic Transaction (SET) protocol[11]. Considering of the speciality of dual signature, we develop dual signature in our e-medical system so that doctor and server could only respectively see partial necessary information. To be more specifically, in DEMS, the server-end won't obtain the original physiological information and the doctor can never get users' personal identity information, which achieves the purpose of privacy protection.

To simplify the following illustration, we list all symbols used later in Table 1.

3. Proposed Secure Scheme

This section specifically illustrates the process of performing DEMS including six phases.

3.1. User Registration and Initialization Phase

In this phase, a user registers his own ID of the medical system in interface layer of WEB and submits his identity information as asked by system. Note that this phase only faces new users who never registered before and old users could begin from phase B. The description of this phase is given below:

Step 1: User signs up to obtain his own ID of this medical system and submits his true identity information(marked as M_2) as told by what web page shows. Then, choose the doctor he want.

Step 2: User-end sends server the information of user ID, $H(M_2)$ and the chosen doctor ID.

3.2. Physiological Data Collection Phase

This phase is designed for data collection and data uploading. Medical devices here accept identity information of user and undertake duties of collecting, encrypting and sending out the physiological data(marked as M_1). The details are as follows:

Step 1: User turns on the medical devices and actives the system to collect M_2 by flashing his ID card.

Step 2: Server-end sends gateway an random number encrypted with PK , which is marked as $E_{PK}(R)$ and gateway will decrypt it with SK . Note that the random number is effective only in one-whole-process, which means that the random number is effective in an integrated set of phase B-C-D-E-F and it will update when the next Physiological data collection phase come.

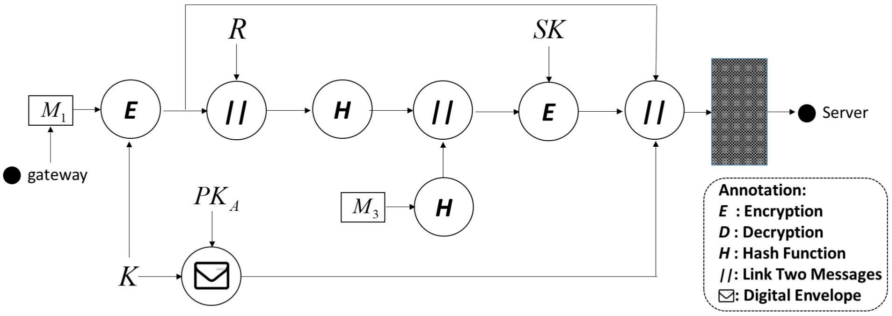

Figure 2. Data processing in Physiological data collection phase.

Step 3: After sensors finish collecting physiological data M_1 , M_1 and M_2 will gather at gateway. Later as showed in Figure 2, gateway will send server the linked result of encrypted physiological information

$$E_K(M_1) \tag{1}$$

the encrypted symmetric key

$$E_{PK_A}(K) \tag{2}$$

and the signed information

$$E_{SK}\{H[E_K(M_1)//R]//H(M_2)\} \tag{3}$$

3.3. Authentication and Relay Phase

In this phase, server authenticates its received information in order to ensure the reliability of information source and make sure the current user is eligible. Then, server will relay all of received information to the doctor user chose before. The exact steps are developed below:

Step 1: server should authenticate the received signature first. As showed in Figure 3, Server decrypts (3) using PK in order to get

$$H[E_K(M_1) // R] \tag{4}$$

and

$$H(M_2) \quad (5).$$

Then, calculate

$$H[E_K(M_1) // R] \tag{6}$$

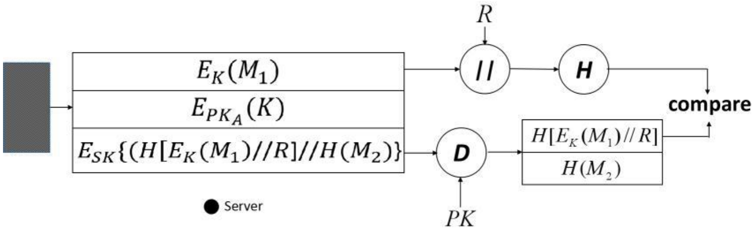

Figure 3. Authentication in authentication and replay phase.

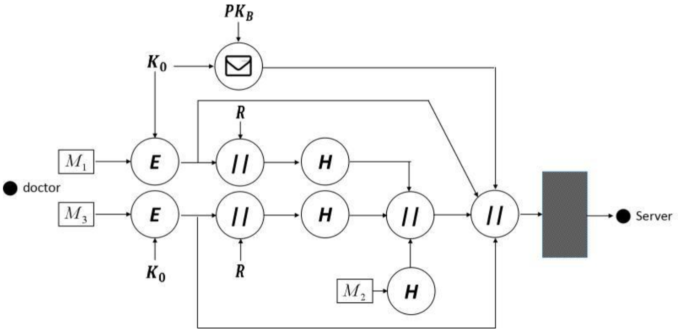

Figure 4. Data processing in diagnosing phase.

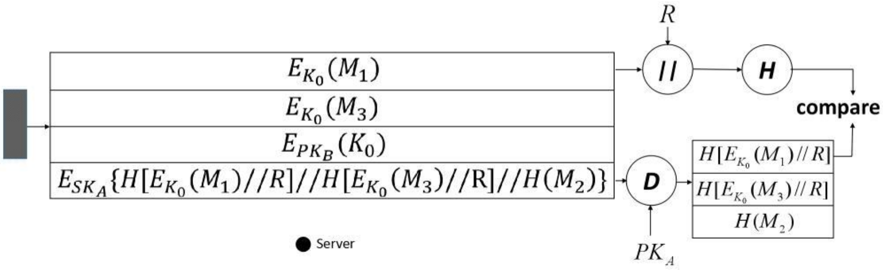

Figure 5. Authentication in authentication and storing phase.

using (1) and R which was generated in physiological data collection phase. If (4) is equal to (6), which means the information were not modified while being transmitted, we can say that (4) and (5) are both trustworthy.

Step 2: server should check whether (5) is existing in database so as to make sure the current user is registered. If yes, server will relay (1), (2), (3) and $E_{PK_A}(R)$ to the doctor user chose before. Else, server will send alarm to device-end to alert current user to sign up first.

3.4. Diagnosing Phase

This phase is performed by doctor. Doctor should authenticate the signature on the information he received to make sure it is believable before diagnosing and send out encrypted diagnosis to server. Details of this phase are given below:

Step 1: As with what has been down in Step1 of phase C, doctor will authenticate the digital signature to ensure (4) and (5) are both trustworthy.

Step 2: Using SK_A, doctor decrypts (2) and $E_{PK_A}(R)$ to obtain the random number R and the symmetric key K used for decrypting (1) so as to get the plaintext of original physiological data M_1.

Step 3: Doctor diagnoses with the physiological data M_1 and comes out the diagnosis (marked as M_3). Later as showed in Figure 4, doctor will link

the encrypted physiological data

$$E_{K_0}(M_1) \tag{7}$$

, the encrypted diagnosis data

$$E_{K_0}(M_3) \tag{8}$$

the encrypted symmetric key

$$E_{PK_B}(K_0) \tag{9}$$

and the signed information

$$E_{SK_A}\{H[E_{K_0}(M_1 // R)] // H[E_{K_0}(M_3 // R)] // H(M_2)\} \tag{10}$$

and send the linked result to server.

3.5. Authentication and Storing Phase

The information that server received from doctor will be authenticated and stored in this phase, waiting to be requested by user from web page later. The details state below:

Step 1: After receiving (7), (8), (9) and (10), as showed in Figure 5, server decrypts (10) with PK_A in order to get

$$H[E_{K_0}(M_1 // R)] \tag{11}$$

$$H[E_{K_0}(M_3 // R)] \tag{12}$$

and

$$H(M_2) \tag{13}$$

Then, using (7) or (8), server calculates

$$H[E_{K_0}(M_1 // R)] \tag{14}$$

or

$$H[E_{K_0}(M_3 // R)] \tag{15}$$

and compare it with (11) or (12). If (11) is equal to (14)(or if (12) is equal to (15)), which means the information were not modified while being transmitted, we can say (7), (8), (9) and (10) are all trustworthy.

Step 2: After finishing authentication, server will match information with its user in accordance to $H(M_2)$ and store (7), (8), (9) and (10) in database, waiting to be selected.

3.6. User Query Phase

In this phase, user will login and ask for his medical information. Some measures ensuring for security such as decryption and authentication will be took here as well:

Step 1: User login the system from web-page-end and request for checking his physiological information M_1 and the diagnosis M_3.

Step 2: Receiving user's request, server will select what user need from database where user ID is matched Then, send the selected result (7), (8), (9), (10) and the encrypted random number $E_{PK_A}(R)$ to user.

Step 3: As what has been down in Step1 of authentication and storing phase, user should authenticate the signature of (10) to ensure the information he received is believable. If yes, using SK_B, user decrypt (9) to get symmetric key K_0 used for decrypting ciphertext (7) and (8) to get the plaintext of original physiological data M_1 and diagnosis data M_3.

The above is the whole process of DEMS.

4. Security Analysis

Involved of two symmetric keys and three pairs of asymmetric keys, our secure scheme needs to execute symmetric encryption two times, asymmetric encryption two times, digital signatures two times and identity authentication four times. We analyse the security performance in this section.

4.1. Privacy Protection

DEMS brings in the idea of dual signature in physiological data collection phase and diagnosing phase. Taking the former for example, we illustrate as follow: The gateway, using secret key SK , signs on the linked result of digest $H[E_K(M_1)//R]$ and $H(M_2)$ to get $E_{SK}\{H[E_K(M_1)//R]//H(M_2)\}$ and send it to server together with $E_K(M_1)$, $E_{PK_A}(K)$. After receiving data mentioned above, server can just achieve authentication through calculating digest of $E_K(M_1)//R$ and comparing the result with $H[E_K(M_1)//R]$, the decryption result of (3) in order to ensure $H(M_2)$ it received is believable.

In that case, server can not get physiological data M_1 because it can never obtain key K from $E_{PK_A}(K)$ for lack of doctor's secret key SK_A but doctor who holds SK_A has the right, which protect patient's privacy.

On the basis of what have been discussed above, physiological data M_1 hides from server and user's identity information M_2 is covered throughout the whole process, which achieve private protection.

4.2. Impersonation Attack

Digital signature and the random number are used several times in DEMS. Enemy can not get the random number R from no matter $E_{PK}(R)$ or $E_{PK_A}(R)$ without SK or SK_A . Taking the diagnosing phase for example, doctor sends server $E_{SK_A}\{H[E_{K_0}(M_1//R)]//H[E_{K_0}(M_3//R)]//H(M_2)\}$ which has been signed by doctor with private key SK_A and server will authenticate the signature. Enemy can not fabricate the correct $H[E_{K_0}(M_1//R)]$ or $H[E_{K_0}(M_3//R)]$, neither can he pretend as the doctor to sign for lack of the private key. By the same reason, enemy can not pretend to be the gateway to send false information.

4.3. Replay Attack

Owing to the specialty of medical data, if enemy launch a replay attack, the latest information won't be delivered in time, which will delay patient's cure and might even endanger life. DEMS bring in the random number R which is effective only in one-whole-process and the number will be update when the next new process comes. For instance, after receiving $E_{SK_A}\{H[E_{K_0}(M_1//R)]//H[E_{K_0}(M_3//R)]//H(M_2)\}$ and $E_{K_0}(M_1)$, server has to authenticate the signature with R in order to guarantee it is the latest information. By the same logic, server would check the signed information received from doctor with R. Thanks to the random number, a replay attack will be detected when enemy attempt to confuse the receiver-end with old data.

4.4. Data Falsification

Due to the high sensibility of objective text, the digest through Hash will change a lot even if the objective text has a tiny modify. DEMS adopts Hash several times and puts signature on digest instead of signing on plaintext directly, dramatically lowering the risk of data falsification.

5. Conclusion

Aiming at existing challenges in e-medical system, we proposed an advanced secure scheme integrating completed functions of data collection, processing, diagnosing and querying. Compared to most existing e-medical health-care secure system, other than dealing with common attacks and eavesdropping from enemies, our proposed scheme brings idea of dual signature so as to hide partial sensitive information from doctor and server for privacy protection. Finally, the paper analyses the security performance of DEMS in regard to impersonation attack, replay attack,etc.

6. References

[1] G.Thamilarasu and A.Odesile, "Securing wireless body area networks: Challenges, review and recommendations," in 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Dec 2016, pp. 1–7.

[2] L. S. Committee, "Ieee standard for local and metropolitan area networks - part 15.6: Wireless body area networks," IEEE Std 802.15.6-2012, pp. 1–271, Feb 2012.

[3] 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, Jan 2010.

[4] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "Ecg-cryptography and authentication in body area networks," IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 6, pp. 1070–1078, Nov 2012.

[5] L. K. Johannessen, A. Obstfelder, and A. T. Lotherington, "Scaling of an information system in a public healthcare market infrastructuring from the vendor's perspective," International Journal of Medical Informatics, vol. 82, no. 5, pp. e180–e188, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1386505612001797

[6] D. Gritzalis and C. Lambrinoudakis, "A security architecture for interconnecting health information systems," International Journal of Medical Informatics, vol. 73, no. 3, pp. 305–309, 2004, realizing Security into the Electronic Health Record. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1386505603002144

[7] C.-L. Hsu, K. C. Tseng, and Y.-H. Chuang, "A secure irb system for assisting the development of intelligent medical devices," Expert Systems with Applications, vol. 39, no. 16, pp. 12 512–12 521, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417412006598

[8] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 2, pp. 94– 107, April 2016.

[9] D. Panescu, "Emerging technologies [wireless communication systems for implantable medical devices]," IEEE Engineering in Medicine and Biology Magazine, vol. 27, no. 2, pp. 96–101, March 2008.

[10] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuang, "Exploiting prediction to enable secure and reliable routing in wireless body area networks," in 2012 Proceedings IEEE INFOCOM, March 2012, pp. 388–396.

[11] S. M. Shedid and M. Kouta, "Modified set protocol for mobile payment: An empirical analysis," in 2010 2nd International Conference on Software Technology and Engineering, vol. 1, Oct 2010, pp. V1–350–V1–355.