A Secure and Efficient Authentication Scheme for Personal Health Care System

Chin-Ling Chen[1,2,a], Po-Tsun Huang[1,b] and Yong-Yuan Deng[1,c],
[1]Department of Computer Science and Information Engineering, Chaoyang University of Technology, 168 Jifeng E. Rd., Wufeng District, Taichung, 41349 Taiwan, R.O.C.
[2]School of Information Engineering, Changchun Sci-Tech University, Changchun 130600, P.R. China

[a]clc@mail.cyut.edu.tw, [b]m4596646@cycu.org.tw, [c]allen.nubi@gmail.com,

Abstract

With the development of network environment and hardware technology, smart devices therefore have become very popular tools. Nowadays, smart facilities are very common in our daily lives. For example, smart refrigerators, smart air conditioners, smart home, smart cities and a large number of applications of Internet of Things have been used. The concept and technology of Internet of Things are being carried out in full swing. Internet of Things in the personal care is one of the concern topics. In order to prevent malicious attacks, resulting in the leakage of patient data, the security of Internet of Things is important. Review the related works about health care service. We found that their article lack of complete security mechanism, therefore we proposed a new architecture which is an IoT-based authentication scheme for personal health care system. In the proposed scheme, doctors can get patients' health status from wearable devices of patients. We complete the goal of electronic medical record sharing. Our scheme can achieve anonymity, mutual authentication, non-repudiation. It can also against forgery attack.

Key words: Internet of Things, health care, electronic medical record, forgery attack

Introduction

In view of the ageing population and the decreasing birth rate, there are many people live alone especially the elders. According to the statistic publish by WHO in 2015 [1]. We found that it is important to face the increasing rate of sudden death. In order to adapt the current society and avoid by sudden death, wearable device in wireless sensor network would be helpful [2]. It makes sense in detecting the patients' symptoms. Wearable device sent out a warning before the symptom getting worse [3]. It may decrease the probability of sudden death.

In general, the wearable devices are functional in IoT, but the resources in IoT are constrained [4]. It is said that the wearable devices restrict in low computation. We avoid high computational encryption method in our scheme when we deliver the message, so it is important of using simple way to reach the security level [5]. Moreover, the wearable devices are used in wireless, it may cause attacks by the adversary [6]. These security issues include privacy and authentication are the most important things must be considered [7]. Therefore, we proposed a secure IoT structure to solve these problems. Our scheme achieved the follow factors: (1) anonymity, (2) mutual authentication, (3) non-repudiation, (4) avoid forgery attack [8].

The rest of the paper organized as follows: we detailed our proposed scheme in session 2. Next, we analyzed the security in session 3. Finally, we made a conclusion of our paper in session 4.

The Proposed Scheme

A. System architecture

In this paper, we use the public-key cryptography to transmit the session keys [9]. Consequently, we used the symmetric-key cryptography to transmit the diagnosed records. The architecture of our scheme is shown in Figure 1.

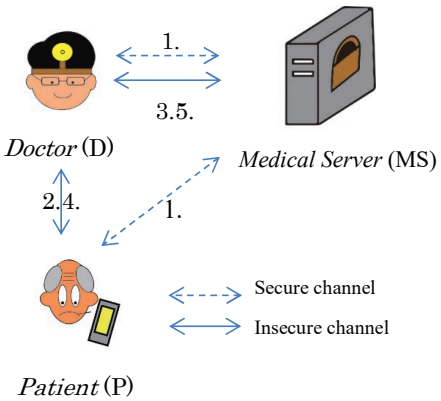

Fig. 1. The architecture of personal health care system

There are three parties involve the personal health system.

1. *Patient:* the owners of the medical mobile device. In anytime, the patient can send the health information to the doctor via the mobile device.
2. *Doctor:* the one diagnoses the information sent by the patient and stored the data in the medical server.
3. *Medical server:* the equipment stores the health record diagnosed by the doctor.

Our scheme divided into two phases. First, the registration phase that the patient and the doctor should register to the medical server. The patient and the doctor saved their IDs in the medical server. Second, the patient will go to see a doctor. This phase is called the doctor visiting phase. The doctor will receive the health status from the patient's mobile device. Then, the doctor will show his doctor license to get the diagnostic record. Therefore, the doctor can make a diagnosis. At the end, the doctor returns the diagnosed information to the patient. Also updates the electrical medical record to the medical server. The steps are described as below:

Step 1: At the beginning, the patient and the doctor register to medical server.
Step 2: Then the patient goes to see a doctor for a medical diagnose in person.

Step 3: The doctor receives the health record which stores in the medical server.
Step 4: The doctor then makes a professional diagnosed the information from the patient and the medical server.
Step 5: The doctor sends the diagnostic information to the patient and updates the electrical medical record in the medical server.

B. Notations

The notations of the proposed scheme are shown in table 1.

Table 1. Notations of this scheme

Notations	Means
ID_x	: identity of x
SK_x	: session key of x
r_x	: random numbers are generated by x
$Cert_D$	: the doctor's certificate
h (.)	: one-way hash function
$\|\|$	:concatenation function
$A \stackrel{?}{=} B$	: determines if A is equal to B
------>	: secure channel
——>	: insecure channel

C. The registration phase

In this phase, the patient chooses a doctor to visit. The patient shares the identity and the information to the doctor. And then the doctor registers to the medical server, the key generation center generates unique information. Both the doctor and the patient store the unique information generates by the medical server, the details are shown as follows:

Step 1: The patient chooses a random number r_P. The patient uses his/her identity ID_P and the random number r_P to compute a masked identity MID_P as follows:
$MID_P = h(ID_P \| r_P)$. (1)
Then, the patient transmits the identity and the masked identity to the doctor through the secure channel.

Step 2: After receiving the message, the doctor generates a random number r_D. And the doctor combines his/her identity and his/her masked identity to computes the masked identity MID_D as follows:
$MID_D = h(ID_D \| r_D)$. (2)
The doctor stores MID_P and ID_P. And the doctor sends the patient's identity ID_p, the masked identity $MID_{P\ of}$ patient, the doctor's identity ID_D, the masked identity MID_D of doctor and the doctor's license $Cert_D$ to the medical server.

Step 3: Upon receiving the messages, the medical server generates a random number r_{PD}. And uses the random number r_{PD}, the patient's masked identity MID_P and the masked identity MID_D of doctor to compute the masked identity MID_{MS} as follows:
$MID_{MS} = h(r_{PD} \| MID_P \| MID_D)$. (3)
And the medical server stores the patient's identity ID_P, the patient's masked identity MID_P, the doctor's identity ID_D of doctor, the masked identity MID_D of doctor. And then the medical server sends the message MID_{MS} to the doctor.

Step 4: After receiving the message, the doctor stores the masked identity MID_{MS} of medical server.

Step 5: Then, the doctor sends the identity ID_D of doctor, the masked identity MID_D of doctor and masked identity MID_{MS} of the medical server to the patient.

Step 6: After receiving the message, the patient stores the doctor's identity ID_D, the masked identity MID_D of doctor and the masked identity MID_{MS} of the medical server.

D. The doctor diagnosed phase

In this phase, the doctor can get the health status from the patient. The doctor also can find the diagnosed record from the medical server. When the doctor completely diagnosed the patient. He/she will send the diagnosis to the medical server and the patient. The details are as follows:

Step 1: The patient uses the doctor's public key PUK_D to encrypt his/her identity ID_P, the doctor's identity ID_D, and the health status M_{INF}. And the patient also signs with his/her identity ID_P and the patient's masked identity MID_P as follows:
$C_P = E_{PUKD}(ID_P \| ID_D \| M_{INF})$. (4)
$Sig_P = S_{PRK}(MID_P \| ID_P)$. (5)
And then, the patient sends C_p and Sig_P to the doctor through an insecure channel.

Step 2: After receiving the message, the doctor decrypts the message C_p as follows:
$ID_P \| ID_D \| M_{INF} = D_{PPKD}(C_P)$. (6)
The doctor checks if the signature Sig_P is valid or not as follows:
$MID_P \| ID_P \stackrel{?}{=} V_{PUKD}(Sig_P)$. (7)
If it is not valid, the doctor will terminate the diagnosed phase.

Step 3: The doctor uses the medical server's public key PUK_{MC} to encrypt the patient's identity ID_P, the doctor's identity ID_D and the doctor's certificate $Cert_D$. And the doctor also signs with his/her identity ID_D, the masked identity MID_D of doctor and the doctor's certificate as follows:
$C_D = E_{PUKMS}(ID_P \| ID_D \| Cert_D)$. (8)
$Sig_D = S_{PRKD}(ID_D \| MID_D \| Cert_D)$. (9)
And then, the doctor sends MID_D, C_D, and Sig_D to the medical server through an insecure channel.

Step 4: After receiving the message, the medical server decrypts the message C_D as follows:
$ID_P \| ID_D \| Cert_D = D_{PRKMS}(C_D)$. (10)
The medical server checks if the signature Sig_D is valid or not as follows:
$ID_D \| MID_D \| Cert_D \stackrel{?}{=} V_{PUKD}(Sig_D)$. (11)
If it is not valid, the medical server will terminate the diagnosed phase.

Step 5: The medical server uses the doctor's identity ID_D, the doctor's masked identity MID_D, the medical server's identity ID_{MS} and the medical masked identity MID_{MS} of server to compute the session key SK_{MS} as follows:
$SK_{MS} = h(ID_D \| ID_{MS} \| MID_D \| MID_{MS})$. (12)
Afterward, the medical server uses the doctor's public key PUK_D to encrypt the session key SK_{MS}, the patient's identity ID_P, the doctor's identity ID_D and the medical server's identity ID_{MS}. Also signs with the medical server's identity ID_{MS}, the medical server's masked identity MID_{MS} and the session key SK_{MS} as

follows:

$C_{MS} = E_{PUKD}(SK_{MS} \| ID_P \| ID_D \| ID_{MS})$. (13)

$Sig_{MS} = S_{PRKMS}(ID_{MS} \| MID_{MS} \| SK_{MS})$. (14)

And then, the medical server uses the session key SK_{MS} to encrypt the electrical medical record M_{EMR} as follows:

$C_{SKMS} = E_{SKMS}(M_{EMR})$. (15)

The medical server sends C_{MS}, Sig_{MS} and C_{SKMS} to the doctor.

Step 6: After receiving the message, the doctor decrypts the message C_{MS} as follows:

$SK_{MS} \| ID_P \| ID_D \| ID_{MS} = D_{PRKD}(C_{MS})$. (16)

The doctor checks if the signature Sig_{MS} is valid or not

$ID_{MS} \| MID_{MS} \| SK_{MS} \stackrel{?}{=} V_{PUKMS}(Sig_{MS})$. (17)

If it is valid, the doctor will decrypt the message M_{EMR} as follows:

$M_{EMR} = D_{SKMS}(C_{SKMS})$. (18)

Step 7: The doctor uses the patient's public key PUK_P to encrypt the patient's identity ID_P, the doctor's identity ID_D and the diagnostic information M_{DINF} which is diagnosed by the doctor. And the doctor also signs with his/her identity ID_D, the doctor's masked identity MID_D and the diagnostic information M_{DINF} as follows:

$C_{D2} = E_{PUKP}(ID_P \| ID_D \| M_{DINF})$. (19)

$Sig_{D2} = S_{PRKD}(ID_D \| MID_D \| M_{DINF})$. (20)

The doctor uses the patient's public key PUB_P to encrypt the doctor's identity ID_D, the patient's identity ID_P, new electrical medical record M_{EMR}^{NEW} which is diagnosed by the doctor and the doctor's certificate $Cert_D$ as follows:

$C_{D3} = E_{SKMS}(ID_D \| ID_P \| M_{EMR}^{NEW} \| CertD)$. (21)

The doctor sends $C_{D2}$and $Sig_{D2}$to the patient and sendsC_{D3} and MID_D to the medical server.

Step 8: After receiving the message, the patient decrypts the message C_{D2} as follows:

$ID_P \| ID_D \| M_{DINF} = D_{PRKP}(C_{D2})$. (22)

The patient checks if the signature $Sig_{D2}$is valid or not as follows:

$ID_D \| MID_D \| M_{DINF} \stackrel{?}{=} V_{PUKD}(Sig_{D2})$. (23)

Step 9: Once receiving the message, the medical server uses the session key SK_{MS} to decrypt the message C_{D3} as follows:

$ID_P \| ID_D \| M_{EMR}^{NEW} \| CertD = D_{SKMS}(C_{D3})$. (24)

If the certificate $Cert_D$ is valid, the medical server updates the electrical medical record as follows:

$M_{EMR} = M_{EMR}^{NEW}$. (25)

Security Analysis

A. Anonymity

In our scheme, all *IDs* of the parties are encrypted by the following Eqs. (4), (8), (13), (19), (21) during the authentication. So, our scheme achieves anonymity.

B. Mutual authentication

Mutual authentication means the parties that authenticates each other during communication [10]. The authenticate phases was divided into two parts.

(1) Authenticate between the patient and the doctor:
In our scheme, the patient authenticates the doctor server through verifying Sig_{D2} as Eq. (23). And the doctor authenticates the patient through verifying Sig_P as Eq. (7).

(2) Authenticate between the doctor and the medical server:
In our scheme, the doctor authenticates the medical server through verifying Sig_{MS} as following Eq. (17). Also the medical server authenticates the patient through verifying Sig_D as Eq. (11).

Therefore, our scheme achieves mutual authentication.

C. Forgery attack

In our scheme, the patient makes a signature during the authentication phase as following Eq. (5). The doctor makes a signature during the authentication phase as Eqs. (9), (20). The medical server makes a signature during the authentication phase as following Eq. (14). The adversary can't forge the signatures. So, our scheme can avoid the forgery attack.

D. Integrity

The patient's signature Sig_P can be verified by the doctor's public key as Eq. (7). Thus, the doctor can ensure the integrity of the message. And the doctor's signature Sig_D can be verified by the medical server's public key as Eq. (11). Thus, the medical server can ensure the integrity of the message. Also the medical server's signature Sig_{MS} can be verified by the doctor's public key as Eq. (17). Thus, the doctor can ensure the integrity of the message. And the doctor's signature Sig_{D2} can be verified by the patient's public key as Eq. (23). Thus, the doctor can ensure the integrity of the message. Our scheme completes the integrity.

E. Non-repudiation

The party not only can check the validity through the signature, but also the party can't deny the message through the signature mechanism [11]. In our scheme, all parties make a signature as following Eqs. (5), (9), (14), (20). It is to say that our scheme has non-repudiation. In table 2, we list the non-repudiation proof.

Conclusions

In this paper, we proposed a secure and efficient scheme for personal health care system. The doctor can easy make diagnoses and store the medical record. We think it is useful in our true life. Our scheme achieved the following security issues: (1) anonymity, (2) mutual authentication, (3) non-repudiation, (4) avoids forgery attack.

Table 2. The non-repudiation proof of our scheme

Evidence	Evidence Issuer	Evidence Holder	Verification Equation
$Sig_P = S_{PRK}(MID_P \| ID_P)$	Patient	Doctor	$MID_P \| ID_P \stackrel{?}{=} V_{PUKD}(Sig_P)$
$Sig_D = S_{PRKD}(ID_D \| MID_D \| Cert_D)$	Doctor	Medical Server	$ID_D \| MID_D \| Cert_D \stackrel{?}{=} V_{PUKD}(Sig_D)$
$Sig_{MS} = S_{PRKMS}(ID_{MS} \| MID_{MS} \| SK_{MS})$	Medical Server	Doctor	$ID_{MS} \| MID_{MS} \| SK_{MS} \stackrel{?}{=} V_{PUKMS}(Sig_{MS})$
$Sig_{D2} = S_{PRKD}(ID_D \| MID_D \| M_{DINF})$	Doctor	Patient	$ID_D \| MID_D \| M_{DINF} \stackrel{?}{=} V_{PUKD}(Sig_{D2})$

References

[1] World Health Organization, "The top 10 causes of death," 2017.

[2] J. Wei, X. Hu, and W. Liu, "An improved authentication scheme for telecare medicine information systems," *Journal of Medical systems*, Vol. 36, 2012, pp. 3597-3604.

[3] Z. Zhu, "An efficient authentication scheme for telecare medicine information systems," *Journal of Medical systems*, Vol. 36, 2012, pp. 3833-3838.

[4] M. K. Khanand and S. Kumari, "An authentication scheme for secure access to healthcare services," *Journal of Medical System*, Vol. 37, No. 4, 2013, pp. 1–12.

[5] F. T. Bin Muhaya, "Cryptanalysis and security enhancement of Zhu's authentication scheme for Telecare medicine information system," *Security and Communication Networks*, Vol. 8, 2015, pp. 149-158.

[6] B. Yüksel, A. Küpçü and Ö. Özkasap, "Research issues for privacy and security of electronic health services," *Future Generation Computer Systems*, Vol. 68, 2017, pp. 1-13.

[7] M. Hossain, S. R. Islam, F. Ali, K. S. Kwak, and R. Hasan, "An Internet of Things-based health prescription assistant and its security system design," *Future Generation Computer Systems*, 2017.

[8] A. K. Das, S. Zeadally and M. Wazid, "Lightweight authentication protocols for wearable devices," *Computers & Electrical Engineering*, Vol. 63, 2017, pp. 196-208.

[9] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah, and J. Shen, "A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server," *Computers & Electrical Engineering*, Vol. 63, 2017, pp. 168-181.

[10] C. T. Li, D. H. Shih and C. C. Wang, "Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems," *Computer methods and programs in biomedicine*, Vol. 157, 2018, pp. 191-203.

[11] P. Mohan and M. Singh, "Security Policies for Intelligent Health Care Environment," *Procedia Computer Science*, Vol. 92, 2016, pp. 161-167.