Hindawi
Journal of Sensors
Volume 2017, Article ID 3734764, 11 pages
https://doi.org/10.1155/2017/3734764

Research Article

An Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing

Jin-Xin Hu,[1] Chin-Ling Chen,[2,3] Chun-Long Fan,[1] and Kun-hao Wang[3]

[1]*School of Computer Science, Shenyang Aerospace University, Shenyang City, Liaoning Province, China*
[2]*Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung, Taiwan*
[3]*School of Information Engineering, Changchun University of Science and Technology, Changchun 130600, China*

Correspondence should be addressed to Chin-Ling Chen; clc@mail.cyut.edu.tw

Received 3 June 2016; Accepted 28 November 2016; Published 3 January 2017

Academic Editor: Hai-Feng Ji

Internet of Things (IoT) is the network of physical objects where information and communication technology connect multiple embedded devices to the Internet for collecting and exchanging data. An important advancement is the ability to connect such devices to large resource pools such as cloud. The integration of embedded devices and cloud servers offers wide applicability of IoT to many areas of our life. With the aging population increasing every day, embedded devices with cloud server can provide the elderly with more flexible service without the need to visit hospitals. Despite the advantages of the sensor-cloud model, it still has various security threats. Therefore, the design and integration of security issues, like authentication and data confidentiality for ensuring the elderly's privacy, need to be taken into consideration. In this paper, an intelligent and secure health monitoring scheme using IoT sensor based on cloud computing and cryptography is proposed. The proposed scheme achieves authentication and provides essential security requirements.

1. Introduction

With the rapid development of the Internet of Things (IoT), medical sensors, and Internet applications, online medical service has become possible in recent years. It is noteworthy that the number of elders with chronic disease is increasing every year. An aging society refers to a population structure model in which the aging population reaches or exceeds a certain proportion. According to the UN's traditional standard a region is regarded as an aging society when people over 60 years old account for 10% of the total population, while the new standard is people over 65 years old representing 7% of the total population. Between 2015 and 2050, the proportion of the world's population over 60 years will nearly double, from 12% to 22% [1]. An aging society means low fertility, aging population structure, and social security system lag. In the meantime, the health of the elderly has become a highlighted social issue. While more and more elders need long-term care, they also want to remain independent and active and reside in their own homes for as long as possible. Due to the lack of medical resources, they cannot be treated appropriately. The hospitals are filling up with an aging population, recovery groups and high risk groups. Continuous monitoring of critical vital signs of patients is a key process in hospitals. Today, this is usually performed via different cabled sensors attached to the patient and connected to bedside monitors [2]. The limitation here is that the elders are tied to bedside devices. Consequently, it has become feasible and necessary to perform personal diagnoses of medical diseases with the measurement repository without visiting hospitals [3]. With the increasing availability of medical sensors and IoT devices for personal use, this situation opens up a new application area for body sensor networks.

Wireless sensor networks (WSNs) are an emerging technology that possesses a huge potential to play an important role in many applications [4]. The rapid growth in physiological sensors, low-power integrated circuits, and wireless communication has enabled a new generation of wireless sensor networks, now used for purposes such as monitoring traffic, crops, infrastructure, and health. The body

area network field is an interdisciplinary area which could allow inexpensive and continuous health monitoring with real-time updates of medical records via the Internet [5].

However, with the presence of sensor networks, many challenges have emerged in terms of flexibility, scalability, and heterogeneous information services. The integration of WSN with cloud provides greater flexibility, unlimited resources, immense processing power, and the ability to provide quick response to the user [6]. Cloud computing provides scientists with a completely new model for utilizing the computing infrastructure. Computer resources and storage resources and applications can be dynamically provisioned (and integrated within the existing infrastructure) on a pay-per-use basis [7]. To provide more suitable and convenient network services, cloud computing has become even more flexible for personal use. Since the cloud is a broad collection of services, organizations can choose where, when, and how they use cloud computing [8]. There are different types of cloud computing services commonly referred to as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Many studies [3, 9] pointed out that cloud computing services are clearly the future trend. Cloud computing services are provided through a browser to access online programming applications, software, and data [9]. Cloud providers have to adhere to security and privacy policies to ensure their users' data remain confidential and secure [10].

Moreover, since the number of smart phones is estimated to reach 1 billion, traditional phones started to be gradually eliminated in 2015. The rapid development of smart phones and the related technology means that mobile computing is no longer the priority; we should also focus on reducing the computation cost and communication cost to achieve the optimal efficiency. Despite the agreement and certification of parties to browse medical information, the public still has concerns about the electronic medical record (EMR) system because of the information security issues, such as hacking, information transfer time, and long-term data management problems.

In recent years, many medical resources have been implemented for people seeking medical advice conveniently [11]. In the literature [12], researchers combine mobile devices and body sensors but do not sufficiently discuss security issues. Security issues of IoT sensors and medical systems have always been a vital aspect part of active research. It is important to consider security solutions to guarantee data authenticity, freshness, replay protection, integrity, and confidentiality. Some research, such as [13–15], specifically address security issues with respect to healthcare applications. In 2014, Ben Othman et al. proposed an efficient solution for securing data transmission, which combines compressive sensing with encryption and integrity checking [16]. In 2015, an ECC-based mutual authentication protocol for secure communication between embedded devices and cloud servers was presented in a paper by Kalra and Sood [17]. In 2016, Lounis et al. proposed a new cloud-based architecture for medical wireless sensor networks which can ensure the security of medical data without patients/doctors interventions [18]. However, these schemes still fail to ensure a patient's privacy and nonrepudiation. In this paper, we propose an intelligent and secure monitoring scheme using IoT sensors based on cloud computing to protect the elders' privacy.

The main problem here is that the elderly population is increasing every day and they should not be tied to their bed with monitoring machines, causing them inconvenience and entailing the waste of medical resources. On the other hand, the elderly with chronic conditions also have a high probability of suffering some acute diseases or episodes, such as heart attacks. Without the appropriate medical assistance, the consequences will be very serious. The EMR will be used in our scheme to provide more flexible and appropriate medical service. Due to the importance of the elders' privacy, the proposed scheme should focus on the advantages offered by the characteristics of cloud computing and the security of the elders' information.

The remainder of the paper is organized as follows: Section 2 describes the current approaches on the configuration of medical sensor networks. Section 3 introduces our scheme architecture for a wireless IoT sensor network and the setup procedure. In Section 4, we analyze the security issues of our scheme and compare it with other schemes. Section 5 contains some conclusions and offers some ideas for future work.

2. The Proposed Scheme

In our scheme, each party should register at the key generation center which will issue a pair of public key and private key, to communicate with other parties. The user also gets the pregenerated key; it can be used to encrypt the private health information. The elders can use a mobile device to connect to the IoT medical sensor which can collect the biological data. Seven parties are involved in our scheme as follows.

(1) Elder (E). The aging population with chronic disease (e.g., heart disease, diabetes, and hypertension) wears the IoT medical sensor which can collect biological data.

(2) Cloud (C): Intelligent Data Storage. The elder can access the cloud service to upload/download the health information via authentication. It can provide smart applications and send private health reports to the elder at set periods of time. Once there is an emergency situation, the cloud will notify the hospital.

(3) Hospital (H). It is a hospital where the elder can get physical inspection and the report. Once the elder's biological data are over a threshold, the hospital will notify the elder and dispatch an ambulance after it gets the cloud's notification.

(4) Key Generation Center (KGC). The key generation center will issue a pair of public key and private key for the registered parties. The user's pregenerated key and the time of the key's generation are stored in the database.

(5) IoT Medical Sensor (MS). It is the collecting device of the elder's biological data. The IoT medical sensor can also

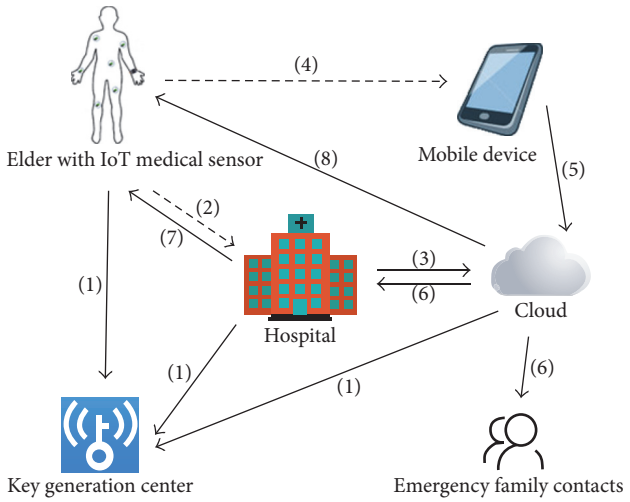

Figure 1: The system architecture.

transfer the collected data to the mobile device via Bluetooth (Bluetooth 4.0) and the mobile device can transfer the data to the cloud.

(6) Mobile Device (MD). A portable computing device with a unique International Mobile Equipment Identity (IMEI) which can connect with the IoT medical sensor. It can locate the elder with Global Positioning System (GPS) when there is an emergency and get the reports for normal situation.

(7) Emergency Family Contacts (EFC). They are the elder's family members.

The elder goes to the hospital for a health inspection and the report will be uploaded to the cloud. Every set period of time, the IoT medical sensor will collect the elder's biological data and transfer them to the cloud via mobile device. The hospital and the cloud process authentication procedure. The scenarios are described in Figure 1.

(1) The elder, the hospital, and the cloud must register at the key generation center in advance via secure channel.

(2) The elder goes to hospital for a physical inspection.

(3) The hospital uploads the elder's physical inspection report to the cloud.

(4) The IoT medical sensor gets the elder's biological data via set periods of time and sends it to the mobile device.

(5) The mobile device uploads the biological data to the cloud.

(6) The cloud compares the data sent from the mobile device with the standard values stored in the database. Once there is an emergency, the cloud notifies the hospital and contacts the elder's family in an acceptable time.

(7) After the hospital gets the notification, it sends messages and dispatches an ambulance to the elder.

(8) If the data collected by the IoT medical sensor are normal, the cloud sends a health report to the elder at set periods of time.

2.1. Notations. The following lists notations that will be used in our scheme:

ID_X: X's identity.

s: the secret value.

x: the KGC's private key.

$h_0()$: the hash function $h_0 : \{0,1\}^* \rightarrow h_1\{0,1\}^l$, $l = 256$.

$h_1()$: the hash function $h_1 : G_2 \times \{0,1\}^* \times G_1 \rightarrow \{0,1\}^l$, $l = 256$.

ΔT: the valid transmission time interval.

T_{X_i}: the ith timestamp generated by X.

$Data_{H_i}$: the elder's physical inspection report generated by the hospital.

$Data_{MS_i}$: the elder's biological data collected by the IoT medical sensor, for example, EGC, heart rate, oxygen saturation, blood pressure, body temperature, and blood glucose.

$Cert_X$: X party's identity certification being issued by the KGC.

IMEI: International Mobile Equipment Identity.

PK_X/SK_X: X's public/private key.

$key_{X\text{-}Y}$: the session key between X and Y.

$SE_K(M)/SD_K(M)$: using the symmetric key K to encrypt/decrypt a message M.

$S_{SK_x}(M)/D_{SK_x}(M)$: using the private key SK_x to sign/decrypt a message M.

$V_{PK_x}(M)/E_{PK_x}(M)$: using the public key PK_x to verify/encrypt a message M.

MSG_X: the patient's health information being generated by X.

MSG_{EM}: the emergency message.

MSG_{NM}: the normal report.

$A \stackrel{?}{=} B$: checking if A is equal to B.

——————→: insecure channel

- - - - - - - - - →: secure channel.

2.2. Registration Phase. Both the elder and the hospital must register at the key generation center in advance. The KGC will issue a pair of public key and private key for each party. The user will get the cloud's public key and use the pregenerated key to encrypt/decrypt the medical information. The KGC will also record the key's generation time in the database. The flowchart of the registration phase is shown in Figure 2.

(1) The elder, the hospital, and the cloud choose the identity $ID_E/ID_H/ID_C$ and send it to the key generation center through a secure channel. The elder should also send his/her

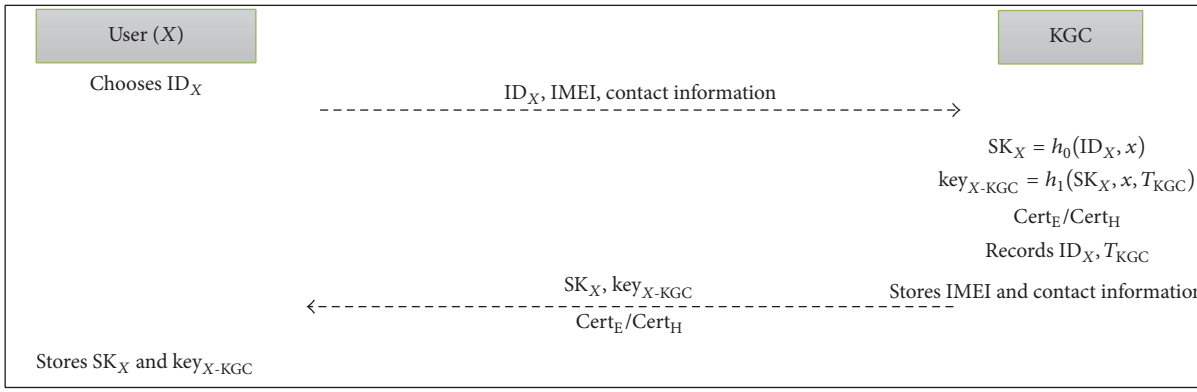

Figure 2: The registration phase.

mobile devices IMEI and personal contact information to the KGC, including emergency family contacts.

(2) After receiving the message, the KGC uses the private key x to compute the user's public key $PK_E/PK_H/PK_C$, the private key $SK_E/SK_H/SK_C$, and the pregenerated session key $key_{E\text{-}KGC}/key_{H\text{-}KGC}/key_{C\text{-}KGC}$ as follows:

$$\begin{aligned} SK_E &= h_0(ID_E, x), \\ SK_H &= h_0(ID_H, x), \\ SK_C &= h_0(ID_C, x), \\ key_{E\text{-}KGC} &= h_1(SK_E, x, T_{KGC}), \\ key_{H\text{-}KGC} &= h_1(SK_H, x, T_{KGC}), \\ key_{C\text{-}KGC} &= h_1(SK_C, x, T_{KGC}). \end{aligned} \tag{1}$$

Then, the KGC sends $(PK_E, SK_E, key_{E\text{-}KGC})$, $(PK_H, SK_H, key_{H\text{-}KGC})$, and $(PK_C, SK_C, key_{C\text{-}KGC})$ to the elder, the hospital, and the cloud, respectively. In addition, the KGC generates the certification $Cert_E/Cert_H$ for the elder and hospital, respectively.

(3) Each party stores $(PK_E, SK_E, key_{E\text{-}KGC})$, $(PK_H, SK_H, key_{H\text{-}KGC})$, and $(PK_C, SK_C, key_{C\text{-}KGC})$, respectively. The elder and hospital can use the certification $Cert_E/Cert_H$ to process authentication.

2.3. The Health Data Uploading Phase

2.3.1. The Hospital Uploads Physical Inspection Report Case. The elder goes to the hospital for a physical inspection. After the hospital and the cloud process authentication, the hospital uploads the physical inspection report to the cloud. The flowchart of the hospital uploading physical inspection report case is shown in Figure 3.

(1) The hospital uses the session key $key_{H\text{-}C}$ to encrypt the physical inspection report and makes a timestamp T_{H1}. The hospital uses the cloud's public key PK_C to encrypt $key_{H\text{-}C}$ and makes a signature Sig_1 as follows:

$$\begin{aligned} &MSG_{H1} \\ &\quad = (ID_H, ID_E, Data_{H1}, Data_{H2}, \ldots, Data_{Hn}, T_{H1}), \end{aligned} \tag{2}$$

$$C_1 = SE_{key_{H\text{-}C}}(MSG_{H1}), \tag{3}$$

$$C_2 = E_{PK_C}(key_{H\text{-}C}), \tag{4}$$

$$Sig_1 = S_{SK_H}(h_1(MSG_{H1})). \tag{5}$$

Then, the hospital sends Sig_1, ID_H, ID_E, $Cert_H$, C_1, C_2, and T_{H1} to the cloud.

(2) The cloud verifies the hospital's signature according to the hospital's identity ID_H and checks if the timestamp T_{H1} is valid or not as follows:

$$T_{C_1} - T_{H1} \leq \Delta T. \tag{6}$$

If (6) holds, the cloud uses the KGC's public key PK_{KGC} to verify the hospital's certification $Cert_H$. Then, the cloud finds $SD_{key_{H\text{-}C}}$ according to ID_H and uses the private key SK_C and session key $key_{H\text{-}C}$ to decrypt C_1 and C_2:

$$V_{PK_H}(Sig_1) \stackrel{?}{=} h_1(MSG_{H1}), \tag{7}$$

$$key_{H\text{-}C} = D_{SK_C}(C_2), \tag{8}$$

$$\begin{aligned} &(ID_H, ID_E, Data_{H1}, Data_{H2}, \ldots, Data_{Hn}, T_{H1}) \\ &\quad = SD_{key_{H\text{-}C}}(C_1). \end{aligned} \tag{9}$$

Afterwards, the cloud stores MSG_{H1} and Sig_1.

2.3.2. The Mobile Device Uploads Biological Data Case. In this phase, we consider the IoT medical sensors embedded into an elder's body. The elder uses the mobile device to transfer the biological data which are measured by IoT medical sensors to the cloud. The flowchart of the mobile device uploading biological data case is shown in Figure 4.

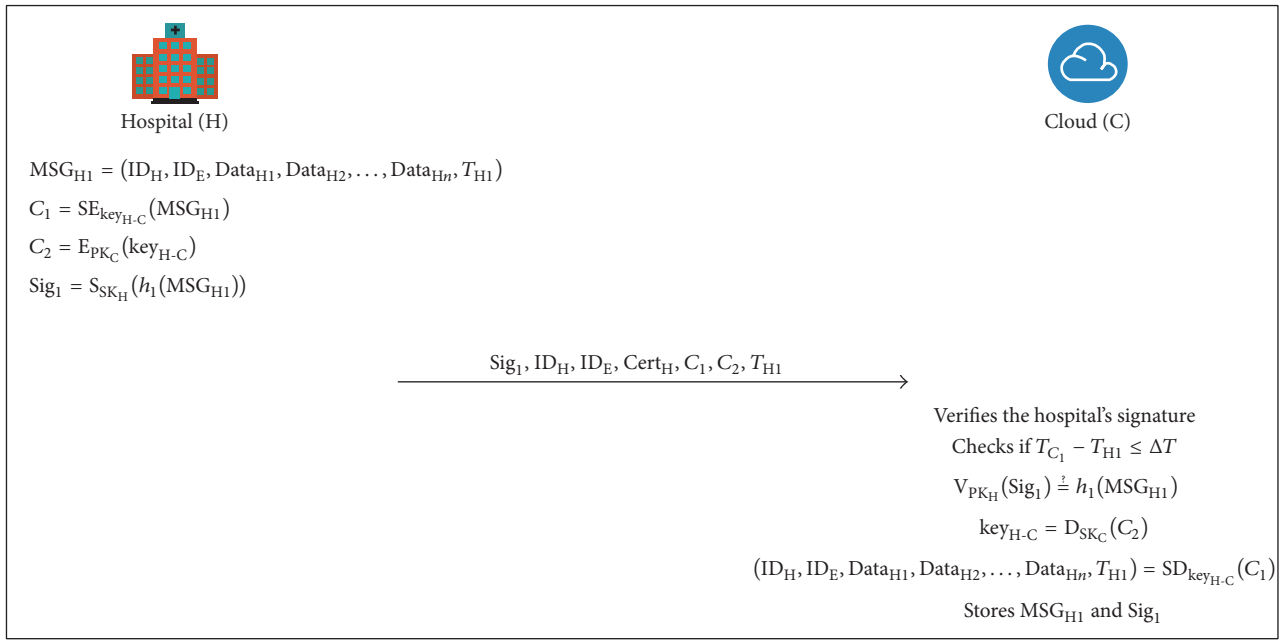

Figure 3: The hospital uploads physical inspection report case.

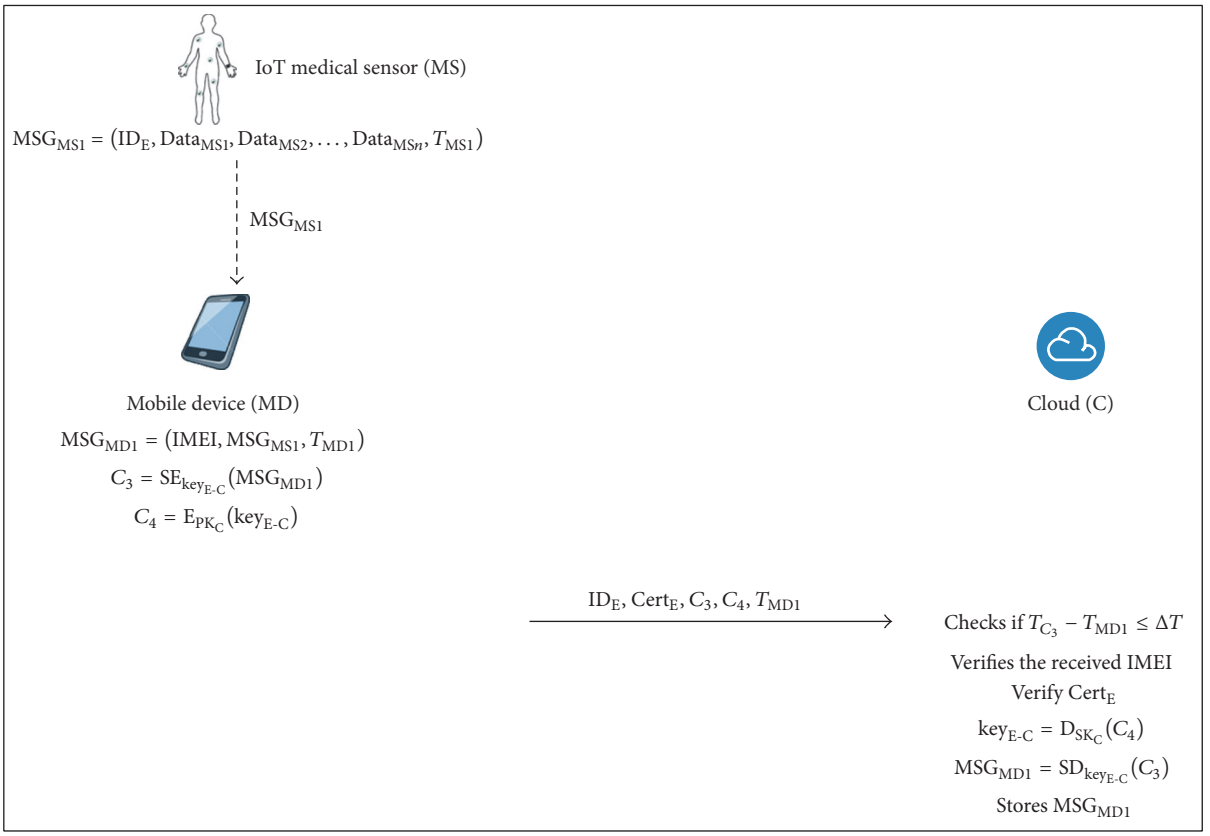

Figure 4: The mobile device uploads biological data case.

(1) The IoT medical sensor collects the biological data $\mathrm{MSG}_{\mathrm{MS1}}$ and sends them to the elder's mobile device through a secure channel:

$$\mathrm{MSG}_{\mathrm{MS1}} = \left(\mathrm{ID}_{\mathrm{E}}, \mathrm{Data}_{\mathrm{MS1}}, \mathrm{Data}_{\mathrm{MS2}}, \ldots, \mathrm{Data}_{\mathrm{MS}n}, T_{\mathrm{MS1}}\right). \tag{10}$$

(2) After receiving the message, the mobile device uses the session key $\mathrm{key}_{\mathrm{E\text{-}C}}$ to encrypt the elder's health information $\mathrm{MSG}_{\mathrm{MD}}$ and makes a timestamp T_{MD}. Afterwards, the mobile device uses the cloud's public key PK_{C} to encrypt $\mathrm{key}_{\mathrm{E\text{-}C}}$:

$$\mathrm{MSG}_{\mathrm{MD1}} = \left(\mathrm{IMEI}, \mathrm{MSG}_{\mathrm{MS1}}, T_{\mathrm{MD1}}\right), \tag{11}$$

$$C_3 = \mathrm{SE}_{\mathrm{key}_{\mathrm{E\text{-}C}}}\left(\mathrm{MSG}_{\mathrm{MD1}}\right), \tag{12}$$

$$C_4 = \mathrm{E}_{\mathrm{PK}_{\mathrm{C}}}\left(\mathrm{key}_{\mathrm{E\text{-}C}}\right). \tag{13}$$

Then, the mobile device sends ID_{E}, $\mathrm{Cert}_{\mathrm{E}}$, C_3, C_4, and T_{MD1} to the cloud.

(3) The cloud checks if the timestamp T_{MD1} is valid or not:

$$T_{C_3} - T_{\mathrm{MD1}} \leq \Delta T. \tag{14}$$

If (14) holds, the cloud verifies the received IMEI by finding the mobile device's registered IMEI which is stored in the database according to the elder's identity ID_{E}. If it holds, the cloud uses the public key $\mathrm{PK}_{\mathrm{KGC}}$ to verify the elder's certification $\mathrm{Cert}_{\mathrm{E}}$. Then, the cloud uses the private key SK_{C} and session key $\mathrm{key}_{\mathrm{E\text{-}C}}$ to decrypt C_3 and C_4, respectively:

$$\mathrm{key}_{\mathrm{E\text{-}C}} = \mathrm{D}_{\mathrm{SK}_{\mathrm{C}}}\left(C_4\right), \tag{15}$$

$$\mathrm{MSG}_{\mathrm{MD1}} = \mathrm{SD}_{\mathrm{key}_{\mathrm{E\text{-}C}}}\left(C_3\right). \tag{16}$$

Afterward, the cloud stores $\mathrm{MSG}_{\mathrm{MD1}}$.

2.4. The Notification Phase

2.4.1. The Emergency Case. When the cloud gets the elder's biological data from the mobile device, the cloud compares the data with the standard values stored in the database. If there is an emergency situation, the cloud sends the alert message to the hospital and contacts the emergency family simultaneously. Then, the hospital will contact the elder and dispatch an ambulance to help the elder, if necessary. The flowchart of the emergency case is shown in Figure 5.

(1) The IoT medical sensor collects the elder's biological data, such as ECG, oxygen saturation, blood pressure, and body temperature. The IoT medical sensor sends the biological data to the mobile device through a secure channel and makes a timestamp T_{MS2}:

$$\mathrm{MSG}_{\mathrm{MS2}} = \left(\mathrm{ID}_{\mathrm{E}}, \mathrm{Data}_{\mathrm{MS1}}, \mathrm{Data}_{\mathrm{MS2}}, \ldots, \mathrm{Data}_{\mathrm{MS}n}, T_{\mathrm{MS2}}\right). \tag{17}$$

(2) After receiving the message, the mobile device makes a timestamp T_{MD2} and integrates IMEI and $\mathrm{MSG}_{\mathrm{MS2}}$:

$$\mathrm{MSG}_{\mathrm{MD2}} = \left(\mathrm{IMEI}, \mathrm{MSG}_{\mathrm{MS2}}, T_{\mathrm{MD2}}\right). \tag{18}$$

The mobile device then uses the session key $\mathrm{key}_{\mathrm{E\text{-}C}}$ to encrypt $\mathrm{MSG}_{\mathrm{MD2}}$ and the cloud's public key PK_{C} to encrypt $\mathrm{key}_{\mathrm{E\text{-}C}}$. In the meantime, the elder uses the private SK_{E} and a signature Sig_2 via mobile device as follows:

$$C_5 = \mathrm{SE}_{\mathrm{key}_{\mathrm{E\text{-}C}}}\left(\mathrm{MSG}_{\mathrm{MD2}}\right), \tag{19}$$

$$C_6 = \mathrm{E}_{\mathrm{PK}_{\mathrm{C}}}\left(\mathrm{key}_{\mathrm{E\text{-}C}}\right), \tag{20}$$

$$\mathrm{Sig}_2 = \mathrm{S}_{\mathrm{SK}_{\mathrm{E}}}\left(\mathrm{IMEI}\right). \tag{21}$$

The mobile device sends Sig_2, ID_{E}, $\mathrm{Cert}_{\mathrm{E}}$, C_5, C_6, and T_{MD2} to the cloud.

(3) After receiving the message, the cloud checks if the timestamp T_{MD2} is valid or not:

$$T_{C_5} - T_{\mathrm{MD2}} \leq \Delta T. \tag{22}$$

If (22) holds, the cloud uses the private key SK_{C} and session key $\mathrm{key}_{\mathrm{E\text{-}C}}$ to decrypt C_6 and C_5 as follows:

$$\begin{aligned} \mathrm{key}_{\mathrm{E\text{-}C}} &= \mathrm{D}_{\mathrm{SK}_{\mathrm{C}}}\left(C_6\right), \\ \left(\mathrm{IMEI}, \mathrm{MSG}_{\mathrm{MS2}}, T_{\mathrm{MD2}}\right) &= \mathrm{SD}_{\mathrm{key}_{\mathrm{E\text{-}C}}}\left(C_5\right). \end{aligned} \tag{23}$$

The cloud then uses the KGC's public key $\mathrm{PK}_{\mathrm{KGC}}$ to verify the elder's certification $\mathrm{Cert}_{\mathrm{E}}$ and check if the mobile device's IMEI is the same as the registered IMEI:

$$\mathrm{V}_{\mathrm{PK}_p}\left(\mathrm{Sig}_2\right) \stackrel{?}{=} \mathrm{IMEI}. \tag{24}$$

The cloud then compares the elder's biological data with the standard value stored in the database. If some of the inspection data is beyond the threshold, the cloud uses the hospital's public key PK_{H} to encrypt the emergency message $\mathrm{MSG}_{\mathrm{C1}}$ and make a timestamp T_{C1}:

$$\mathrm{MSG}_{\mathrm{C1}} = \left(\mathrm{ID}_{\mathrm{C}}, \mathrm{ID}_{\mathrm{E}}, \mathrm{MSG}_{\mathrm{EM}}, T_{\mathrm{C1}}\right), \tag{25}$$

$$C_7 = \mathrm{E}_{\mathrm{PK}_{\mathrm{H}}}\left(\mathrm{MSG}_{\mathrm{C1}}\right). \tag{26}$$

The cloud sends ID_{C}, ID_{E}, $\mathrm{Cert}_{\mathrm{E}}$, $\mathrm{Cert}_{\mathrm{C}}$, C_7, and T_{C1} to the hospital.

(4) After receiving the message, the hospital checks if the timestamp T_{C1} is valid or not as follows:

$$T_{C_7} - T_{\mathrm{C1}} \leq \Delta T. \tag{27}$$

If (27) holds, the hospital uses the public key $\mathrm{PK}_{\mathrm{KGC}}$ to verify the cloud's and the elder's certification. Then, the hospital uses the private key SK_{H} to decrypt C_7:

$$\mathrm{MSG}_{\mathrm{C1}} = \mathrm{D}_{\mathrm{SK}_{\mathrm{H}}}\left(C_7\right). \tag{28}$$

(5) The hospital gets the elder's identity and obtains his/her contact information which is stored in the database. The hospital then gets the elder's location via the mobile device. According to $\mathrm{MSG}_{\mathrm{C1}}$, the hospital evaluates the elder's situation to determine whether to dispatch the ambulance to help the elder. If the elder is able to receive the message,

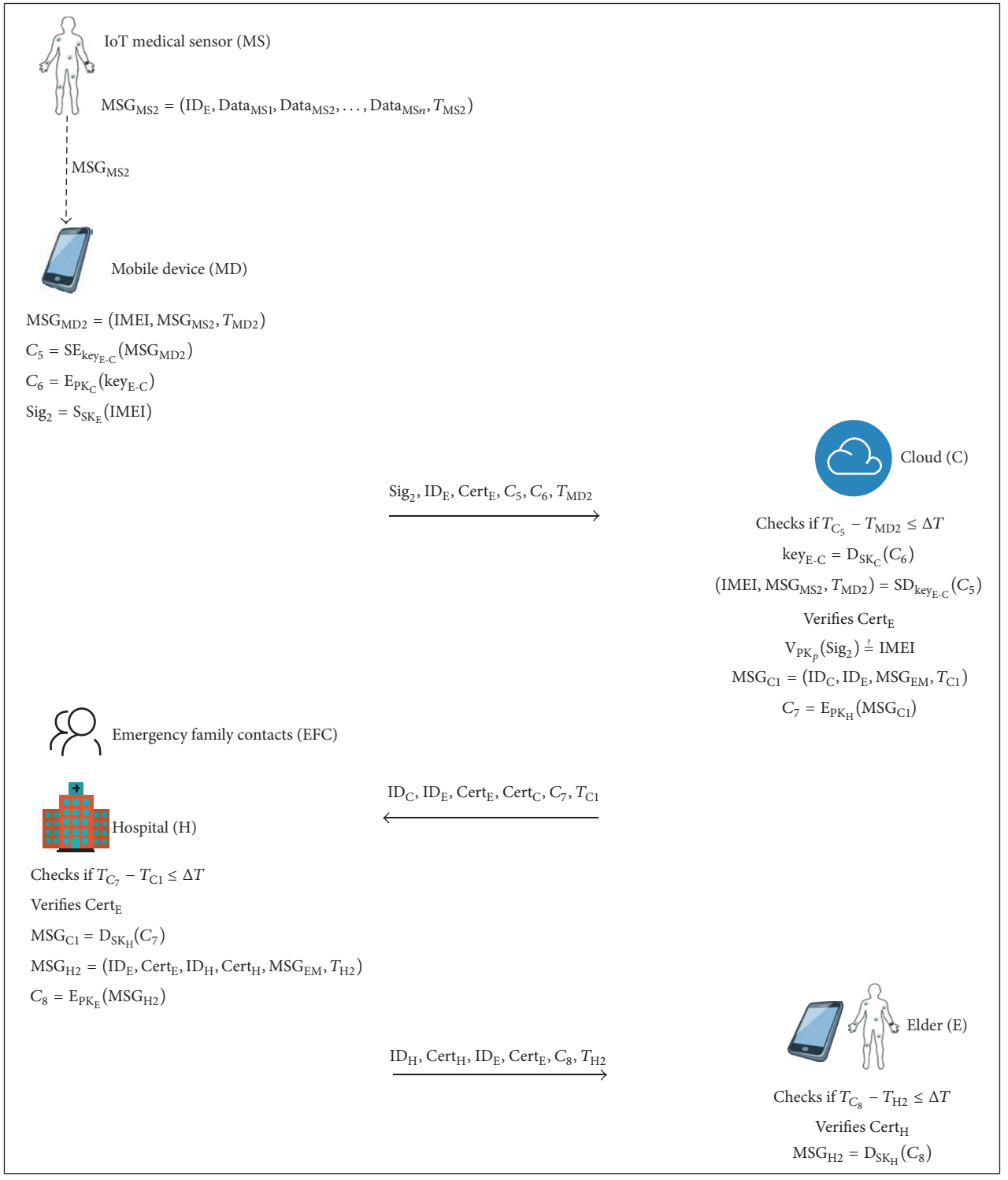

FIGURE 5: The emergency case.

the hospital uses the elder's public key PK_E to encrypt the notification MSG_{H2} and makes a timestamp T_{H2}:

$$MSG_{H2} = (ID_E, Cert_E, ID_H, Cert_H, MSG_{EM}, T_{H2}), \quad (29)$$

$$C_8 = E_{PK_E}(MSG_{H2}). \quad (30)$$

The hospital then sends ID_H, $Cert_H$, ID_E, $Cert_E$, C_8, and T_{H2} to the elder.

(6) The elder checks if the timestamp T_{H2} is valid or not when he/she receives the message:

$$T_{C_8} - T_{H2} \leq \Delta T. \quad (31)$$

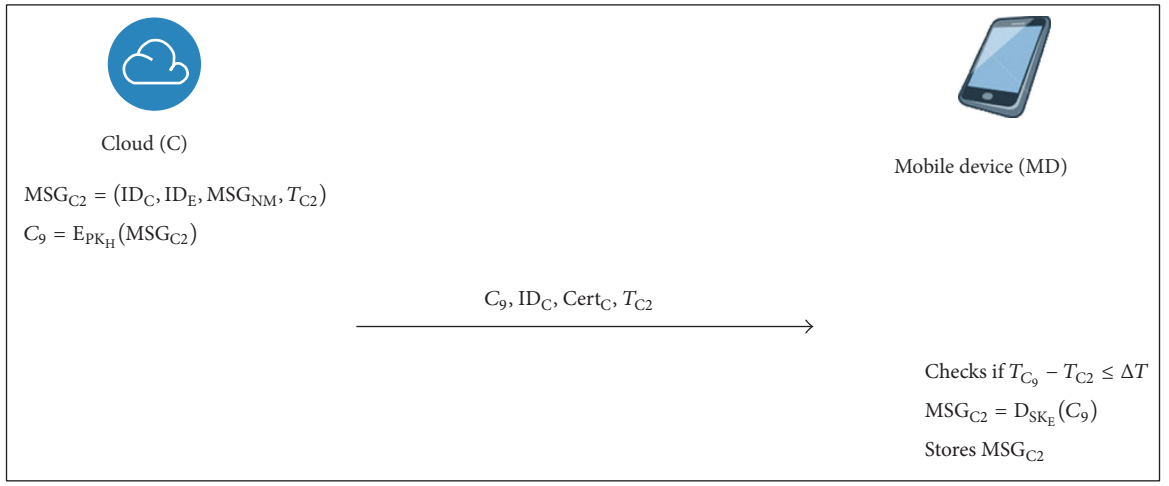

Figure 6: The normal case.

If (31) holds, the elder uses the public key PK_{KGC} to verify the hospital's certification and uses the private key SK_E to decrypt C_8:

$$MSG_{H2} = D_{SK_H}(C_8). \quad (32)$$

(7) If the elder is unconscious and cannot respond to the hospital's notification, the hospital gets the elder's location via GPS and dispatches an ambulance to help him/her directly.

2.4.2. The Normal Case. If the elder's biological data fall in the average scope, the cloud will send a report back to the elder via period of time. The flowchart of the normal case is shown in Figure 6.

(1) The cloud uses the elder's public key PK_E to encrypt the normal health report MSG_{C2} and makes a timestamp T_{C2}:

$$MSG_{C2} = (ID_C, ID_E, MSG_{NM}, T_{C2}), \quad (33)$$

$$C_9 = E_{PK_H}(MSG_{C2}). \quad (34)$$

The cloud sends the encrypted health information C_9, ID_C, $Cert_C$, and T_{C2} to the elder via set period time.

(2) After receiving the message, the elder checks if the timestamp T_{C2} is valid or not as follows:

$$T_{C_9} - T_{C2} \leq \Delta T. \quad (35)$$

If (35) holds, the elder uses the public key PK_{KGC} to verify the cloud's certification $Cert_C$. The elder then uses the private key SK_E to decrypt C_9.

$$MSG_{C2} = D_{SK_E}(C_9). \quad (36)$$

The elder stores MSG_{C2}.

3. Security Analysis

In this section, we present a security analysis to discuss how our scheme can defend against various attacks.

3.1. Replay Attack. In our scheme, we use the timestamp mechanism to defend against the replay attack. The receiver will verify if the timestamp is valid or not by checking the valid time interval via (6), (14), (22), (27), (31), and (35). Therefore, our scheme can defend against replay attack.

3.2. Man-in-Middle Attack. If there is a man-in-middle attack, our scheme will be able to resist it by checking the timestamps to verify if the messages are valid.

The elder, the hospital, and the cloud can prove his/her identity via certification in our scheme. The elder sends the certification $Cert_E$ to the cloud and the hospital. The hospital sends the certification $Cert_H$ to the cloud and the elder. The cloud sends the certification $Cert_C$ to the elder and the hospital. Every party will check if the received certification is valid or not.

In our scheme, during the health data uploading phase, the hospital and the mobile device use the session key $key_{H\text{-}C}/key_{E\text{-}C}$ and the public key PK_C to encrypt the information via (3), (4), (12), (13), (19), (20), (26), (30), and (34).

Other parties cannot decrypt the message without the private key or the session key, so attackers cannot achieve the man-in-middle attack.

3.3. Integrity. In the transmission process, the mobile device's IMEI is authenticated:

$$V_{PK_E}(Sig_2) \stackrel{?}{=} IMEI. \quad (37)$$

Therefore, tampering behaviors can be rapidly detected, so the proposed scheme can ensure data integrity.

3.4. Data Security. Our scheme involves the digital envelope mechanism. In order to ensure the elder's privacy, we use the public key to encrypt the symmetric key via (3), (12), (19), (26), (30), and (34), emergency information MSG_{EM}, and normal report MSG_{NM}. We use the symmetric key to protect the elder's secret biological data, via (4), (13), and (20).

Table 1: The nonrepudiation proof.

Nonrepudiation proof	Issuer	Holder	Nonrepudiation verification
$Sig_1 = S_{SK_H}(h_1(MSG_{H1}))$	Hospital	Cloud	$V_{PK_H}(Sig_1) \stackrel{?}{=} h_1(MSG_{H1})$
$Sig_2 = S_{SK_E}(IMEI)$	Elder	Cloud	$V_{PK_E}(Sig_2) \stackrel{?}{=} IMEI$

Table 2: The security comparisons of related works.

Security issue	Proposed scheme			
	Ben Othman et al. [16]	Kalra and Sood [17]	Lounis et al. [18]	Our scheme
Replay attack	N/A	Yes	N/A	Yes
Man-in-middle attack	N/A	Yes	Yes	Yes
Integrity	Yes	N/A	Yes	Yes
Data security	N/A	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes
Nonrepudiation	N/A	N/A	N/A	Yes
Privacy	N/A	N/A	N/A	Yes

3.5. Confidentiality. In our scheme, we use the asymmetric/symmetric key to ensure the safety of the patient's personal information as shown in (3), (4), (12), and (13).

In the notification phase, the mobile device uses the session key $key_{E\text{-}C}$ and cloud's public key PK_C to encrypt the information as shown in (19) and (20).

Then, the cloud uses the hospital's public key PK_H to encrypt the emergency message as shown in (26).

Afterwards, the hospital uses the elder's public key PK_E to encrypt the notification as shown in (30).

In the normal case, the cloud uses the elder's public key PK_E to encrypt the normal health report as shown in (34).

The elder's privacy information is protected. Therefore, our scheme can achieve confidentiality.

3.6. Nonrepudiation. The cloud can use the hospital's public key to verify the uploaded data via (7). The hospital cannot deny the uploading fact. The cloud can verify the correctness of the mobile device's IMEI via (24). The mobile device cannot deny the transmission. Every party can use the KGC's public key PK_{KGC} to verify whether the sender's certification is valid or not. The nonrepudiation proof is shown in Table 1.

3.7. Privacy. Data transmission on the Internet is insecure and the elder's private information may be revealed in the transmission process. In this paper, we use symmetric encryption to protect his/her personal privacy from unauthorized access. The elder's privacy is ensured.

3.8. Transmission Continuity. The elder's physical report and the biological data which are measured by IoT medical sensors will be stored in the cloud. In order to ensure transmission continuity, the receiver will send information to the sender. If the cloud has not received the elder's biological data in an acceptable time, which is recommended by the doctor, the cloud will notify the elder and contact his/her emergency family.

3.9. Security Analysis Comparison. According to the security issue, we make a comparison with other schemes in Table 2. In Table 2, Ben Othman et al.'s scheme [16] and Lounis et al.'s scheme [18] have some weaknesses. They cannot resist the replay attack. Ben Othman et al.'s scheme cannot ensure the security of data. And Kalra and Sood's scheme [17] cannot achieve integrity. The proposed scheme can resist the replay attack and man-in-middle attack and provide integrity and data security.

4. Discussions

4.1. The Computation Cost of Our Scheme. In this subsection, we present the proposed scheme's computation cost in Table 3. We use SHA-256 hash function, AES-symmetric encryption, Menezes-Vanstone cryptosystem, and signature generated by the ECDSA [20].

4.2. The Communication Cost of Our Scheme. In this subsection, we show the communication cost of the proposed scheme in Table 4. The highest communication cost in our scheme is for emergency case, while the cost is $5T_{ID} + 3T'_{AS} + 1T'_S + 1T'_{Sig} + 3T_T + 5T_{Cert} = 5*80 + 3*1024 + 1*256 + 1*1024 + 3*16 + 5*8192 = 45{,}760$ bits. The time of transmitting these messages is $45{,}760/20 * 10^{-6} = 0.9152$ ms under the 20 Mbps bandwidth network environment. Fast transmission makes our scheme feasible and efficient.

5. Conclusions

The elder's continuous medical monitoring is a serious problem. In this paper, we proposed a scheme with IoT sensor based on cloud computing to make the elder safely and conveniently monitored. In our scheme, the digital envelope, digital certification, signature, and timestamp mechanisms are involved. We also use the cloud's characteristics to make

Table 3: The computation cost of our scheme.

Case	Party		
	Elder	Hospital	Cloud/key generation center
The case when hospital uploads physical inspection report	N/A	$2T_{AS} + 1T_{Sig} + 1T_S + 1T_H$	$1T_{AS} + 1T_{Sig} + 1T_S$
The case when mobile device uploads biological data	$1T_{AS} + 1T_S$	N/A	$1T_{AS} + 1T_S$
The emergency case	$3T_{AS} + 1T_{Sig} + 1T_S$	$2T_{AS}$	$2T_{AS} + 1T_{Sig} + 1T_S$
The normal case	$1T_{AS}$	N/A	$1T_{AS}$

T_H: the time to execute a one-way hash function.
T_S: the time to execute a symmetric encryption/decryption operation.
T_{AS}: the time to execute an asymmetric encryption/decryption operation.
T_{Sig}: the time to execute/verify a signature.

Table 4: The communication cost of our scheme.

Case	Cost
The case when hospital uploads physical inspection report	$2T_{ID} + 1T'_{AS} + 1T'_S + 1T'_{Sig} + 1T_T + T_{Cert}$
The case when mobile device uploads biological data	$1T_{ID} + 1T'_{AS} + 1T'_S + 1T_T + T_{Cert}$
The emergency case	$5T_{ID} + 3T'_{AS} + 1T'_S + 1T'_{Sig} + 3T_T + 5T_{Cert}$
The normal case	$1T_{ID} + 1T'_{AS} + 1T_T + T_{Cert}$
Total	$8T_{ID} + 6T'_{AS} + 3T'_S + 2T'_{Sig} + 6T_T + 8T_{Cert}$

T_{ID}: the time to transmit the identity (80 bits).
T_T: the time to transmit a timestamp (16 bits).
T'_S: the time to transmit a symmetric encryption, ciphertext (256 bits).
T'_{AS}: the time to transmit an asymmetric encryption, ciphertext (1,024 bits).
T'_{Sig}: the time to transmit a signature (1024 bits).
T_{Cert}: the time to transmit a certificate (8192 bits) [19].

sure that the elder can get the available medical service conveniently. The asymmetric/symmetric encryption technology is used to protect the inspection report and the biological data of the elder. The elder's biological data and other personal information can be uploaded to the cloud via authentication. The hospital can notify the elder or dispatch an ambulance directly to him/her if there is an emergency situation. The elder can receive his/her personal health reports via set periods of time and browse the reports on their mobile device. Therefore our scheme can provide more flexible and accurate medical service as well as reduce the waste of medical resource.

Besides, our scheme can defend against the replay attack and man-in-middle attack and offer data security, integrity, nonrepudiation, and confidentiality in a cloud environment. As a result, the elder need not worry about the insecure access of medical records in our proposed medical environments.

In the future, we will focus on the bioinformatics certification to make the whole process easier for the elderly.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the Ministry of Science and Technology, China, under Contract nos. MOST 103-2632-E-324-001-MY3, MOST 105-2221-E-324-007, and MOST105-2622-E-305-004-CC2.

References

[1] World Health Organization, http://www.who.int/mediacentre/factsheets/fs381/en/.

[2] H. Baldus, K. Klabunde, and G. Müsch, "Reliable set-up of medical body-sensor networks," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2920, pp. 353–363, 2004.

[3] H. J. La, H. T. Jung, and S. D. Kim, "Extensible disease diagnosis cloud platform with medical sensors and IoT devices," in *Proceedings of the 3rd International Conference on Future Internet of Things and Cloud (FiCloud '15)*, pp. 371–378, IEEE, Rome, Italy, August 2015.

[4] Z. Zhang and X. Hu, "ZigBee based wireless sensor networks and their use in medical and health care domain," in *Proceedings of the 7th International Conference on Sensing Technology (ICST '13)*, pp. 756–761, Wellington, New Zealand, December 2013.

[5] https://en.wikipedia.org/wiki/Body_area_network.

[6] F. Banaie and S. A. H. Seno, "A cloud-based architecture for secure and reliable service provisioning in wireless sensor network," in *Proceedings of the International Conference on Computer and Knowledge Engineering (ICCKE '14)*, pp. 96–101, Mashhad, Iran, October 2014.

[7] C. Vecchiola, S. Pandey, and R. Buyya, "High-performance cloud computing: a view of scientific applications," in *Proceedings of the 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN '09)*, pp. 4–16, IEEE, Kaohsiung, Taiwan, December 2009.

[8] https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas.

[9] C.-L. Chen, T.-T. Yang, M.-L. Chiang, and T.-F. Shih, "A privacy authentication scheme based on cloud for medical environment," *Journal of Medical Systems*, vol. 38, article no. 143, 2014.

[10] A. Hendre and K. P. Joshi, "A semantic approach to cloud security and compliance," in *Proceedings of the IEEE 8th International Conference on Cloud Computing (CLOUD '15)*, pp. 1081–1084, New York, NY, USA, June 2015.

[11] C.-L. Chen, T.-T. Yang, and T.-F. Shih, "A secure medical data exchange protocol based on cloud environment," *Journal of Medical Systems*, vol. 38, no. 9, article 112, 2014.

[12] P. Tudor, W. Martin, B. Natalia, P. Zeeshan, and B. Leon, "Ambient Health Monitoring: the smartphone as a body sensor network component," *Innovation in Medicine and Healthcare Inmed*, vol. 6, no. 1, pp. 62–65, 2013.

[13] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1529–1535, 2012.

[14] S. Sahaa and S. Kumar Tomar, "Issues in transmitting physical health information in m-healthcare," *International Journal of Current Engineering and Technology*, vol. 3, no. 2, pp. 411–413, 2013.

[15] Q. Pu, J. Wang, and R.-Y. Zhao, "Strong authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 4, pp. 2609–2619, 2012.

[16] S. Ben Othman, A. Trad, and H. Youssef, "Security architecture for at-home medical care using Wireless Sensor Network," in *Proceedings of the 10th International Wireless Communications and Mobile Computing Conference (IWCMC '14)*, pp. 304–309, IEEE, Nicosia, Cyprus, August 2014.

[17] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," *Pervasive and Mobile Computing*, vol. 24, pp. 210–223, 2015.

[18] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Healing on the cloud: secure cloud architecture for medical wireless sensor networks," *Future Generation Computer Systems*, vol. 55, pp. 266–277, 2016.

[19] X.509—Wikipedia, https://en.wikipedia.org/wiki/X.509.

[20] D. Johnson and A. Menezes, "The elliptic curve digital signature algorithm (ECDSA)," Tech. Rep. CORR 99-34, Department of C & O, University of Waterloo, 1999.