Design and Implementation of a Secure Cloud Platform for Protecting and Managing Healthcare Medical Information

Chien-Lung Hsu¹, Hui-Ming Feng² & Bo-Yu Huang³*

¹,²,³Department of Information Management, Chang Gung University

Abstract

In present medical environment, hospitals purchase physiological measuring devices from different manufacturers because of multiple factors. However, protocols of physiological measuring devices are variety and are insecure for protect healthcare medical information. This study aims to design and implement a mobile application to measure and collect healthcare medical information from variety of medical devices which meet ISO/IEEE 11073 or Generic Attribute Profile (GATT) standards, and a cloud platform to manage such data sent from the proposed healthcare mobile application for healthcare. Since the healthcare medical information is sensitive for users, this study further designs a secure cryptographic protocol to protect the healthcare medical information from being disclosed. Contributions of this study are below: (i) The cloud platform is an integration one to collect and manage healthcare medical information from variety of medical devices. (ii) A cryptographic key management mechanism is proposed for cryptographic protocols used in the healthcare systems. (iii) The healthcare medical information is transmitted in a secure channel from being disclosed. (iv) A secure and efficient password-based user authentication protocol with key agreement is proposed.

Introduction

Due to some problems like legal and mutual competition between equipment manufacturers, usually only physiological measuring device provided by the same vendor that measuring information can communicate with each other. So interoperability between existing physiological measuring devices often be ignored. In fact, there are several issues emerge, when information of the physiological measuring device cannot communicate with each other. For example, recording data and adjusting the devices require to operate in manual mode, which will cause a waste of paper and time. The device cannot communicate also cause inconvenience on procurement. Probably because replace certain brands of equipment (Bajorek, 2011), the entire system must be replaced and the user will afford high cost of time and money.

If the physiological measuring devices between manufacturers can communicate with the same standards, physiological information can automatically uploaded to the server and managed by users with management platform. Users can take advantage of the management platform to collect, organize and analyze data. As a result, using management platform can reduce health care time and medical errors (Garguilo, 2007). Users also don’t worry about devices bought from different vendors cannot communicate. In order to integrate data transmission between measuring equipment and communication devices, ISO, IEEE and CEN standard organizations develop ISO / IEEE 11073, an open international communications standard (Garguilo, 2007; Noueihed, 2010). But still a few physiological measuring devices don’t use this standard (Van der Velde E.T., 2013).

In this study, taking into consideration that a variety of physiological measuring devices use different protocol, we implement a physiological information integration platform with ISO / IEEE 11073 and GATT protocol. However, the healthcare medical information is sensitive for users. We designs a secure cryptographic protocol to protect the healthcare medical information from being disclosed.

Related Works

It is divided to point of care (POC) and personal health data (PHD) in ISO/IEEE 11073. POC corresponds to the medical instruments in a hospital, and PHD corresponds to small measuring devices, such as sphygmomanometer,
pulse oximetry, etc., that make medical measuring devices have interoperability with communicating equipment under the standard.

There are two roles in ISO/IEEE 11073 PHD. One is manager, and the other is agent. Managers can be personal computers, mobile phones, health appliances, set-top boxes, and other related communication equipment. Agents can be treadmill, body weight scale, activity monitors, blood pressure monitors and other related small measuring devices (ISO, 2014). ISO/IEEE 11073 PHD is responsible for communications passing between both roles. Agents can transfer measurement values to the manager with ISO / IEEE 11073 PHD, and then the managers can provide these values to the remote service providing the corresponding service.

ISO / IEEE 11073 PHD consists of three main parts, namely service model, domain information model, and communication model. Managers and agents execute the instruction by service model during transmission. Its services divided into four kinds and defined as follows.

- GET service: Managers request corresponding information service to agents.
- SET service: Managers can set a property value that agents want to monitor.
- EVENT REPORT service: Agents return messages which can be divided into transmit equipment configuration properties, transmit measuring data and related events to managers.
- ACTION service: Managers call methods which agents supporting, like change agents of time, turn off the transmission and other functions.

Domain information model is an object-oriented model which allows an object contains a collection of multiple object messages and these object messages contain the device’s attributes, patterns, measuring values, historical data storage, remind event values, status, etc. Communication model transmits information according to the connected status between agents and managers in ISO/IEEE 11073-20601. It also describes the management status between agents and managers and can do stop instruction at any time in the state have been linked or transmission and confirming time overtime will be suspended back unconnected state.

In this study, heart rate watches and heart rate belt device was used base on Bluetooth 4.0 transmission. Both are currently using the GATT specification that was developed by Bluetooth Special Interest Group (SIG). The GATT turns attribute functions of Attribute Profile (ATT), such as reading, writing, accessing, and other basic functions, into the corresponding Universally Unique Identifier (UUID) Services (“Bluetooth Developer Porta,”). Currently UUID services are show as Table 1. Medical measuring equipment will depend on the different product, providing UUID service from one to multiple and allow users to select received information that they want according to the corresponding service. Heart rate watches and heart rate belt belong to measuring device which detect the heartbeat frequency, so we use equipment message 0x180A and heartbeat frequency 0x180D as main services.

<table>
<thead>
<tr>
<th>Specifications Name</th>
<th>Allocation Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Notification Service</td>
<td>0x1181</td>
</tr>
<tr>
<td>Battery Service</td>
<td>0x180F</td>
</tr>
<tr>
<td>Blood pressure</td>
<td>0x1810</td>
</tr>
<tr>
<td>Body Composition</td>
<td>0x181B</td>
</tr>
<tr>
<td>Bond Management</td>
<td>0x181E</td>
</tr>
<tr>
<td>Current Time Service</td>
<td>0x1805</td>
</tr>
<tr>
<td>Electric bicycle</td>
<td>0x1818</td>
</tr>
<tr>
<td>Bike speed and cadence</td>
<td>0x1816</td>
</tr>
<tr>
<td>Equipment message</td>
<td>0x180A</td>
</tr>
<tr>
<td>Universal access</td>
<td>0x1800</td>
</tr>
<tr>
<td>Universal attributes</td>
<td>0x1801</td>
</tr>
<tr>
<td>Glucose</td>
<td>0x1808</td>
</tr>
<tr>
<td>Thermometer</td>
<td>0x1809</td>
</tr>
<tr>
<td>Heart rate</td>
<td>0x180D</td>
</tr>
<tr>
<td>Human Interface Device</td>
<td>0x1812</td>
</tr>
<tr>
<td>Immediately alert</td>
<td>0x1802</td>
</tr>
<tr>
<td>Quick depletion</td>
<td>0x1803</td>
</tr>
<tr>
<td>Positioning and navigation</td>
<td>0x1819</td>
</tr>
<tr>
<td>Daylight Saving Time Changing</td>
<td>0x1807</td>
</tr>
<tr>
<td>Phone alert state service</td>
<td>0x180E</td>
</tr>
<tr>
<td>Reference time update service</td>
<td>0x1806</td>
</tr>
<tr>
<td>Running speed and rhythm</td>
<td>0x1814</td>
</tr>
<tr>
<td>Scanning parameters</td>
<td>0x1813</td>
</tr>
</tbody>
</table>
The Proposed System

System Architecture and Services

Physiological measuring information integration platform consists of two parts. One is physiological information integration platform, the other is physiological measuring APP. Physiological information integration platform is a website which let administrator control medical measuring information that health care worker and case manager could view, and manage medical measuring equipment. The health care worker and case manager can also view their patients’ information via the website and transform the measuring data into chart information. Patients can also view their physiological information on the website and more understand their own physical condition. Physiological measuring APP provide physiological measuring device to transmit data information with Bluetooth or transmit to wireless access point (WAP) in RF mode and then physiological measuring APP transmit physiological information to physiological information integration platform via WAP. Health care workers and patients can view physiological information and historical charts and curves that belong to their own authority through the physiological information integration platform. In addition, our study can be not only used in medical institutions, but also used in nursing home and medical community. The system structure is show as Figure 1.

![System Structure Diagram]

**Figure 1:** The system structure of physiological measuring information integration platform

The physiological information integration platform is divided to system management module, Nursing care module, and personal health management module according to perspective of manager, medical workers, and patient. The system function modules is show as Figure 2. In system management module, managers can control the following functions, mainly able to add care information and other data control which were required by medical workers and patients quickly, including a data table control, data table field management, the existing column compose new information table, medical measuring equipment sheet management, user authority management, data sheets authority management and user data management, etc., seven functions. In nursing care module, the health care workers can control the following functions, mainly able to view patients’ care information and enter related physiological information, including caring patients, measuring data chart and view information, etc., three functions. In personal health management module, patients can control the following functions, mainly able to view own information and set authority that let their family member view, including personal health, measuring data chart and sharing information, etc., three functions. In measurement module from physiological measuring APP, mainly able to help medical workers identify patients and read patients measuring information quickly. It is divided to two inputting
functions. One is single measuring device information corresponds to much patients, the other is single patient corresponds to multiple measuring devices information.

Figure 2: The system function modules

Secure Transmission Protocol

Algorithm:

- Choose a large prime number \( q \) and determine an elliptic curve function
  \[
  y^2 = x^3 + ax + b \mod q \neq 0
  \]
  such that it must satisfy that
  \[
  4a^2 + 27b^3 \mod q \neq 0
  \]
  where \( x, y \in \mathbb{Z}_q^* \) and \( a, b \in \mathbb{Z}_q \)

- Generate groups \( G_1 \) and \( G_2 \) of prime order \( q \) and the bilinear pairings is given as
  \[
  \hat{e} : G_1 \times G_1 \rightarrow G_2^*
  \]

- Select a base point \( P \in G_1 \) with order \( q \).

- Pick a random number \( s \in \mathbb{Z}_q^* \) as the system private key and compute \( P_{pub} = sP \) as the system public key.

- Choose two one-way hash functions
  \[
  H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^* \quad \text{and} \quad H_3 : \{0,1\}^* \rightarrow G_1^*
  \]

- Choose a symmetric cryptosystem (Ex: DES) such that \( E_k(m) \) means an encryption of the message \( m \) under key \( k \); \( D_k(m) \) means a decryption of the message \( m \) under key \( k \).

- Publish \( Pub_{params} = (G_1, G_2, P, q, H_2(.), H_3(.), P_{pub}, E_k(m)) \) and keep \( Priv_{params} = s \) secret.
Figure 3. Key generation phase of the proposed protocol from pairings

\[ a = \hat{\epsilon}(P + Q_j, S_i) \]
\[ B = \theta Q_i \]
\[ v_i = a^\theta \]
\[ C = E_{v_i}(ID_i) \]
\[ MAC_i = H_2(a \parallel v_i \parallel t_1 \parallel C \parallel ID_i) \]
\[ (B, MAC_i, t_1, C) \]
Check \( t_1 \)
\[ v'_i = \hat{\epsilon}(P_{pub} + S_j, B) \]
\[ ID_i = D_{v'_i}(C) \]
\[ a' = \hat{\epsilon}(P_{pub} + S_j, Q_i) \]
\[ H_2(a' \parallel v'_i \parallel t_1 \parallel C \parallel ID_i) \neq MAC_i \]
\[ v_j = (a')^{\lambda} \]
\[ K_{ij} = (v'_i)^{\lambda} \]
\[ MAC_j = H_2(K_{ij} \parallel v_j \parallel v'_i \parallel t_2 \parallel ID_j) \]
Check \( t_2 \)
\[ K_{ij} = v_j^{\theta} \]
\[ H_2(K_{ij} \parallel v_j \parallel v_i \parallel t_2 \parallel ID_j) \neq MAC_j \]
Implementation

In system implementation, we introduce the physiological information integration platform and physiological information integration platform measuring APP. There are three modules in physiological information integration platform, including system management module, nursing care module and personal health management module. We will introduce them one by one.

In system management module, it can control all data table and its columns. Managers can also give different authority that can use patient data according to different work by medical workers and case manage and set patients data table that was viewed by medical workers and case manager and the table which manager customize. The table which manager customize can arrange according to the columns of data table and then create a new table that was provided to health care workers to view. It also can create a new table and add measuring devices in equipment table management. In addition, the same measuring device can log in system by its ID to identify each device.

In nursing care module, medical workers can view patient who was cared now information by caring patient function. They also can view many patients physiological information in charts by measuring data function. Managers set the authority that allow to view patients related information in advance to medical workers.

In personal health management module, patient can display the newest measuring data or information on Personal Health. The measuring data can be showed in charts according to the measuring devices and measuring items that patient using. Patient also can know that who can view their information and set the authority by sharing information function.

In measuring module, Mobile nursing information system is based on Bluetooth 4.0 which enable mobile phones to receive physiological measuring devices data. It is divided to single patient corresponds to multiple measuring device and much patients corresponds to single measuring device. For the purpose to change patients ID quickly, we set three mode to switch ID, such as NFC, QR CODE and manual inputting.

Conclusion

In this study, we design an integration platform with three-tier architecture which can expand different physiological measuring protocols, such as ISO/IEEE 11073 and GATT standards and integrate the data from physiological measuring devices. Two protocols were also integrated in a physiological measuring APP. In addition, we also implement this platform from the standpoint of hospital and expect to be used in clinical care. Finally a cryptographic protocol can protect personal information when measuring data transmitted between devices.

References


