Design and Implementation of Secured u-Health Application Middleware with Smartphone and OTP

Inhyun Kim, Soo Young Kim, Sungsuk Kim, Heon Chang Yu, and Kwang Sik Chung

***Abstract*—As IT technologies are developing rapidly and people lives longer than before, demands of healthy lifestyle gets bigger. There is a growing need to intelligent medical treatment system in preparation for the aging society. Thus so many kinds of seamless medical monitoring system or u-health system were designed and built. u-health system collects and manages personal medical information so that u-health system and personal medical information should be secured.**

In this paper, we design and implement u-health application middleware that manages and controls emergency alert system connected with national emergency rescue system and u-health information system with patient medical information at hospitals. u-health application middleware collects patients' medical information with secured One Time Password(OTP), and analyses patients' medical information with u-health information system. After u-health information analysis, u-health application middleware decides status of patient and prepares for appropriate treatment and alert message. Patient medical information is relayed by smartphone in this paper.

***Index Terms*—U-health, medical information, medical data, OTP, security.**

I. Introduction

As information technology is developed and gets complex and confused, personal information get various and huge. And the ratio of aged population continuously rise, and insurance costs and medical costs will increase. u-health system can provide personalized healthcare and real-time emergency treatment for patient with wearable sensors and smartphone add-on sensors [1]-[4]. Since u-health system is based on seamless communication and personal medical information, and patient medical information is periodically delivered to u-health system through wired/wireless network, personal medical information could be attacked and hacked [5]. But secured personal patient medical information was not dealt with by previous research. And security guide and standardization secure protocol for u-health medical information are not constructed nor discussed. Now almost u-Health System does not mention nor dealt with secured medical information. As u-health system get widely used, secured patient medical information get important.

In this research, we propose u-health System with OTP that improves the security of patient medical data and does not burden patient medical information delivery networks. We design secured u-health Application Middleware that manages smartphone add-on sensors and collects and analyses patient medical information. Proposed u-health Application Middleware sends alert message to patients, patient family, doctors and emergency relief squad agents. Patient medical information between u-health application middleware and smartphone add-on sensors and u-health Application Middleware and u-health Emergency system is secured by OTP. Proposed u-health system uses OTP based key management method, and deliver real-time medical data and alert messages. The remainder of paper is organized as follows. Previous related works are analyzed in Section II. We introduce the architecture and function modules of proposed u-health application middleware and u-Health information exchange scenario with OTP. And in Section IV, we show implementation of u-health application middleware and demonstration. Finally, we conclude in Section V.

II. Related Works

Now u-health systems does mean not only remote medical treatments but also real-time patient health care, medical information tracking and alert service for emergency patients [6], [7]. Hospital information systems and Emergency alert systems should be included in u-health system. U-health system senses patients' medical data and medical data with attached sensors or smart phone sensors. As sensors become smaller and accurate, more medical data and medical data could be collected and more medical data and medical data could be vulnerable to IT hacking and IT attack. [8] Implemented several security algorithms such as Blowfish, data encryption standard (DES), advanced encryption standard (AES) and Rivest Cipher 4 (RC4) for u-health monitoring system. But this research has sensors and mobile device constraints such as low computing capacity, low power capacity and limited memory volume.

III. Proposed u-Health System

In u-health application middleware, sensors on patient body collect vital signals and send them in the form of medical data to the u-health application middleware. Those data are analyzed by the server in predetermined manner or doctor's order, and then the results are stored into patient medical information database as the form of medical information. Medical data are stored into patient medical

Manuscript received March 27, 2015; revised June 2, 2015.

Inhyun Kim is with IBM Korea, Inc., Seoul, Korea (e-mail: kinhyun@kr.ibm.com).

Soo Young Kim was with Korea Advanced Institute of Science and Technology, Daejeon, Korea (e-mail: sooyoungkim@kaist.ac.kr).

Sungsuk Kim is with Department of Computer Science, Seokyeong University, Seoul, Korea (e-mail: sukkim91@gmail.com).

Heon Chang Yu is with the Department of Computer Science and Engineering, Korea University, Seoul, Korea (e-mail: yuhc@korea.ac.kr).

Kwang Sik Chung) is with Department of Computer Science, Korea National Open University, Seoul, Korea, (e-mail: kchung0825@knou.ac.kr).

information database or informed to the target person after conversion into alert data. Whenever medical information is measured, u-health application middleware checks whether the medical information are within the predefined range.

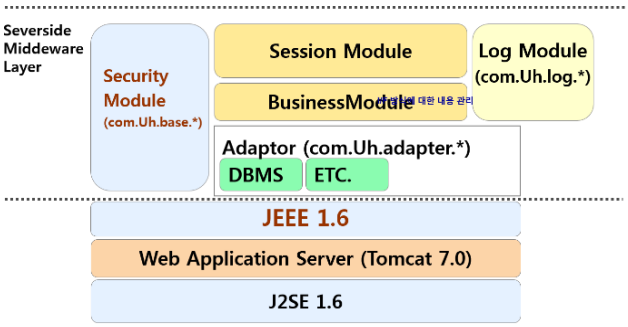

Fig. 1. Architecture of u-health application middleware.

If the medical information is out of the predefined range, it is designed to be initiated as alert, which will be delivered to the guardian, patients or doctors. When u-health application middleware decides that there may be a problem while it analyzes medical data based on the predefined conditions and collected information in medical analysis system, it sends emergency alert to the emergency alert system. A doctor or social workers can check either medical data or medical information for patients and can set to transmit urgent alert message for the patients.

TABLE I: FUNCTIONS OF U-HEALTH APPLICATION MIDDLEWARE

Manager	subcategory	Explanations of role
Interface Manager		The basic operation, administration parts necessary for the basic overall setup, registration to manage and control middleware
Session Manager		The setup/management parts for the compress of connecting objects to middleware
Security Manager		The setup/management parts for middleware security (with OTP)
Business Engine	Log/Update Module	Management processing parts for system maintenance : 1) to find the device executing the necessary functions for each service, 2) to return the service execution messages/results to the device, and 3) to check the presence of error by monitoring the system
	Database Adaptor	Module responsible for connection setup between Databases
	ETC Adaptor	Interface processing modules to the other external services

U-health application middleware consists of interface manager, session manager, security manager and Business Engine. Session manager plays a role of managing the data communication between server side middleware and the other devices as like in Fig. 1 and Table I. Security manager manages OTP using time value and open key. Security is maintained as following: at the initial connection, it gives a private key to the device. And some time later, it again generates another private key. Biz. Manager supports data transmission or smooth communication by registering setup information in case that there are different things in communication protocols or mechanisms.

IV. IMPLEMENTATION

U-health System consists of u-health application middleware, urgent rescue system, medical information analysis system, emergency alert system. Also, it includes sensors for measurement of vital signals and mobile devices (smartphones) which integrate and transmit collected medical data. u-health application middleware consists of u-health application middleware, sever management, security manager and u-health data control screen. Security Manager Deals with security keys distribution, encryption and decryption of data with J2EE 1.6 based Open Source with 'One-Time Password Generator' RFP 2289. Server management and u-health Data control screen is based on JSP 2.0. It consists of storage management of server operation information, u-health sensor device management, log management, and u-health data management.

By u-health application middleware, administration operation, patient information and patient's mobile device information, u-health data can be monitored. Function menu of u-health application middleware is made up of basic setting function, connection server setting function, interface registration function, log setting function, code management function, user management function, and u-health information management function. Basic setting function is for basic environment settings for operating servers, and database connection information for storing server information. Log setting function is a part that administration condition for operation logs management of u-health application middleware. Source code management function is application code in the implemented system. User management function administers user access rights for the u-health application middleware.

In Fig. 2 and Fig. 3, data in u-health application middleware is classified into three parts. Data division classifies sent data, and the criteria are IN(INVITE), KS(KeySend), KR(KeyRequest of smartphone), ES(ErrorSend) and DD(DataSend). Device ID is a unique id, given for each mobile device. Data division and DeviceID area are not transmitted with encryption specially.

Lastly, Data field is encrypted for transmission and composed of u-health type and u-health data before the encryption. u-health Type is defined and implemented by four characteristics, U01(blood pressure), U02(high blood pressure), U03(low blood pressure), and U04(body temperature). u-health Data is measured by real sensors. The actual transmitted data looks like below.

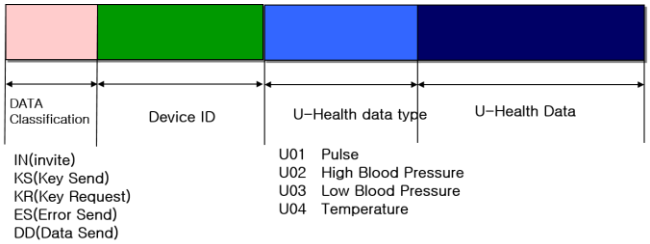

Fig. 2. Medical data transmission structure.

Medical analysis system is implemented to return 'true' for the normal range of u-health data, having distinction code of temperature(U04), blood pressure(U02, U03), pulse(U01), and return 'false' for abnormal range.

```
[I] Source DATA::::DD::er0007::w11Dg1Fdf9JgbFp1LlzPmw==
```

Fig. 3. Transmitted medical data.

Medical analysis system is implemented to return true for the normal range of u-health data, having distinction code of temperature(U04), blood pressure(U02, U03), pulse(U01), and return false for abnormal range. Urgent Rescue System is implemented to receive alert messages from u-health Application via TCP Socket transmission. The system sends SMS to designated mobile after receiving the alert call. Notification relay sever is a device which transfers notification information from u-health service, typically composed of SMS server or message server. In this paper, it is integrated to transfer data to corresponding mobile device when receiving those by transmission.

Vital signals are a heartbeat, blood pressure, body temperature. We utilized the random number, rather than the actual data, in order to generate body signals. Vital signals generator module is integrated into a function in mobile transmission module. Random number generation function produces one number given the minimum and the maximum for the random value, as shown below.

We assumed that medical data periodically are collected from external sensors and transferred to u-health application middleware. For this, we exploited J2EE-based android encoding module, network processing and multi-thread. The transmission from sensors to mobile device is described in a number of researches, so we omitted this. The actual implementation of mobile device and the log is shown below. Implemented u-health system is composed of u-health Application Middleware, medical information system and medical information analysis system. We integrate Urgent Rescue System into u-health urgent system and SMS Transmission Server. And the collection of medical data from patient sensor is supplemented with automated process module of smartphone (u-health client). Also, u-health client, a transmitter between mobile devices to u-health application middleware is implemented in smartphone.

```
[I] SRC Data : u01::93 [I] SND DATA : DD::er0007::eFjgfubC4pyh4qMZh2LOcw==
[SI] Source DATA :DD::er0007::eFjgfubC4pyh4qMZh2LOcw==
[GI] GET DATA :DD::er0007::7pwUdhfz+ZVvNqzq4ju6wg==/count:::3
[GI] GET DATA :DD::er0007::7pwUdhfz+ZVvNqzq4ju6wg==
[GI] GET DATA [0] CHECK :DD
[ICCCC] GET DATA::::DD::er0007::7pwUdhfz+ZVvNqzq4ju6wg==
```

Fig. 4. Encrypted low blood pressure value.

There are three scenarios for demonstration. First scenario is that medical data is collected by sensors, transmitted through u-health Client (smartphone) to u-health application middleware, and stored normally to medical information database. Second scenario is that the data, processed under the same condition, are received by u-health application middleware. But abnormality is detected by Medical Analysis System and medical information is sent to guardians and emergency rescue system. Lastly, if the encrypted medical data and information are periodically sent and transferred and OTP encrypted key is expired by u-health application middleware, u-health application middleware generates new OTP key with OTP Generate module and transmits medical data and information with the new OTP key. U-health application middleware includes medical information system, medical information analysis system.

At the first stage, sensors collects blood pressure(U01) 93, and the u-health client sends collected blood pressure to u-health application middleware in Fig. 4. The value U01 and 93 is encrypted with the given OTP key.

U-health application middleware receives and decrypts the encrypted medical data(blood pressure) in the data area, and stores the encrypted medical data(blood pressure) in medical information database in Fig. 5.

```
DD++++++++++++++++>>>>aRtnStr[0]DD
DD++++++++++++++++>>>>aRtnStr[1]er0007
DD++++++++++++++++>>>>aRtnStr[2]eFjgfubC4pyh4qMZh2LOcw==
[DECODE] skey=REINCUTSWAYRENTH
DD++++++++++++++++>>>>vdatau01: 93
 DB :: MOZ
```

Fig. 5. Decrypted low blood pressure data.

Authorized user can sign in u-health application middleware and check the blood pressure on-line. Captured display is as Fig. 6. U-health client sends blood pressure value 115 to server. Medical information analysis system decides that the blood pressure value 115 is abnormal for a patient.

```
[I] SRC Data : u01::115 [I] SND DATA : DD::er0007::F07pWFywq+LcFSbtCjonQA==
[SI] Source DATA :DD::er0007::F07pWFywq+LcFSbtCjonQA==
[GI] GET DATA :DD::er0007::7pwUdhfz+ZVvNqzq4ju6wg==/count:::3
[GI] GET DATA :DD::er0007::7pwUdhfz+ZVvNqzq4ju6wg==
[GI] GET DATA [0] CHECK :DD
[ICCCC] GET DATA::::DD::er0007::7pwUdhfz+ZVvNqzq4ju6wg==
```

Fig. 6. Decrypted low blood pressure data.

U-health application middleware analyzes the blood pressure with Medical Information analysis System and confirms abnormality in blood pressure of a patient in Fig. 7. Transmitted data to the Urgent Rescue System is shown as below.

```
DD++++++++++++++++>>>>aRtnStr[0]DD
DD++++++++++++++++>>>>aRtnStr[1]er0007
DD++++++++++++++++>>>>aRtnStr[2]F07pWFywq+LcFSbtCjonQA==
[DECODE] skey=REINCUTSWAYRENTH
DD++++++++++++++++>>>>vdatau01: 115
 DB :: MOZ
 USER :: uhealth
 PWD :: pass
 .URL :: jdbc:mysql://localhost:3306/uhealth?user=uhealth&pass=pass
 DRIVER :: com.mysql.jdbc.Driver
Connection OK!!!
[I] Medical Check
[I] Medical Check IN ======================
[I] VVVV : u01////115
 DB :: MOZ
 USER :: uhealth
 PWD :: pass
 .URL :: jdbc:mysql://localhost:3306/uhealth?user=uhealth&pass=pass
 DRIVER :: com.mysql.jdbc.Driver
Connection OK!!!
DD++++++++++++++++>>>>3
EM SEND Complete!
EM SEND Complete!
```

Fig. 7. Encrypted analyzed medical information.

Urgent Rescue System sends SMS to the registered mobile devices of related person (doctors, patient, patients family, etc.). Transmitted SMS is described in Fig. 8.

```
[I] ..... client Connect !!!!   Starting date=2014/03/24 오전 09:55
[I] SMS SEND    Starting date=2014/03/24 오전 09:55
[I] getdata=>u01::01049958612::abnormal, pulse is 115<=
[I] getdata1=>01049958612<=
[I] getdata2=>abnormal, pulse is 115<=
[I] Client END  Starting date=2014/03/24 오전 09:55
```

Fig. 8. Emergency alert SMS.

Whenever u-health application middleware receives the blood pressure, u-health application middleware 1) checks the OTP key usage number. If the OTP key usage maximum

number exceeds 300, u-health application middleware 2) sends KS for reproduction and distribution of new OTP key. u-health client (3) detects KS and medical data and medical information are encrypted with new OTP key and retransmit, after key usage number is reset to 0 in Fig. 9 and Fig. 10.

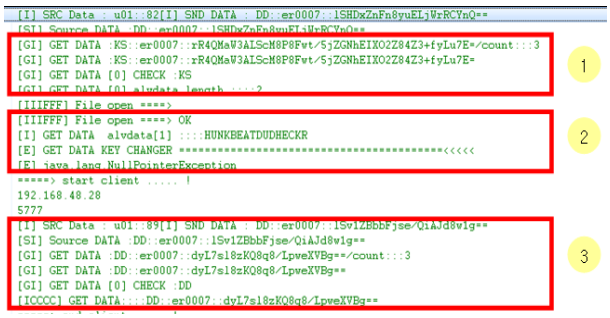

Fig. 9. OTP key regeneration process result.

Fig. 10. Encryption with new OTP key.

V. Conclusions

In this study, we propose secured u-health Application Middleware that securely and safely delivers patient's medical information with OTP protocol. OTP protocol is vulnerable to malicious IT attacks and economically very cheap. OTP protocol is used to send encrypted patient medical data to u-health application middleware. Proposed u-health system consists of u-health application middleware, u-Health clients and emergency alert system. U-health Application Middleware manages server administration function, patient information, patient mobile device information, and u-health data management web pages. . u-health clients is basically built on smart phone that could have sensors and collect patient medical data. U-health client periodically sends patient medical data that is sensed from patients. Emergency alert system manages alert messages for patient. If u-health application middleware detect abnormal situations of a patient, according to u-health application middleware's order, emergency alert system would classify person who receives an alert message.

Proposed secured u-health application middleware uses OTP protocol so that patient personal medical data and medical data can be protected from hacking and snooping. Also if patient medical information would be sent to outbound system as like emergency alert system and medical information management system, patient medical information would be encrypted by OPT key. Encrypted personal medical data and information can be safely delivered among u-health Application Middleware, u-health clients and emergency alert system. OTP protocol is light and economic to deal with mobile devices and sensors demands so that battery requirement, communication overhead and development complexity are satisfied.

In the future works, we will study security for communication between sensors and smart phone.

References

[1] H.-T. Lee, "Design and implementation of OTP authentication system supporting selective query," MS Thesis, Sangju University, Department of Computer Engineering, 2008.

[2] K. Y. Kim, "One-time password authentication system based on a study on," *KIISC*, vol. 17, no. 3, 2007.

[3] J. A. Harris, "OPA: A one-time password system," presented at ICPPW'02, 2002.

[4] S.-I. Cho, "Stream cipher-based OTP authentication protocols using clock-counter," MS Thesis, Donhseo University, Department of Ubiquitous IT, 2010.

[5] I. Kim, J. W. Kim, H. C. Yu, and K. S. Chung, "Design of secured u-health application middleware based on OTP," *WIT Transactions on Information and Communication Technologies*, vol. 49, pp. 1108-1113, March 2014.

[6] A. S. Almazyad and Y. Ahmad, "A new approach in T-FA authentication with OTP using mobile phone," *Communications in Computer and Information Science*, 2009.

[7] H. Raddum, L. H. Nestas, and K. J. Hole, "Security analysis of mobile phone used as OTP generators," *Lecture Notes in Computer Science*, p. 6033, 2010.

[8] J. Park, Y.-G. Lee, and G. Yoon, "Implementation of security algorithms for u-health monitoring system," *World Academy of Science, Engineering and Technology*, vol. 6, pp. 717-720, 2011.

Inhyun Kim obtained his bachelor's degree from the School of Life Science, Andong University of korea in 1999. He is currently a master student under the supervision of Prof. Kwang Sik Chung. His research is centered on development of secured u-health application server with OTP.

Sooyoung Kim received the B.E. in computer science from Korea University, Seoul, Korea, in 2014, and is pursuing the M.S. in computer science at Korea Advanced Institute of Science and Technology, Daejeon, Korea. Since 2014, she joined User and Information Lab as a research assistant. Her current research interests include machine learning, social network analysis, computational social science, and probabilistic topic modeling. Ms. Kim is a student member of ACM. She was the recipient of four-year full scholarship of Korea University.

Heonchang Yu received the B.S., M.S., and Ph.D. degrees in computer science and engineering from Korea University, Seoul, Korea, in 1989, 1991, and 1994, respectively.

He has been a professor of computer science and engineering with Korea University since 1998. From February 2011 to January 2012, he was a visiting professor of electrical and computer engineering in Virginia Tech. His research interests include cloud computing, grid computing, distributed computing, and fault-tolerant systems.

Sungsuk Kim received his B.S., M.S. and Ph.D. degrees in computer science and engineering from Korea University, Seoul, South Korea, in 1997, 1999, and 2003, respectively. From 2001 to 2003, he was an adjunct professor in Korea Polytechnic University. After then, he is an associate professor in the Department of Computer Science at Seokyeong university. His primary research interests lie in the areas of mobile/pervasive computing, data processing issues in wireless sensor networks/IoT. He is a member of the ACM and IEEE.

Kwang Sik Chung received the B.S., M.E., and Ph.D. degree from Korea University, in 1993, 1995 and 2000, respectively. His major was distributed mobile computing. Currently he has interesting in m-learning and cloud computing for smart learning. He is an assistant professor at Korea National Open University.