http://dx.doi.org/10.14400/JDPM.2014.12.1.573

# 원격의료서비스에서 생체정보를 이용한 암호화키 생성방법 연구

송충건*, 이근호*, 류갑상**
백석대학교 정보통신학부*, 동신대학교 컴퓨터학과**

# Process of the Encryption key using a Physical Information in the U-Healthcare Service

**Chung-Geon Song*, Keun-Ho Lee*, Gab-Sang Ryu****
**Division of Information and Communication, Baekseok University***
**Department of Computer Science, Dongshin University****

**요 약** 최근 세계가 고령화 사회로 진입함에 따라 U-Healthcare 서비스가 새롭게 각광받고 있다. 이러한 U-Healthcare 서비스가 발전하기 위해서는 U-Healthcare 환경에 최적화된 보안 솔루션이 요구된다. 그러나 U-Healthcare 환경은 기존 보안 솔루션의 적용이 어렵고 표준이 부재한 상황에 있다. 이러한 시점에서 안전한 U-Healthcare 환경을 구축하기 위해 데이터의 기밀성을 보장하는 목적으로 신체정보를 이용한 암호화키 생성방법을 제안하고자 한다.

**주제어** : 유헬스케어, 사물지능통신, 암호, 생체키, 키 관리

**Abstract** Recently as we enter into the world of an aging society, the U-Healthcare service is newly spotlighted. In order to secure this U-Healthcare, a development of security solution that is suitable for the U-Healthcare environment is required. But the U-Healthcare environment is difficult to apply the existing security solution with the lack of standards, a security solution with high completeness was not developed. At this point, in order to structure the safe U-Healthcare environment, a generating method of an encryption key using the body information that helps the effective key management and ensuring the confidentiality of the data is proposed.

**Key Words :** U-Healthcare, M2M, Encryption, Bio-key, Key management

## 1. Introduction

As the average human life expectancy increases, the world enters into an aging society and the U-Healthcare service is newly spotlighted. The medical paradigm will change the treatment to the prevention and the health care service under the ubiquitous environment will allow the health care to be taken anytime and anywhere will be located deep in our day-to-day life[1].

Received 17 December 2013, Revised 17 January 2014
Accepted 20 January 2014
Corresponding Author: Gab-Sang Ryu(Dongshin University)
Email: gsryu@dsu.ac.kr

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.otg/licenses/by-nc/3.0), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

In order for this type of U-Healthcare to be carried out safely, security technology for protecting against various security threats need to be preceded. Representative technology would be an accurate certification technology for user and hospital. Moreover, it is necessary to establish approach control for all the services[2].

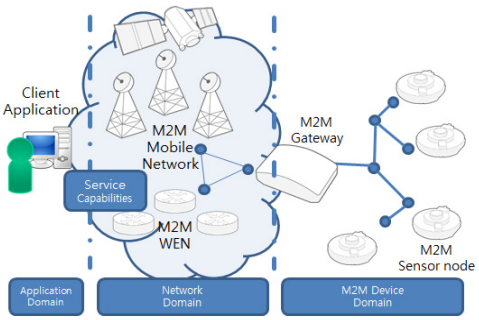
However, U-Healthcare service uses wired and wireless networks in a composite manner due to the application of M2M. Because application of mobile communication network is being considered, there is a limit when it comes to the direction of applying security solution that is developed based on the existing Internet net as it is.

Accordingly, this juncture requires a new method related to certification and approach control. As such, this paper seeks to propose a technique that is suitable for the U-Healthcare service environment when it comes to the data encryption method that is used to guarantee confidentiality in the data transmission domain.

## 2. Related Work

### 2.1 M2M

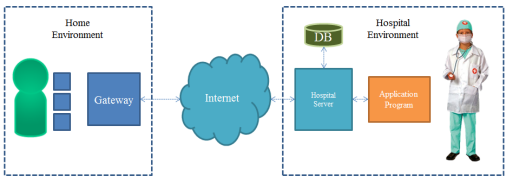
U-Healthcare service is one of the M2M applied services, and the structure follows the M2M structure that is shown on Figure 1[3]. M2M is the abbreviation for the Machine to Machine, and it refers to the communication form that takes place automatically among objects without direct human intervention. This is considered new communication paradigm, and it has infinite potential as the promising next generation technology.




[Fig. 1] M2M structure

Standardization for the M2M took place in the beginning at the standardization organizations such as ETSI and 3GPP[4]. Meanwhile, individual nations carried out their own standardization work. Currently, a world standardization organization called the oneM2M was established with the effort spearheaded by seven standard development institutions such as TTA, ATIS, ETSI, ARIB and others. As such, benefits such as increased compatibility of M2M products, and decreased development cost are expected[5].

### 2.2 U-Healthcare service




[Fig. 2] Remove medical service structure

U-Healthcare service has composite network structure in order to move data anytime, any where. The overall form is shown on Figure 2[6].

Sensor collects user information on real-time basis, and communicates with the Gateway using wireless means. Close range wireless communication technologies that are used in this part include RFID, Zigbee, Bluetooth and others. It is referred to as WBAN(Wireless Body Area Network), and extensive researches took place for the realization of U-Healthcare service[7][8][9][10].

Moreover, in order for the information collected from the Home Environment to get transmitted to hospital's server, Internet and mobile communication net that enable long distance networking are used. When Internet is used in this part, an advantage is that easy

compatibility with diverse existing systems is ensured. Meanwhile, it may run security risk due to the nature of public network. On the contrary, when mobile communication net is used, only specific subscribers can use it. Thus, although relatively secure, there is a limit to compatibility.

Information that is moved by using this type of broadband network is managed in the hospital's database. To carry out diagnosis, doctor verifies data using applied program in order to carry out diagnosis.

### 2.3 Algorithm for light weight symmetric key encryption

In general, public key encryption method is used to move cypher key safely, and symmetric-key encryption method is used to encrypt data in a very advanced manner. Because U-Healthcare service uses wireless and wired networks in a composite manner, structure-wise, light weight symmetric-key encryption method is required to carry out data encryption when realizing service. Currently, ARIA and HIGHT are the representative light weight symmetric-key encryption methods[11].

#### 2.3.1 ARIA

ARIA is the abbreviation comprised of the first letters of the Academy, Research Institute and Agency, and it expresses joint effort made by these three entities.

ARIA is optimized to the light weight, and it is a symmetric-key encryption algorithm that is designed by factoring in the realization of the hardware. Moreover, this is the block cypher algorithm that has Involutional SPN structure, and it has a block size of 128 bit. Arithmetic operation that is used in ARIA is the XOR operation, and it is carried out with simple byte unit operation.

#### 2.3.2 HIGHT

HIGHT is the abbreviation for HIGh security and light weigHT, and it is the cypher algorithm that was developed to apply to the computing environment that requires low power consumption and light weight.

This is the block cypher method and it assumes a block size of the 64 bit. Moreover, it is enacted as the standard for the international ISO/IEC block cypher algorithm.

〈Table 1〉 Comparison of HIGNT and AES performances

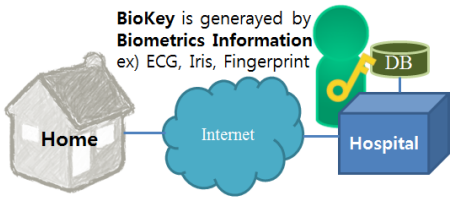
| Algorithm | GEs | Mbps | MHz |
|---|---|---|---|
| AES | 3400 | 9.9 | 80 |
| HIGHT | 3048 | 150.6 | 80 |

<Table 1> is the chart that compared the performance of the HIGHT algorithm and the performance of the AES that got designated by the NIST of the US as the standard for information processing. This demonstrates that the HIGHT's performance in the field of light weight encryption field is higher than that of the AES in overall.

## 3. Proposal on the key generation and management method

### 3.1 Encryption key generation using body information

U-Healthcare service requires in-depth health check-up in order to provide optimized service to user. Because this uses precise medical equipment, visit to the hospital is essential. Method for generating the cypher key that is proposed takes place when a user visits hospital for the first time.

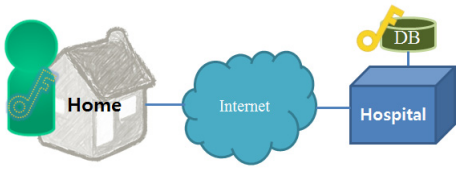



[Fig. 3] Generation of symmetric-key using body information

Encryption is carried out by using symmetric-key encryption method in order to maintain confidentiality when using data of user via network. When symmetric-key encryption method is used, it is necessary for the sender and receiver to share the same cypher key via Secure Chanel.

In case of the proposed cypher key generation method, this becomes the most ideal Secure Chanel since cypher key is set during the first visit to the hospital, and thus key is generated when the sender and receiver are at the same space.

When cypher key is generated, this is carried out by using user's body information. Key generated as such is stored in hospital's database. When hospital needs it, it is used by exporting from database. Moreover, user does not need to store key separately since user's body information is the key. If necessary, sensor acquires body data to generate key.




[Fig. 4] Status after symmetric-key generation

After completing the above mentioned process, user receives U-Healthcare service from Home Environment, and user and hospital manage the same symmetric-key and use the key to send and to receive each other's data.

## 3.2 Body information requirements used for cypher key

### 3.2.1 Uniqueness

In case of symmetric-key encryption method, the person who has the key has the authority to interpret encrypted data. It should be made impossible to provide this authority to a third party and to have other same key. Thus, body information that is used for the cypher key generation has to be unique to discern out user.

### 3.2.2 Ease of collection

In the U-Healthcare, collection of body information takes place on a real-time basis from remote area, and it takes place repeatedly at specific time. Thus, collection method should be easy, and less time is required for the collection.

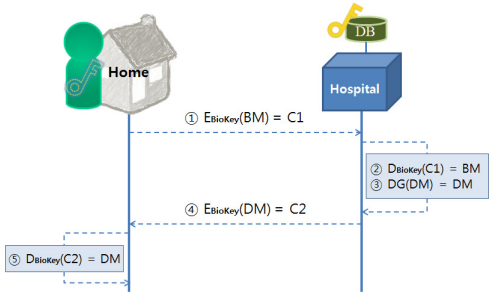
### 3.2.3 Inalterability

Completely different key will be generated when the body information used for the generation of cypher key changes. In this case, service solubility is affected. Thus, body information that is used for cypher key should be that which does not change forever.

## 3.3 Encryption process

〈Table 2〉 Project selection matrix rules

| | |
|---|---|
| **BM** | Biometrics Message |
| **DM** | Diagnosis Message |
| **BioKey** | Biometrics Symmetric-key |
| **E()** | Encryption function |
| **D()** | Decryption function |
| **C1, C2** | Cryptograph |




[Fig. 5] Data transmission process

1) Transmission of C1 that encrypted BM by using BioKey

Encryption is carried out using E() function, which is symmetric-key encryption method to transmit in order to prevent disclose of the BM, which is user's

body information to a third party when transmitting to hospital. As for the encryption key, BioKey generated with user's body information is used.

2) BM acquisition by deciphering C1 with BioKey

Hospital server uses D() function in order to decipher the encrypted data. Because encrypted E() function uses symmetric-key encryption method, deciphering is carried out by using the BioKey that is the same as that of the cypher key.

3) DM extraction using BM

DG is the function that can extract DM, which is diagnosis information and that uses body information as the medium variable, and it plays the role of executing automatically by detailing out the doctor's diagnosis process.

4) Transmission of C2 encrypted with DB using BioKey

Message is encrypted using E() function which is symmetric-key encryption method to transmit in order to transmit DM, diagnosis information extracted from hospital to user safely while maintaining confidentiality.

5) DM acquisition by deciphering with C2 function BioKey

User can get diagnosis for body information in the end after receiving the C2 which is the encrypted diagnosis information from hospital and after deciphering it.

## 4. Performance analysis

### 4.1 Confidentiality

Biometric characteristics are very complex. so that one encryption key is generated using the encryption used is sufficient enough to ensure confidentiality.

User's body information that moves via network is encrypted by using symmetric-key encryption method so that a third party cannot open it. Thus, confidentiality for the data is guaranteed.

### 4.2 Key management

In existing authentication systems, authentication key management is required to user. But, In proposing solution, authentication key is automatically governed.

Because key is generated based on user's physical characteristics, key is always in the user's body. Moreover, key is collected automatically with sensor. Thus, user is freed from the burden of having to manage the key. <Table 3> express comparison with other certification systems.

〈Table 3〉 Comparison with other certification systems

| Means of Authentication in U-Healthcare | Key Management |
|---|---|
| ID/PASSWORD | Passive |
| Certificate | Passive |
| Proposed Solution | Automatic |

## 5. Conclusion

In this paper, for securing the efficient confidentiality of the data in the U-Healthcare service environment, a creation of the symmetric key was proposed. After the completion of the standardization of M2M which are currently being progressed in the oneM2M, will be expected to contribute to the structuring of a safe U-Healthcare service by proposing the detailed protocol.

## REFERENCES

[1] JiEun Song, "Security Issues and Its Technology Trends in u-Healthcare", Electronics and Telecommunications Trends, Vol.22, No.1,

February, 2007.
[2] Bo-Soo Kim, U-Healthcare & Medical Information System of Status and Operative Challenges for Integrated Medical Information System, Digital Policy Journal, 2011.
[3] David Boswarthick, “M2M Activities in ETSI”, SCS Conference, July, 2009.
[4] Sanggeun Yu, “Smart Mobile Services - M2M Technology and Its Standardization Trends“, Electronics and Telecommunications Trends, Vol.26, No.2, April, 2011.
[5] http://www.onem2m.org
[6] ChungGeun Song, “Threat to Security of Remote-Controlling Medical Care Service and Countermeasure Under U-Healthcare Environment”, 2nd ICCT, pp. 319-321, July, 2012.
[7] Jeong YoonSu, Lee SangHo, "U-Healthcare Service Authentication Protocol based on RFID Technology" The Journal of Digital Policy & Management, Vol.10, No.2, March, 2012.
[8] Chang YunSeok, Kim Bo Yeon, "A Wireless ECG Measurement System based on the Zigbee USN", Korea Information Processing Society Journal, Vol.18-C, No.3, June, 2011.
[9] Gil Lee, Gopal Gupta, Lakshman Tamil, "A Scalable Wireless Body Area Network for Bio-Telemetry", Journal of Information Processing Systems, Vol.5, No.2, June, 2009.
[10] Cory Cornelius, David Kots, “On Usable Authentication for Wireless Body Area Networks”, Journal Title, Presented at HealthSec, August, 2010.
[11] http://seed.kisa.or.kr
[12] Byung-Seok Yu, Sung-Hyun Yun, “The Design and Implementation of Messenger Authentication Protocol to Prevent Smartphone Phishing”, Journal of the Korea Convergence Society, Vol.1, No.1, pp. 9~14, 2010
[13] Won-Jun Jang, Hyung-Woo Lee, “Biometric One-Time Password Generation Mechanism and its Application on SIP Authentication“, Journal of the Korea Convergence Society, Vol.1, No.1, pp. 93~100, 2010
[14] Seung-Soo Shin, Kun-Hee Han, “Design of the Mail Protocol with Perfect Forward Security”, Journal of the Korea Convergence Society, Vol.2, No.2, pp. 13~19, 2011

**송 충 건(Song, Chung Geon)**

・2010년 3월 ~ 현재 : 백석대학교 정보통신학부(이학사)
・E-Mail : security0730@naver.com

**이 근 호 (Lee, Keun Ho)**

・2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
・2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
・2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수
・관심분야 : M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호, ISMS(정보보호관리체계), 정보보호사전점검
・E-Mail : root1004@bu.ac.kr

**류 갑 상(Ryu, Gab Sang)**

・1983년 2월 : 전남대학교 전산학과 (공학사)
・1985년 2월 : 전남대학교 전산학과 (공학석사)
・2000년 2월 : 고려대학교 컴퓨터학과(이학박사)
・1985 ~ 1996. : Research Engineer, Korea Institude of Machine and Metal
・1996년 3월 ~ 현재 : 동신대학교 컴퓨터학과 교수
・관심분야 : CAD/CAM, Software Engineering, Cloud Computing
・E-Mail : gsryu@dsu.ac.kr