Journal of the Korea Academia-Industrial cooperation Society
Vol. 15, No. 6 pp. 3865-3871, 2014

http://dx.doi.org/10.5762/KAIS.2014.15.6.3865
ISSN 1975-4701 / eISSN 2288-4688

U-Health환경에서 안전한 개인정보 관리를 위한 통합 인증스키마 설계

민소연[1*], 진병욱[2]
[1]서일대학교 정보통신과, [2]숭실대학교 컴퓨터학과

Design of Integrated Authentication Scheme for Safe Personal Information Management in a U-Health Environment

So-Yeon Min[1*], Byung-Wook Jin[2]
[1]Department of Information Communication, Seoil University
[2]Department of Computer Science, Soongsil University

요 약 U-health Service는 환자와 의료진과의 언제 어디에서나 의료서비스를 제공하는 것을 지칭하며 정보통신 기술과 보건의료를 융합한 서비스로 정의하고 있다. 그러나 환자의 의료정보, 개인정보 유출과 같은 사례가 발생하고 있고, 또한 네트워크를 통하여 데이터 송수신을 계승하므로써 기존 유・무선기반의 보안위협사항을 계승하는 취약점이 있다. 그러므로 본 논문에서는 U-Health Service에서 발생하는 취약점을 보완하고자 통합 인증스키마를 설계하여 안정한 개인정보에 대한 관리 시스템을 제안하였다. 제안프로토콜에서는 ID-Based Encryption을 활용하여 사용자 등록, 의료기관과 사용자간의 인증, 데이터 통신 암·복호화, 사용자 정보 폐기에 대한 프로토콜을 설계하였으며, 이에 따른 기존시스템 및 PKI Based 기반 통신과정과 보안성과 안전성에 관하여 분석하였다.

Abstract The U-health service provides medical services with patients anytime or anywhere and is defined as the service that combines information and communication technology with health and medical service. However, it causes some troubles, such as the disclosure of patients' medical information or data spills (personal information extrusion). Moreover, it has the weak point of the security threats associated with data based on existing wire-wireless systems because it conducts data transmission and reception through the network. Therefore, this paper suggests a safe personal information management system by designing integrated certification schema that will help compensate for the weaknesses of the U-health service. In the proposal, the protocols for user information, certification between medical institution and users, data communication encryption & decryption, and user information disuse were designed by applying the ID-Based Encryption, and analyzed such existing systems and PKI Based-based communication process, securely and safely.

Key Words : U-Healthcare Service, Integrated Authentication Scheme

1. 서론

U-Healthcare 서비스는 사용자가 다양한 의료장비를 활용하여 언제 어디서나 개인의 건강정보를 원격 지원으로 통하여 의료진에게 송수신하여 진찰을 받을 수 있는 서비스로 정의하고 있다. 또한 건강정보를 발송하는 USN, 모니터링 의료장비 및 서버, 유・무선 통신을 담당하는 네트워크, 건강 정보를 분석하는 의료서버 등 다양한 기술로 이루어진 융합된 서비스이다[1].

서비스 과정을 살펴보면 사용자는 Zigbee, UWB방식

본 논문은 2014년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : So-Yeon Min(Seoil Univ.)
Tel: +82-2-490-7583 email: symin@seoil.ac.kr
Received May 27, 2014 Revised June 11, 2014 Accepted June 12, 2014

의 Ubiquitous Sensor Device 및 Smart Phone기반 등의 디바이스를 이용하여 유・무선 인터넷을 통해 건강 정보를 의료기관으로 전송 후 사용자의 건강상태를 실시간으로 모니터링 하여, 이를 분석한 의료진이 적절한 조치를 취하는 방식이다[1,5].

U-Healthcare는 의료정보 및 개인정보를 관리함으로 보안/프라이버시에 대한 위협이 존재한다. 또한 유・무선 네트워크기반의 발생하는 보안취약점을 계승하므로써 안전성, 신뢰성 보장, 데이터 보호를 위한 보완사항이 요구된다[3,8].

그러므로 본 논문에서는 U-health환경에서 유•무선 네트워크 보안취약점, 사용자의 의료정보 및 개인정보를 관리를 위한 통합 인증 스키마구조를 제안한다.

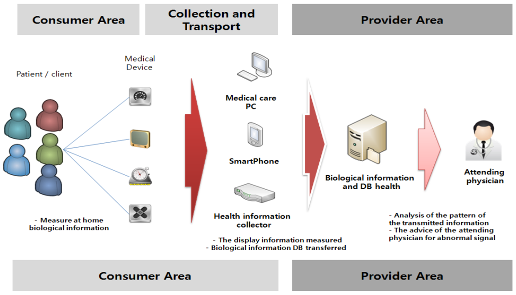
본 논문의 구성은 다음과 같다. 즉, 2장에서는 U-Health환경의 서비스 구조 및 보안위협사항과 신원기반 암호화 방식에 관하여 설명하였고, 3장에서는 제안 프로토콜을 서술하는 부분으로서 등록, 인증, 통신, 폐기 프로토콜에 관한 부분을 설명하였다. 4장은 성능분석에 관한 내용으로 제안시스템과 기존시스템에 관한 보안성 및 안전성을 비교분석하여 기술하였다. 그리고, 5장에서는 결론과 향후 연구 방향에 대하여 제시하였다.

2. 관련연구

2.1 U-Health

2.1.1 기술개발 목표

U-Health 다양한 단말기를 통하여 환자의 건강정보를 검사 후 측정하여 환자 개개인에 관한 생체정보 및 의료정보를 의료기관 또는 건강관리회사에서 운영하는 의료기기 시스템으로 전송한다.



[Fig. 1] U-Healthcare Component technologies

이후 건강 및 생체정보를 분석하여 건강 관리사나 주치의 대상으로 사용자에 대한 건강정보를 체크하여 이에 대한 의료서비스 피드백을 제공한다. U-Healthcare 서비스의 흐름도는 Fig. 1과 같다[2].

2.1.2 기술개발 목표

U-healthcare Service는 유·무선 원격통신으로 사용자와 주치의와의 진료 및 피드백에 대한 정보가 송수신이 가능하므로, 시간 및 공간영역이 제한 없다. 또한 스마트폰의 보급이 4,000만이 넘어가면서 Smart Device장비를 이용한 실시간 생체 측정, 화상 상담, 영상진료 등 다양한 폭이 넓어져서 공간적 활용이 넓어지고 있다. 또한 지능화, 상황인식 및 추론, Ubiquitous computing의 속성으로 사용자의 각종 정보 및 정보패턴을 분석하여 상황에 최적화된 소비자 중심적인 서비스 접근이 가능하다[5].

2.1.3 U-health환경의 서비스 정보 보호 요구사항

U-Health 시스템의 정보 보호 안전성과 신뢰성 확보를 위해 기술적, 정책적 대책이 요구되고 있으며. 정보보호 관련 표준(TTAK.KO-10.0464)에서 제시한 각 요소의 보안요구사항은 다음과 같다.

U-Health User, U-Health Provider, 의료기관, 유관기관 등의 모든 네트워크의 구성요소들 간의 전송되는 정보들은 비인가된 사용자로부터 안전하게 보호되어야 한다[3].

U-Health Service는 기본적으로 유·무선 네트워크기반의 통신을 사용하고 있어 각각의 다양한 U-Health Device로부터 수집된 생체 및 개인정보와 같은 데이터에 관하여 사용자인증, 키 관리, 암호화, 무결성 등의 보안기능 요소가 포함할 것을 권장한다.

U-Health Service Administrator, 유관기관, 의료주치의 등 서비스를 사용하는 구성원은 사용자 식별을 위한 사용자 인증, 권한관리 및 사용내역이 체계적으로 관리되어야 한다[3,5].

U-Health Service는 원격진료를 통하여 습득한 의료정보보호는 미국 내 규정인 HIPAA 혹은 그에 준하는 보안체계를 제공해야한다[3].

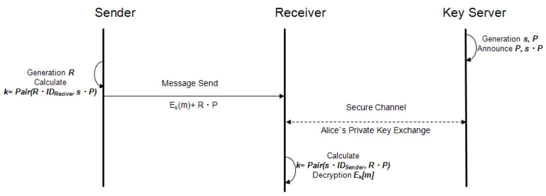
2.2 ID U-Health

1984년 Adi Shamir가 증명한 새로운 공개키 암·복호화 방식으로 사용자의 신원정보를 활용하여 공개키를 암

호화하는 방식이다. 이후 2001년 Dan Boneh, Matthew Franklin이 Weil Pairing기반의 암호 알고리즘을 연구하여 현재 실용적인 방안에서 사용되어지고 있다. 이에 대한 특징은 공개키 인증서가 사용하지 않으며 관리요소의 절감을 통하여, 보다 안전한 암호 시스템의 보급이 가능해진다는 장점이 있다. ID Based Encryption은 Bilinear map이라고 불리는 수학적 구조를 적용하여 Id-based의 암호를 구현하였다[6,7].

$$Pair(a \cdot X, b \cdot Y) = Pair(b \cdot X, a \cdot Y) \qquad (1)$$

일반적으로 위에 연산자 •는 타원 곡선상의 곱을 나타내고 있지만 X와 $a \cdot X$를 알고 있어도 a의 값을 찾는 역산은 불가능하다는 특징이 있다. Pairing기반의 암호화 방식은 Fig. 2와 같다[6].



[Fig. 2] Weil Paring Encryption System

$s \cdot P$는 서버에서 계산한 값이며, $r \cdot ID_{Receiver}$는 송신측에서 계산한 값으로 공개된 값이다.

$$k = Pair(r \cdot ID_{Receiver}, s \cdot P) \qquad (2)$$

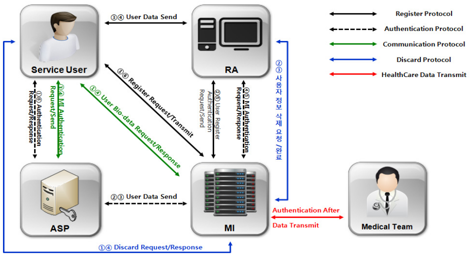
이를 활용하여 메시지 m을 암호화 후 Receiver로 전송 후 $r \cdot P$와 메시지를 송신자의 개인키 값인 $s \cdot ID_{Sender}$을 사용하여 복호화 한다.

$$k = Pair(s \cdot ID_{Sender}, r \cdot P) \qquad (3)$$

3. 제안 프로토콜

3.1 개술개발 내용

기존 U-health환경에서 보안위협과 취약점을 보완하고자 본 논문에서는 안전한 개인정보 관리를 위한 통합 인증 스키마를 설계하였다. 사용자, 인증 서비스 제공자, 등록기관, 의료기관으로 구성되어 있으며, 사용자 등록 후 의료기관에서 인증을 확인한다. 이 후 사용자의 생체정보를 의료기관으로 전송 후 의료진에서 검진이 끝나면 사용자가 의료기관으로 본인의 개인정보를 폐기를 요청 작업이 수행됨에 따라 본 논문에서 제안하는 프로토콜이 완료된다. Fig. 3은 U-Health환경에서 제안한 통합 인증 스키마의 구성이다.



[Fig. 3] Configuration of integrated authentication scheme in U-health environment proposed in this paper

3.2 상세 프로토콜

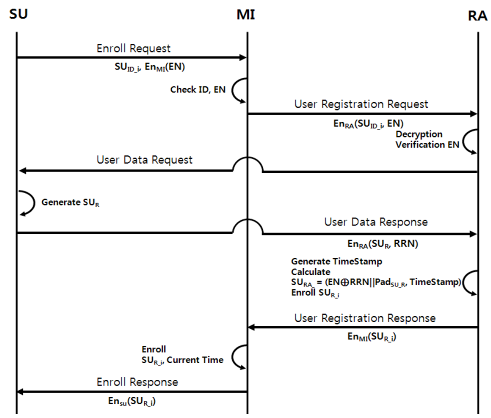
본 논문에서 제안하는 통합 인증스키마의 프로토콜 구조는 ID Based Encryption기반으로 암·복호화를 수행하고 있으며, 등록, 인증, 통신, 폐기 프로토콜에서 사용되어지고 있는 약어는 Table 1과 같다.

[Table 1] Abbreviation

SU	Service User
MI	Medical Institution
MIC	Registration Agency
RA	Authentication Service Provider
ASP	Service User's ID
SU_{ID-i}	Service User's ID
PAD	Padding Value
ASP_X	ASP's Parameter
RA_Y	RA's Parameter
RRN	Resident Registration Number
EN	Examination Number
$Cert_{MI}$	MI's Generate Certification Value
X_R	Entity's Random value
U_{MIN}	Medical Institution Number
SU_{R-i}	Service User's Registration Value

3.2.1 등록 프로토콜

서비스 사용자는 의료기관을 통해 등록 기관에 요청을 하고 사용자의 데이터를 송·수신 후 검증하여 등록완료 메시지를 사용자한테 전송한다. 등록 프로토콜을 Fig. 4에서 도시하였다.



[Fig. 4] Registration Protocol

① SU는 MI로 자신의 공개된 아이디(ex. 휴대전화번호)와 EN을 MI의 ID값으로 암호화하여 등록요청 메시지를 발송한다.

$$SU_{ID-i}, EN_{MI}(EN) \quad (4)$$

② MI는 SU에게 수신된 ID와 검진번호(EN)를 검사 후 RA로 수신 받은 메시지를 복호화 후 RA의 ID 값으로 암호화하여 사용자 등록요청 메시지를 전송한다.

$$EN_{RA}(SU_{ID,} EN) \quad (5)$$

③ RA는 SU로부터 사용자 데이터값을 요청 후 SU는 난수를 생성 후 RRN을 RA의 ID값을 암호화 하여 메시지를 전송한다.

$$EN_{RA}(SU_R, RRN) \quad (6)$$

④ SU로부터 수신받은 메시지를 복호화 하고 SU_{RA-i} 계산 후 생성하여 등록 후 MI으로 전송한다.

$$SU_{RA} = (EN \oplus RRN \| Pad_{SU-R}, Time\,stamp) \quad (7)$$

⑤ RA로 수신 받은 메시지를 등록하여 사용자한테 SU_{R-i}를 전송한다.

3.2.2 인증 프로토콜

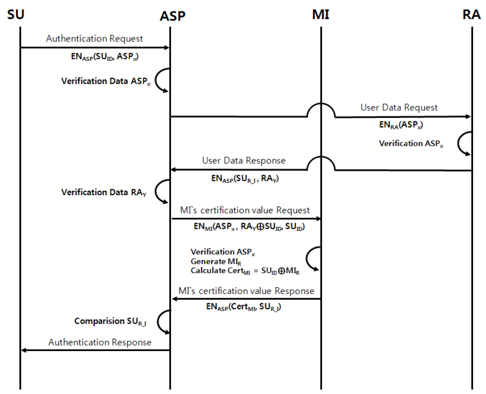
서비스 사용자는 인증 프로토콜 제공자를 통하여 사용자 등록 후 의료기관으로부터 인증값을 요청받아 검증 후 사용자에게 인증 완료 메시지를 전송한다. 인증 프로토콜은 Fig. 5와 같다.

① SU는 ASP로 SU_{ID}와 ASP_X를 ASP의 ID값으로 암호화하여 인증 요청 메시지를 전송한다.

$$EN_{ASP}(SU_{ID}, ASP_X) \quad (8)$$

② ASP는 ASP_X를 검증 후 RA로 ASP값을 RA의 ID 값으로 암호화 하여 사용자 데이터값을 요청한다.

$$EN_{RA}(ASP_X) \quad (9)$$



[Fig. 5] Authentication Protocol

③ RA는 ASP_X를 검증 후 SU_{R-i}, RA_Y을 ASP의 ID 값으로 암호화하여 사용자 데이터값을 전송한다.

$$EN_{ASP}(SU_{R-i}, RA_Y) \quad (10)$$

④ ASP는 RA_Y값을 검증 후 ASP_X $RA_Y \oplus SU_{ID}$, SU_{ID}을 MI의 ID값으로 암호화 하여 인증 값을 요청한다.

$$EN_{MI}(ASP_{X,} RA \oplus SU_{ID}, SU_{ID}) \quad (11)$$

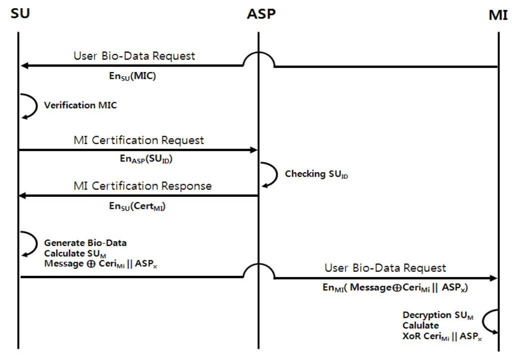
⑤ MI는 수신된 인증 요청 메시지를 복호화 후 ASP_X를 검증 후 $Cert_{MI}$값을 생성 후 ASP로 인증 값을 전송한다.

$$Cert_{MI} = SU_{ID} \oplus MI_R\,,\ EN_{ASP}(Ceri_{MI}, SU_{R-i}) \quad (12)$$

⑥ 인증 값을 수신 받은 ASP는 SU_{R-i}를 기존에 저장되었던 값과 비교 후 값을 확인하여 SU로부터 인증 완료 메시지를 전송한다.

3.2.3 통신 프로토콜

의료기관은 사용자에게 생체 데이터를 요청 후 인증 프로토콜 제공자로부터 인증 메시지를 송수신 후 검증하여 생체 데이터 메시지를 전송한다. 통신 프로토콜은 Fig. 6과 같다.



[Fig. 6] Communication Protocol

① MI는 SU로부터 MIC를 SU의 ID로 암호화하여 사용자 생체데이터를 요정 메시지를 발송한다.

$$EN_{SU}(MIC) \quad (13)$$

② SU는 MIC를 검증 후 ASP로 SU_{ID}값을 ASP의 ID 값으로 암호화 후 인증 요청 메시지를 발송한다.

$$EN_{ASP}(SU_{ID}) \quad (14)$$

③ ASP는 SU_{ID}를 검사 후 SU로 $Cert_{MI}$를 SU의 ID 값으로 암호화 후 인증 응답 메시지를 발송한다.

$$EN_{SU}(Cert_{MI}) \quad (15)$$

④ SU는 생체 데이터를 생성 후 SU_M값을 생성하여 MI로 메시지를 전송한다.

$$EN_{MI}(Message \oplus Ceri_{MI}, ASP_X) \quad (16)$$

⑤ MI는 수신된 메시지를 복호화 후 Xor $Cert_{MI}$ 값을 연산 후 메시지를 확인한다.

3.2.4 폐기 프로토콜

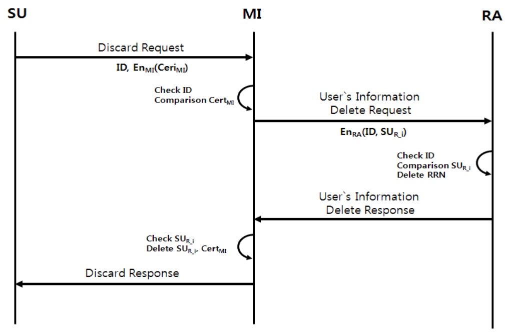
서비스 사용자는 의료기관에 자신의 개인정보 및 등록정보를 폐기요청 한다. 의료기관은 등록기관에 사용자의 개인정보 폐기 요청을 메시지를 송수신 후 사용자에게 완료 메시지 전송한다. 폐기 프로토콜은 Fig. 7과 같다.

① SU는 MI로부터 ID과 $Cert_{MI}$값을 MI의 ID값으로 암호화하여 폐기 요청 메시지를 전송한다.

$$ID, EN_{MI}(Cert_{MI}) \quad (17)$$

② 수신받은 메시지를 복호화 후 기존의 $Cert_{MI}$값과 비교 후 RA로 ID와 SU_{R-i}을 RA의 ID값으로 암호화하여 사용자 정보 삭제 요청 메시지를 전송한다.

$$EN_{RA}(ID, SU_{R-i}) \quad (18)$$



[Fig. 7] DisCard Protocol

③ ID를 검사 및 SU_{R-i}를 비교 후 RRN값을 삭제하여 MI로 사용자 요청 삭제 메시지를 발송한다.

④ MI는 SU_{R-i}를 검사 후 $SU_{R-i}, Cert_{MI}$를 삭제하여 SU로 폐기 응답 메시지를 발송한다.

4. 성능분석

4.1. 시스템 구조 따른 보안성 분석

본 절에서는 기존 통신 시스템과 제안하는 통합 인증 시스템의 구조에 따른 보안성에 관하여 분석하였다. 비교분석한 내용은 Table 2와 Table 3과 같다.

제안시스템에서는 사용자 측면의 개인정보 관리 프로토콜을 설계하여 치료가 끝난 후 폐기 프로토콜을 통하여 사용자의 개인정보를 보호할 수 있으며, 기존의 U-health에서 사용한 PKI암호기반의 암·복호화 방식이 아닌 ID-based Encryption을 활용하여 통신의 효율성을 높을 수 있었다. 또한 권한 관리 메커니즘을 설계하여 의료기간에서 Certificate Value를 통하여 상호간의 안전한 통신을 제공 및 사용자에 대한 식별성을 제공하였다.

[Table 2] Analysis of the safety of the proposed system with the existing system

	Proposed System	Exist System
Personal information management of the user side	Support	No Support
Data Encryption	ID-Base Encryption	PKI
Rights management mechanism	Support	No Support
Identification of user provided	Support	Support
Mutual authentication	Certificate Value	PKI, RRN

4.2 안전성 분석

기존 U-health환경에서 주로 발생하는 보안위협 항목인 무결성, 기밀성, 부인방지, 도청/위변조, 인가되지 않은 접근, 중간자 공격에 대한 안전성을 분석하였다.

[Table 3] Stability analysis of the proposed system with the existing system

	Proposed System	PKI Based System	Exist System
Confidentiality	O	O	O
Integrity	O	O	O
Authentication	O	O	O
Non-repudiation	O	O	
Unauthorized access	O	O	
Personal Information Management	O		
In middle Attack	O		

① 기밀성 및 무결성

신원기반 방식의 암호화 방식을 활용하여 각각의 서로 공유하고 있는 파라미터를 활용하여 메시지를 송·수신하였으며, 통신 프로토콜상의 $Cert_{MI} \| ASP_X$을 송신하였으므로, 메시지에 대한 기밀성 및 무결성을 보장하도록 하였다.

② 인증 및 부인 방지

사용자 등록 및 인증 과정에서 EN값을 암호화하여 송수신후 검증받은 값과 RRN을 값을 기반으로 SU_{RA}를 생성하였고, 또한 $Cert_{MI}$값을 생성하여 이를 검증하여 상호간에 인증 프로토콜을 설계하여 부인 방지를 가능하도록 하였다.

③ 인가되지 않은 접근 및 개인정보 관리

본 논문에서는 제안하는 통합 인증 스키마에서는 $Cert_{MI}$와 SU_{R-i}의 값을 생성하여 상호간의 안전한 통신을 설계하였다. 이후 사용자의 개인정보를 폐기를 요청하는 프로토콜을 설계하여 사용자의 개인정보를 검증 후 삭제하도록 하였다.

④ 중간자 공격

각각의 Domain간에 신원기반 암호방식을 사용하여 ASP_X, RA_Y값을 송·수신 및 검증하는 방식을 사용하여, 중간자 공격에 대한 보안위협을 방지하였다. 또한 메시지를 복호화 후 $Cert_{MI} \| ASP_X$을 Xor연산을 통하여 메시지를 확인하므로 재전송공격을 완화할 수 있다.

5. 결론

본 논문에서는 기존 U-health 시스템에서 존재하는 보안위협을 보완하고자 통합 인증 스키마를 설계 및 제안하였다. U-Health Service에서 등록, 인증, 통신, 폐기 프로토콜을 설계하여 사용자의 생체, 개인정보를 안전하게 통신 후 사용자 개인정보를 안전하게 관리할 수 하였다.

제안 프로토콜은 사용자 측면의 개인정보 관리, 데이터 암호화, 권한관리 메커니즘, 사용자에 대한 식별성 제공, 상호간 인증에 관한 보안성을 보완하였다. 또한 PKI 기반 암호시스템과 기존시스템과의 비교분석을 하여 인가되지 않은 기본적인 안정성과 사용자의 접근, 개인정보 관리, 중간자 공격에 대한 안정성을 높였다.

향후 제안한 인증 스키마는 최근 각광받고 꾸준히 진행하고 있는 Smart-care Service에서 적용하기 위해 활용 폭넓은 연구가 필요하다. 본 논문에서 제안한 인증스키마가 아닌 소형 Device에서도 활용할 수 있는 인증 프로토콜 및 보안 프레임워크에 대한 안정성 및 보안요구사항 설계가 요구된다. 또한 빠르게 발전되어지고 있는 U-Healthcare 및 SmartCare에서 알려지지 않은 보안위협사항과 이에 따른 공격 유형에 대한 연구가 필요하다.

References

[1] Chan-Yong Park, "Technical Trend of U-Healthcare Standardization", No. 25, Vol 4, pp.48~59 2011.8
[2] A Development of Standard and Bio-Authentication Technology for Telemedicine, KISA, 2007.12
[3] TTA, Information Security Reference Model for u-Health Service, TTA, 2010.12.
[4] TTA, Health Data Gateway, Server Protocol, 2011.6
[5] TTA, u-Health Service Reference Model, TTA, 2010.12
[6] Adi Shamir. "Identity-Based Cryptosystems and signature System". SpringerLink. 1985
[7] Dan Boneh, Matthew Franklin. "Identity-Based Encryption from the Weil Pairing". Crypto. 2001
[8] M. Martínez-Espronceda et al., "Standard- Based Homecare Challenge: Advances of ISO/IEEE11073 for

u-Health," Series in Biomedical Engineering, Handbook of Digital Homecare, Oct. 2009, pp.179~202.
DOI: http://dx.doi.org/10.1007/978-3-642-01387-4_9

민 소 연(So-Yeon Min) **[종신회원]**

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 일반대학원 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 일반대학원 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신과 부교수

<관심분야>
통신 및 신호처리, 임베디드 시스템

진 병 욱(Byung-Wook Jin) **[정회원]**

- 2010년 2월 : 청운대학교 멀티미디어학과 (문학사)
- 2013년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2013년 3월 ~ 현재 : 숭실대학교 컴퓨터학과

<관심분야>
사물지능통신, USN, 네트워크 통신