Journal of Digital Convergence
Vol. 18. No. 9, pp. 57-62, 2020

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2020.18.9.057

Shuai등의 스마트 홈 환경을 위한 익명성 인증 기법에 대한 프라이버시 취약점 분석

최해원[1], 김상진[2], 정영석[2], 류명춘[2*]
[1]DGIST 기술벤처경영 교수, [2]경운대학교 항공컴퓨터학과 교수

Privacy Vulnerability Analysis on Shuai et al.'s Anonymous Authentication Scheme for Smart Home Environment

Hae-Won Choi[1], Sangjin Kim[2], Young-Seok Jung[2], Myungchun Ryoo[2*]
[1]Department of Innovation Management, DGIST
[2]Department of Aeronautical Computer Engineering, Kyungwoon University

요 약 사물인터넷에 기반한 스마트 홈은 아주 흥미로운 연구와 산업 분야의 하나로 급격한 관심을 받아오고 있다. 하지만 무선 통신 채널의 열린 특성 때문에 보안과 프라이버시는 중요한 이슈가 되었다. 이러한 연구를 위한 노력의 일환으로 Shuai등은 타원곡선암호시스템을 사용하는 스마트 홈 환경을 위한 익명성 인증 기법을 제안하였다. Shuai등은 정형화된 검증과 휴리스틱 보안 분석을 제시하고 그들의 기법이 비동기화 공격과 모바일 장치 분석 공격을 포함한 다양한 공격에 안전하고 사용자 익명성과 비추적성을 제시한다고 주장하였다. 하지만, 본 논문에서는 Shuai등의 기법이 사물인터넷 네트워크 환경에서 제시된 사용자 익명성과 비추적성에 초점을 맞춘 취약점을 도출하였다.

주제어 : 스마트 홈, 타원곡선암호시스템, 인증, 프라이버시, 익명성

Abstract Smart home based on Internet of things (IoT) is rapidly emerging as an exciting research and industry field. However, security and privacy have been critical issues due to the open feature of wireless communication channel. As a step towards this direction, Shuai et al. proposed an anonymous authentication scheme for smart home environment using Elliptic curve cryptosystem. They provided formal proof and heuristic analysis and argued that their scheme is secure against various attacks including de-synchronization attack, mobile device loss attack and so on, and provides user anonymity and untraceability. However, this paper shows that Shuai et al.'s scheme does not provide user anonymity nor untraceability, which are very important features for the contemporary IoT network environment.

Key Words : Smart Home, Elliptic Curve Cryptosystem, Authentication, Privacy, Anonymity

1. 서론

오늘날 사물인터넷을 기반으로 상호 연결된 세계에서, 보안 및 개인 정보보호에 대한 다양한 위협이 존재한다[1-3]. 특히, 사물인터넷 기반 스마트 홈을 위한 다양한 보안 및 프라이버시를 위한 연구들이 진행되었다[4-11]. 2011년 Vaidya등은 일회성 패스워드를 사용하는 원격 사용자 인증 기법을 제안하였다[4]. 하지만 논문 [5]에서

*Corresponding Author : Myungchun Ryoo(chw@ikw.ac.kr)
Received July 29, 2020
Revised August 18, 2020
Accepted September 20, 2020
Published September 28, 2020

는 Vaidya등의 기법이 패스워드 추측 공격에 취약하고 사용자 익명성과 전방향 보안을 제공하지 못함을 보였다. 그 후 Vaidya등은 타원곡선암호시스템(Elliptic curve cryptosystem) 기반 스마트 에너지 홈 네트워크를 위한 장치 인증 기법을 제안하였다[6]. 이와는 다른 연구로 Santoso와 Vun은 타원곡선암호시스템을 사용한 스마트 홈을 위한 인증 기법을 제안하였다[8]. 이들 기법에서 게이트웨이(Gateway, GWN)가 사용자와 스마트 장치간 상호인증을 수행하는 주요 노드로 사용되었다. 하지만, 이들 기법은 사용자 익명성과 비추적성을 제시하지 못한다. 이러한 문제를 해결하기 위해서 Shuai등은 스마트 홈 환경을 위한 익명성 인증 기법을 제안하였다[11]. 특히, 보안 분석을 위해 정형화된 보안 검증 및 휴리스틱한 분석을 제시하였다. 이러한 보안 분석 결과 익명성과 비추적성을 제시하고 다양한 공격에 안전하다고 주장하였다.

본 논문에서는 Shuai등의 익명성 인증 기법이 프라이버시를 제공하지 못함을 보인다. 특히, 익명성과 비추적성에 초점을 맞춘 Shuai등의 기법에 대한 프라이버시 취약점 분석을 제시한다.

2. 스마트 홈 환경

Fig. 1은 전형적인 스마트 홈 환경을 보여준다. 스마트 홈 네트워크 모델은 집안 내의 스마트 장치들(Smart devices), 게이트웨이노드와 종단 사용자(User) 그리고 등록기관(Registration authority, RA)로 구성된다.

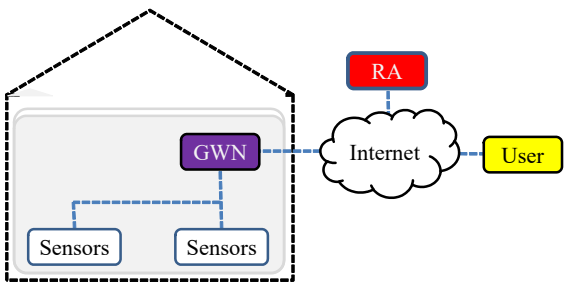

Fig. 1. Typical smart home environment

스마트 장치들은 다양한 이기종 장비들로 구성되고 일반적으로 자원 제약적인 속성을 가진다. 이들 장치들은 센서기능을 기반으로 하는 조명제어, 감시, 온도 제어 등 다양한 사용 목적을 제시한다. 가정 내에 설치되는 GWN은 사용자와 스마트 장치간의 네트워크 브릿지(Bridge) 역할을 수행한다. 사용자는 이기종 스마트 홈 장치들을 원격으로 조정할 수 있다. RA는 높은 계산능력과 통신능력을 가지고 다른 네트워크 참가자들에게 높은 신뢰도를 가진다. RA는 시스템 파라미터를 생성하고 네트워크 참여자들에게 이들 정보를 분배하는 역할을 담당한다. 그리고 사용자와 스마트 장치들의 등록을 담당하고 키 관리와 유지보수를 지원한다.

3. Shuai등의 익명성 인증 기법

Shuai등은 효율적이면서 익명성을 제공하는 타원곡선암호시스템 기반의 스마트 홈 환경을 위한 인증 기법을 제안하였다[11]. Shuai등은 Table 1에서 제시한 기호를 이용하여 익명성 인증 기법을 제안하고 정형화된 보안 분석을 포함한 다양한 보안 분석을 제시하였고, 본인들의 기법이 보안과 효율성 간 밸런스를 달성한다고 주장하였다[12-15].

Table 1. Notations and abbreviations

Notation	Descriptions
ECC	Elliptic curve cryptography
U_i	Remote user
GWN	Gateway node
SD_k	Smart device in the home
ID_i	Unique identity of U_i
PW_i	Password of U_i
DID_i	Pseudonym identity of U_i
GID_j	Unique identity of GWN
SID_k	Unique identity of SD_k
RA	Registration authority
K	Master secret key of GWN
SK	Session key
R_1, R_2, R_3, a	Random numbers
$h(\cdot)$	One-way hash function
$X \| Y$	Concatenate operation
$\oplus$	XOR operation

3.1 초기화 단계

초기화 단계는 RA에 의해 안전하게 수행된다. 먼저 RA는 유한필드 F_p에 기반한 타원곡선 E를 선택하고 오더(Order) q를 가진 E의 덧셈군 G와 G의 생성자인 P를 선택한다. 그리고 RA는 시스템 개인키 $x \in Z_q^*$를 생성하고 시스템 공개키 $X=xP$를 계산한다. RA는 장기간 사용할 비밀키 K와 해쉬함수 $h(\cdot):\{0,1\}^* \rightarrow Z_q^*$를 선택한다. 또한, RA는 x와 K를 GWN의 메모리에 안전하고 저장하고 파라미터 $\{E(F_p), G, P, X, h(\cdot)\}$를 발표한다. RA는 스마트장치 SD_k의 유일한 식별자로 랜덤 값 SID_k를 선택하고 이것을 SD_k의 메모리에 저장한다. 이 단계에서 설정된 파라미터 $\{E(F_p), G, P, X, h(\cdot)\}$는 모든 사용자에게

알려져야 하고 GWN과 모든 스마트 장치에 미리 업로드 되어야 한다.

3.2 등록 단계

Shuai등의 기법은 사용자 등록 단계와 스마트 장치 등록 단계가 필요하다.

[사용자 등록 단계] 스마트 장치로부터 수집된 민감한 데이터를 접근하기 위해서 각 사용자는 RA에게 등록해야 한다. 사용자 등록 단계는 다음과 같다.

(1) 새로운 사용자 U_i는 식별자 ID_i와 패스워드PW_i를 선택하고 난수 a를 생성한다. U_i는 $HWP_i=h(PW_i||a)$ 계산하고 안전한 채널을 사용하여 $\{ID_i, HWP_i\}$를 RA에게 보낸다.

(2) 등록 메시지를 받은 후 RA는 사용자 정보 테이블에서 ID_i가 존재하는지 체크한다. 만약 존재한다면 RA는 U_i에게 새로운 ID_i를 보내도록 요청한다. 그렇지 않다면 RA는 $K_{GU}=h(ID_i||K)$와 $A_1=K_{GU}\oplus HPW_i$를 계산한다. RA는 사용자 로긴 실패 횟수를 기록하기 위한 랜덤 값 $TEMP$를 생성하고 0으로 초기화 한다. 그리고 RA는 $\{A_1\ TEMP\}$를 안전한 채널을 이용해 U_i에게 전송한다.

(3) RA로부터 데이터를 받은 후 U_i는 $A_2=a\oplus h(ID_i||PW_i)$와 $A_3=h(ID_i||HPW_i)$를 계산하고 A_2와 A_3을 모바일 장치에 쓴다. 모바일 장치는 $\{A_1, A_2, A_3, TEMP\}$를 저장한다.

[스마트 장치 등록 단계] 스마트 장치의 등록 은 다음 단계를 따른다.

(1) 스마트 장치 SD_k는 식별자 SID_k를 선택하고 안전한 채널을 사용하여 RA에게 보낸다.

(2) SID_k를 받은 후 RA는 스마트 장치 정보 테이블에서 SID_k가 존재하는지 체크한다. 만약 존재한다면 RA는 스마트 장치 등록 요청을 거절한다. 그렇지 않다면 RA는 $K_{GS}=h(SID_k||K)$를 계산하고 SD_k에게 안전하게 전송한다.

(3) RA로부터 데이터를 받은 후 SD_k는 K_{GS}를 자신의 메모리에 안전하게 저장한다.

3.3 로긴과 인증 단계

사용자 U_i가 식별자 SID_k의 스마트 장치 SD_k의 실시간 데이터를 접근하기 원할 때, U_i, SD_k와 GWN간의 상호인증이 수행되어야 하고 뒤 따르는 안전한 통신을 위해서 사용자 U_i와 스마트 장치 SD_k간의 세션키 SK가 설립되어야 한다. 로긴과 인증은 다음 절차를 따른다.

(1) U_i는 ID_i와 PW_i를 모바일 장치에 입력한다. 모바일 장치는 $a^*=A_2\oplus h(ID_i||PW_i)$, $HPW_i^*= h(PW_i||a^*)$와 $A_3^*=h(ID_i||HPW_i^*)$를 계산하고 A_3^*가 A_3와 같은지 체크한다. 두 값이 같지 않으면 모바일 장치는 로긴 요청을 거절하고 $TEMP$를 1 증가시킨다. 만약 $TEMP$의 값이 사전에 정의된 임계치를 초과(예를 들어 3)하면 그 모바일 장치가 공격당하고 있다고 간주하고 U_i의 재등록을 요구한다. 그렇지 않으면 모바일 장치는 난수 R_1과 w를 생성하고 U_i는 접근하기를 원하는 SID_k의 스마트 장치 SD_k를 선택한다. 모바일 장치는 $K_{GU}=A_1\oplus HPW_i$, $A_4=w\cdot P$, $A_5=w\cdot X$, $DID_i=ID_i\oplus A_5$, $M_1=(SID_k||R_1)\oplus K_{GU}$와 $V_1=h(ID_i||R_1||K_{GU}||M_1)$를 계산한 후 로긴 메시지 $\{DID_i, A_4, M_1, V_1\}$를 공개 채널을 이용하여 GWN에게 전송한다.

(2) 로긴 요청을 받은 후 GWN은 저장된 비밀 값 x를 사용하여 $A_5^*=x\cdot A_4$를 계산한다. GWN은$ID_i^*=DID_i\oplus A_5^*$, $K_{GU}=h(ID_i^*||K)$, $SID_k||R_1^*=M_1\oplus K_{GU}$와 $V_1^*=h(ID_i^*||R_1^*||K_{GU}||M_1)$를 계산하고 V_1^*와 V_1가 같은지 체크한다. 만약 같지 않다면 GWN은 세션을 종료한다. 그렇지 않으면 GWN은 U_i의 적합성을 믿고 난수 R_2를 생성하고 $K_{GS}=h(SID_k||K)$, $M_2=(ID_i||GID_j||R_1||R_2)\oplus K_{GS}$와 $V_2=h(ID_i||GID_j||K_{GS}||R_1||R_2)$를 계산한다. GWN은 공개 채널을 통해 스마트 장치 SD_k에게 $\{M_2, V_2\}$를 전송한다.

(3) 메시지를 받은 후 SD_k는 $(ID_i||GID_j||R_1||R_2)=M_2\oplus K_{GS}$와 $V_2^*=h(ID_i||GID_j|| K_{GS}||R_1||R_2)$를 계산하고 V_2^*와 V_2가 같은지 체크한다. 만약 두 값이 다르다면 SD_k는 세션을 종료한다. 그렇지 않다면 SD_k는 난수 R_3를 생성하고 $SK=h(ID_i||GID_j||SID_k||R_1||R_2||R_3)$, $M_3=R_3\oplus K_{GS}$와 $V_3=h(R_3||K_{GS}||SK)$를 계산한다. 그리고 SD_k는 공개 채널을 통해 GWN에게 $\{M_3, V_3\}$를 전송한다.

(4) SD_k로부터 메시지를 받은 후 GWN은 $R_3=M_3\oplus K_{GS}$, $SK=h(ID_i||GID_j||SID_k||R_1||R_2||R_3)$와 $V_3^*=h(R_3||K_{GS}||SK)$를 계산하고 V_3^*와 V_3가 같은지 체크한다. 만약 두 값이 다르다면 GWN은 세션을 종료한다. 그렇지 않다면 GWN은 $M_4=(GID_j||R_2||R_3)\oplus K_{GU}$와 $V_4=h(K_{GU}||SK||R_2||R_3)$를 계산하고 $\{M_4, V_4\}$를 U_i에게 전송한다.

(5) GWN으로부터 메시지를 받은 후 U_i는 $(GID_j||R_2||R_3)=M_4\oplus K_{GU}$, $SK=h(ID_i||GID_j||SID_k||R_1||R_2||R_3)$와 $V_4^*=h(K_{GU}||SK||R_2||R_3)$를 계산하고 V_4^*와 V_4가 같은지 체크한다. 만약 두 값이 다르다면 U_i

는 세션을 종료한다. 그렇지 않다면 SD_k는 U_i에 의해 인증되었고, 세션키 SK가 U_i와 SD_k간에 설립되었다.

3.4 패스워드 변경 단계

사용자 U_i는 GWN과 상호작용하지 않고 패스워드를 다음과 같이 변경할 수 있다.

(1) U_i는 ID_i와 PW_i를 모바일 장치에 입력한다.

(2) 모바일 장치는 $a^*=A_2 \oplus h(ID_i||PW_i)$, $HPW_i^*=h(PW_i||a^*)$와 $A_3^*=h(ID_i||HPW_i^*)$를 계산하고 A_3^*가 A_3와 같은지 체크한다. 두 값이 같지 않으면 모바일 장치는 패스워드 변경 요청을 거절한다. 그렇지 않다면 모바일 장치는 U_i의 적법성을 믿고 U_i가 새로운 패스워드 PW_i^{new}를 입력하게 한다.

(3) 모바일 장치는 $HPW_i^{new}=h(PW_i^{new}||a^*)$, $A_1^{new}=K_{GI} \oplus HPW_i^{new}=A_1 \oplus HPW_i \oplus HPW_i^{new}$, $A_2^{new}=a^* \oplus h(ID_i||PW_i^{new})$와 $A_3^{new}=h(ID_i||HPW_i^{new})$를 계산한다. 마지막으로 모바일 장치에 저장된 A_1, A_2와 A_3가 각각 A_1^{new}, A_2^{new}와 A_3^{new}으로 대체된다.

4. 프라이버시 취약성 분석

Shuai등은 자신들의 기법이 다양한 보안 특성을 제공할 수 있고 사용자 익명성과 비추적성을 포함한 다양한 공격에 강함을 증명하였다. 하지만, 본 절에서는 Shuai 등의 익명성 인증 기법이 사용자 익명성과 비추적성을 제시하지 못함을 보인다.

4.1 사용자 익명성

Shuai등은 자신들이 제안한 기법에서 사용자의 실제 식별자 ID_i가 어떤 메시지에도 포함되지 않기 때문에 공격자가 사용자의 식별자 ID_i를 획득할 수 없다고 주장하고 있다. 특히, 식별자 ID_i 관련 정보가 메시지 DID_i, M_1, V_1, M_2 와 V_2들 내에 포함되어 있어서 GWN의 비밀키인 x와 K를 알지 못하는 공격자는 사용자의 실제 식별자 ID_i를 통신 메시지로부터 찾을 수 없다고 주장하였다.

Shuai등의 기법에 대한 사용자 익명성 공격을 위해서는 기법에서 사용하는 기호들의 비트 수에 대한 명확한 고려가 제시되어야 한다. 본 논문에서 제시한 각 기호들의 비트 수는 Shuai등의 5.2절 통신 오버헤드에서 제시한 바와 동일한 Table 2의 길이를 가정한다.

Table 2. Length of primitives

Primitive	Length	Primitive	Length
User identity	128 bits	User Pseudonym	128 bits
User password	128 bits	Sensor identity	128 bits
Timestamp	32 bits	Secret key	160 bits
Random number	160 bits	ECC point multiplication	320 bits
Ciphertext block	256 bits	Hash function	160 bits
MAC	160 bits		

Shuai등의 기법에서는 사용자 익명성을 제공하기 위해서 로긴과 인증 단계의 (1)번에서 $DID_i=ID_i \oplus A_5$와 (2)번에서 $M_2=(ID_i||GID_j||R_1||R_2) \oplus K_{GS}$를 이용하였다. 특히, M_2에서 '⊕' 연산을 기본 연산으로 제시하고 있고 왼쪽 피연산자는 문자 결합연산자인 '||'을 이용하고 있다. 즉 M_2 계산을 위해서는 Fig. 2와 같은 연산을 수행한다. Fig. 2의 연산에서 각각의 기호들의 비트 수를 적용하면 Fig. 3과 같다. Fig. 3을 통해서 M_2 계산 결과가 전체 576 비트이고 이중 최하위 160 비트 만이 '⊕' 연산의 영향을 받아서 $M_2=(ID_i||GID_j||R_1||R_2 \oplus K_{GS})$로 계산됨을 확인할 수 있다. 즉 Shuai등의 기법은 M_2 연산을 통해서 사용자 ID_i를 마스킹 할 수 없음을 명확히 확인할 수 있다. 이를 통해 임의의 공격자는 M_2의 최상위 128 비트를 확인함으로서 어떤 사용자가 통신의 주체인가를 명확히 확인할 수 있다.

$$\begin{array}{rc} & (ID_i||GID_j||R_1||R_2) \\ \oplus & K_{GS} \\ \hline & M_2 \end{array}$$

Fig. 2. Configuration of ⊕ operation for M_2

$$\begin{array}{rc} & (128||128||160||160) \\ \oplus & 160 \\ \hline & (128||128||160||160) \end{array}$$

Fig. 3. Configuration of ⊕ operation with bits for M_2

4.2 비추적성

Shuai등은 자신들이 제안한 기법에서 사용자가 각 세션에서 난수 w와 R_1을 생성하고 현재 세션의 메시지가 다른 세션의 메시지와 다르다고 주장하였다. 그래서 Shuai등의 기법이 비추적성을 제시할 수 있다고 분석에서 제시하였다. Shuai등이 논의 한 것처럼 비추적성은 공격자가 통신 세션의 사용자를 알 수 없고 같은 사용자

에 의해 수행된 연속 세션을 구별할 수 없을 때 제공될 수 있다.

하지만 Shuai등의 기법은 사용자 익명성 분석에서 보여준 것처럼 M_2 연산을 통해서 사용자 ID_i를 효과적으로 마스킹 할 수 없고 이로 인해서 세션간 추적성을 제공할 수 있는 프라이버시에 치명적인 문제가 존재한다.

5. 결론

본 논문에서는 Shuai등의 익명성 인증 기법에 대한 프라이버시 취약점 분석을 제시하였다. 이를 위하여 스마트 홈 환경에 대한 구성과 Shuai등의 인증 기법에 대한 리뷰를 제시하였다. 특히, Shuai등의 기법이 논문에서 주장한 익명성과 비추적성을 제시하지 못함을 보였다.

현재에도 다양한 보안 기법에 대한 다양한 공격이 진행 중에 있고, 이에 대한 해결책 제시 또한 아주 중요한 연구 분야이다. 특히 정형화된 보안 증명이 제시된 기법이라고 하더라도 다양한 연구에서 보안 및 프라이버시 문제점이 도출되고 있다. 그러므로 새로운 보안 기법에 대한 설계는 다양한 보안 분석이 명확히 제시되어야 할 것이다. 저자들은 현재 Shuai등의 기법에 존재하는 프라이버시 문제점들을 해결하기 위한 동적식별자를 사용하는 기법에 대한 연구를 진행하고 있다.

REFERENCES

[1] H. Kim. (2017). Data Centric Security and Privacy Research Issues for Intelligent Internet of Things. *ICSES Interdisciplinary Transactions on Cloud Computing, IoT, and Big Data, 1(1),* 1-2.

[2] Y. Kim. (2019). A Study on Smart Contract for Personal Information Protection. *Journal of Digital Convergence, 17(3),* 215-220.

[3] H. Kim. (2019). Research Issues on Data Centric Security and Privacy Model for Intelligent Internet of Things based Healthcare. *ICSES Transactions on Computer Networks and Communications, 5(2),* 1-3.

[4] B. Vaidya, J. H. Park, S. S. Yeo & J. Rodrigues. (2011). Robust one-time password authentication scheme using smart card for home network environment. *Computer Communications, 34,* 326-336.

[5] H. J. Kim & H. S. Kim. (2011). Auth hotp-hotp based authentication scheme over home network environment. *Lecture Notes in Computer Science, 6784*, 622-637.

[6] B. Vaidya, D. Makrakis & H. T. Mouftah. (2011). Device authentication mechanism for smart energy home area networks. *Proc. of IEEE International Conference on Consumer Electronics,* 787-788.

[7] I. H. Cho & K. H. Lee. (2019). A Scheme of User Face Recognition using a Moire Phenomenon in IoT Environment. *Journal of Digital Convergence, 17(2),* 171-176.

[8] F. K. Santoso & N. C. H. Vun. (2015). Securing IoT for smart home system, *Proc. of IEEE International Symposium on Consumer Electronics,* 1-2.

[9] H. W. Choi, S. Kim & M. Ryoo. (2019). Cryptanalysis and Solution on Secure Communication Scheme for Healthcare System using Wearable Devices, *Journal of Digital Convergence, 17(2),* 187-194.

[10] W. J. Lee, K. W. Kim & H. Kim. (2012). Ticket-Based Authentication Protocol Using Attribute Information over Home Network. *IEMEK Journal of Embedded Systems Applications, 7(1)*, 53-59.

[11] M. Shuai, N. Yu, H. Wang & L. Xiong. (2019). Anonymous authentication scheme for smart home environment with provable security. *Computers & Security, 86*, 132-146.

[12] H. Kim, E. K. Ryu & S. W. Lee, (2011), Security Considerations on Cognitive Radio based on Body Area Networks for u-Healthcare, *Journal of Security Engineering, Vol. 10, No. 1*, pp. 9-20.

[13] S. Y. Mun, Y. M. Yun, T. H. Han, S. E. Lee, H. J. Chang, S. Y. Song&H. C. Kim, (2017),Public Awareness of Digital Healthcare Services, *Journal of Digital Convergence, Vol. 18, No. 4*, pp. 621-629.

[14] J. E. Song, S. H. Kim, M. A. Chung & K. I, Chung, (2007), Security issues and its technology trends in u-Healthcare, *Electronics and Telecommunications Trends, Vol. 22, No. 1*, pp. 119-129.

[15] T. M. Song & S. H. Jang, (2011), u-Healthcare : Issue and Research Trends, *Korea Institute for Health and Social Affairs*, pp. 119-129.

최 해 원(Hae-Won Choi) [정회원]

- 2000년 2월 : 경북대학교 컴퓨터공학과(공학석사)
- 2009년 2월 : 경북대학교 컴퓨터공학과(공학박사)
- 2016년 2월 : 대구경북과학기술원 (DGIST) MOI
- 2006-2017년 : 경운대학교 항공컴퓨터학과 교수
- 2018년 3월 ~ 현재 : DGIST 기술벤처경영 겸직교수
- 2016년 10월 ~ 현재 : ㈜티에이싱크 대표
- 관심분야 : 알고리즘, 유비쿼터스 컴퓨팅, 보안
- E-Mail : chw@ikw.ac.kr

김 상 진(Sang-Jin Kim) [정회원]

· 1994년 2월 : 계명대학교 컴퓨터공학과 (공학사)
· 1996년 2월 : 경북대학교 컴퓨터공학과 (공학석사)
· 2000년 8월 : 경북대학교 컴퓨터공학과 (공학박사)
· 1999년 9월 ~ 현재 : 경운대학교 항공컴퓨터학과 교수
· 관심분야 : 알고리즘, 게임이론, 보안
· E-Mail : sjkim@ikw.ac.kr

정 영 석(Young-Seok Jung) [정회원]

· 1995년 2월 : 영남대학교 컴퓨터공학과(공학사)
· 1998년 2월 : 영남대학교 컴퓨터공학과(공학석사)
· 2003년 2월 : 영남대학교 컴퓨터공학과(공학박사)
· 2000년 3월 ~ 현재 : 경운대학교 항공컴퓨터학과 교수
· 관심분야 : 지능형 네트워크, 모바일 컴퓨팅, 빅 데이터
· E-Mail : ysjung@ikw.ac.kr

류 명 춘(Myung-Chun Ryoo) [정회원]

· 1989년 2월 : 영남대학교 컴퓨터학과 (공학사)
· 1991년 2월 : 영남대학교 컴퓨터공학과(공학석사)
· 2009년 2월 : 영남대학교 컴퓨터공학과(공학박사)
· 1997년 3월 ~ 현재 : 경운대학교 항공컴퓨터학과 교수
· 관심분야 : 지능정보시스템, Bioinformatics, 보안
· E-Mail : mcryoo@ikw.ac.kr