Journal of KIIT. Vol. 19, No. 12, pp. 85-96, Dec. 31, 2021. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2021.19.12.85

멀티서버 환경에서 대칭키 기반 이중채널 인증스킴 설계

신 광 철*

Design of Symmetric Key-based Dual-Channel Authentication Scheme in Multi-Server Environment

Kwang-Cheul Shin*

요 약

개인에게는 의료정보가 민감한 정보이기 때문에 환자의 민감한 정보가 유출되는 것을 차단하여 합법적인 사용자만 TMIS에 접근하도록 할 수 있도록 하는 것이 매우 중요하다. 그동안 많은 연구자들이 보안강화와 사용자 익명성을 위해 퍼지 추출기와 ECC를 사용하는 생체기반의 3-factor 인증방식을 제시했다. 그러나 계산과 통신 및 저장 요구사항에 대한 비용이 매우 높고 그들의 주장만큼 효과적이지 못하여 Barman et al′.s이 헬스케어에 대한 인증스킴을 제안하였다. 그러나 Ali et al′.s는 이 기법이 알려진 많은 공격에 취약하다고 분석하였으며, 인증 및 키 동의 (KSA) 방식의 또 다른 기법을 제안하였다. 본 논문에서는 Ali et al′.s의 스킴이 중간자 공격(MITM)에 의한 세션 키 노출, 스마트카드 도난에 의한 사용자 위장공격, 상호인증에 취약하다고 분석하고 이러한 보안 위협을 해결하기 위해 멀티서버환경에서 QR-code를 이용한 2중 채널과 2-factor를 사용하는 대칭키 기반의 인증스킴을 제안한다.

Abstract

Since medical information is sensitive information to each individual, it is necessary to prevent leakage of patient's sensitive information. It is very important to ensure that only legitimate users have access to TMIS. For a long time, many researchers have proposed a biometric-based 3-factor authentication method using fuzzy extractors and ECC for security enhancement and user anonymity. However, the cost of computation and communication and storage requirements is very high and not as effective as their claims, so Barman et al's proposed an authentication scheme for healthcare. However, Ali et al's analyzed that it is vulnerable to many known attacks and proposed another method of authentication and key agreement (KSA). In this paper, we analyzed that Ali et al's scheme is vulnerable to session key exposure by man-in-the-middle attack (MITM), user impersonation attack by smart card loss, and mutual authentication. In addition, to solve these security threats, we propose a dual-channel using QR-code and a symmetric key-based authentication scheme using 2-factor in a multi_server environment.

Keywords
man-in-the-middle attack, authentication, session key, TMIS, smart card, multi-server

* 성결대학교 산업경영공학과 교수
- ORCID: https://orcid.org/0000-0003-2375-0640

· Received: Nov. 10, 2021, Revised: Dec. 10, 2021, Accepted: Dec. 13, 2021
· Corresponding Author: Kwang-Cheul Shin
Dept. of Industrial Management Engineering, Sungkyul University, Anyang, Korea,
Tel.: +82-31-467-8916, Email: skcskc12@hanmail.net

Ⅰ. 서 론

원격 사용자인증은 모든 보안 구조설계의 중요한 구성요소로써 인가된 사용자와 불법적인 사용자를 정확하게 구분할 수 있는 메커니즘이어야 한다[1]. 원격인증의 활용은 인터넷에 의해 PC와 모바일기기로 원격의료, 원격모니터링, 헬스케어, 온라인뱅킹, 온라인교육 등 수많은 서비스가 있다[2][3].

원격진료 의료정보시스템(TMIS, Telecare Medicine Information System)을 이용하면 의사가 오픈 채널을 통해 환자에게 실시간으로 의료상태에 대해 빠르게 접근하고 모니터링 할 수 있다[4]. 원격의료가 개인에게는 민감한 의료정보이기 때문에 공격자가 환자의 민감한 정보를 유추하는 것을 차단하는 것이 매우 중요하며 이를 위해 원격 사용자 인증시스템을 구현하여 합법적인 사용자만 TMIS에 접근하도록 할 수 있도록 하여야 한다[5]-[7].

최근 다수의 연구에서 많은 연구자들이 아이디, 비밀번호, 생체(예: 지문, 홍채) 및 스마트카드를 결합하여 보안을 강화하고 사용자 프라이버시를 보장하기 위해 3 파라미터 인증기법을 제안했다[8][9].

사용자의 개인 정보보호와 익명성을 위해 많은 연구에서 퍼지 추출기와 ECC(Elliptic Curve Cryptography)를 사용하는 생체기반 다중서버 인증방식을 제시했지만 계산, 통신 및 저장 요구사항에 대한 비용이 매우 높고 그들의 주장만큼 안전하지 않다는 것이 밝혀지고 있다[10]-[15]. 따라서 다중 서버 환경에서 합법적인 사용자를 위한 효율적인 보안 서비스를 제공하기 위해서는 안전한 인증 및 키 동의(AKA, Authentication and Key Agreement) 방식이 필요하다. 2019년 Barman et al'.s[4]는 퍼지추출기를 사용하여 헬스케어에 대한 인증스킴을 제안하였으나 알려진 많은 공격(서버/사용자 위장공격, 임시 비밀번호 유출, 사용자 익명성 부족 등)에 취약하다고 2020년 Ali et al'.s[16]이 분석하고 설계오류 문제를 개선한 인증 및 키 동의 방식의 인증스킴을 제안했다.

Ali et al'.s는 다중서버 환경에서 보안 서비스를 제공하기 위해 생체기반 키 동의 방식을 설계하여 위장공격, 세션 키 노출 및 내부자 공격과 같은 다양한 보안 위협에 안전하며 상호인증, 익명성 및 완전한 순방향 비밀성을 보장할 수 있다고 주장했다.

본 논문에서는 Ali et al'.s 스킴이 중간자공격(MITM, Man-In-The-Middle)에 의한 세션 키 노출, 스마트카드 도난에 의한 사용자 위장공격, 상호인증에 취약하다는 것을 증명하고 이러한 보안 위협을 해결하기 위한 개선방안을 제안한다.

제안방식은 QR-code와 데이터의 전송경로를 2중 채널로 하여 중간자공격의 위험성을 감소시키고 2-factor(QR_Code, 스마트카드)를 사용하는 대칭키 기반의 인증시스템으로 트랜잭션의 섹션에서만 유효한 비밀파라미터를 임시 저장하는 데이터베이스를 활용하여 설계한 스킴이다.

Ⅱ. Ali et al.'s 스킴 리뷰

Ali et al.'s scheme은 Barman et al.'s scheme[4]의 설계오류와 익명성, 사용자/서버의 위장공격 등 취약성을 분석하고 이에 따른 결함을 해결하기 위해 다중 서버 환경에서 대칭키 기반 인증 및 키 동의 방식을 제안하였다.

Ali et al.'s 스킴의 구조는 등록센터(RC, Regis_tration Center), 사용자/환자(User/Patient), 의료서버(MS, Medical Server)이고 과정프로세스는 등록프로세스와 로그인 및 키 동의 프로세스로 구성되며 사용된 표기는 표 1에서 용어를 정리하였다.

표 1. 표기 및 기술
Table 1. Notation and description

Symbol	Description
U_i	User i
RC	Registration center
S_j	Server j
PID_i,PWD_i	Identifier and password of U_i
SID_j	Identifier of S_j
Gen(), Rep()	Fuzzy extractors
SC	Smart card
K_{RC}, K_{Sj}	Secret key of RC and S_j
σ, τ	Biometric secret key and public reproduction
SK_{ij}	Session key of S_j and U_i
h()	Hash function
$\|$	Concatenation operation
$\oplus$	XOR operation

2.1 등록 과정

이 단계에서는 사용자/환자(이하 사용자)들과 의료서버(이하 서버)들이 등록센터에 등록하는 절차(그림 1)이다.

그림 1. 등록프로세스요약
Fig. 1. Summary of registration process

2.1.1 서버등록 프로세스

모든 서버는 등록센터에 등록해야 한다. 등록을 위해 각 서버 $S_j(1 \le j \le n)$는 아이디 SID_j를 안전한 채널로 등록센터에 전송하고 등록센터는 비밀키 K_{RC}를 사용하여 $S_{privj}=h(SID_j||K_{RC})$를 계산하고 S_j로 전송한다. 모든 서버의 $S_{priv*}(1 \le * \le n)$는 등록센터와 서버간의 공유키로 등록센터의 데이터베이스에 저장한다.

2.1.2 사용자등록 프로세스

모든 사용자들도 서비스를 이용하기 위해 등록센터에 등록해야 한다. 사용자 및 등록센터는 다음 단계를 수행함으로써 등록을 완료한다.

1단계 : 사용자가 자신의 아이디와 패스워드(PID_i, PWDi)를 선택하고 $HID_i=h(PID_i)$를 계산하여 등록센터에 전송, 등록요청을 한다.

2단계 : 등록센터는 무작위수 R_{rand1}과 사용자의 일시적(임시) 식별자 $TPID_i$를 선택한 후 $Auth_i=h(K_{RC} \| HID_i \| R_{rand1})$, $R_i=E_{KRC}[Auth_i, R_{rand1}, HID_i]$, $K_i=h(HID_i \| R_{rand1})$을 계산한다. 등록센터는 스마트카드에 $\{K_i, R_i, TPID_i\}$를 저장하여 안전한 채널로 사용자에게 전송한다.

3단계 : 사용자는 생체정보(BIO_i)를 퍼지추출함수 이용하여 생성자 $Gen(BIO_i)=(\sigma_i, \tau_i)$로 정규화된 랜덤스트링 σ_i와 헬퍼스트링 τ_i를 생성하고 이후 로그인 메시지 생성 할 때 사용자 자신의 인증을 위해 $A_i=h(PID_i \| PWD_i \| \sigma_i)$를 계산한다. 또한 스마트카드의 보안을 목적으로 $R'_i=R_i \oplus h(PWD_i \| \sigma_i)$, $K'_i=K_i \oplus h(PWD_i \| \sigma_i)$, $TPID'_i=TPID_i \oplus h(PWD_i \| \sigma_i)$을 계산하여 스마트카드에 다시 저장한다. 스마트카드는 $\{R_i, K_i, TPID_i\}$을 $\{R'_i, K'_i, TPID'_i\}$으로 대치하여 최종 저장되는 파라미터는 $\{A_i, R'_i, K'_i, TPID'_i, Gen(), Rep(), \tau_i\}$이다.

2.2 로그인 및 키 동의 과정

사용자가 서버에 로그인과 인증, 키 동의 과정을 수행하는 단계(그림 2)이다.

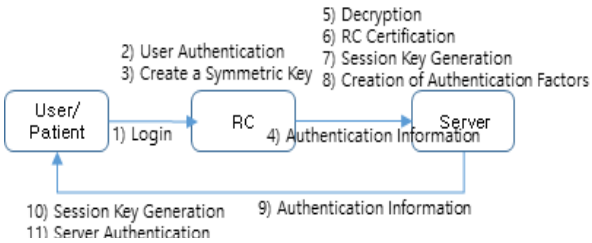

그림 2. 로그인 및 인증과정요약
Fig. 2. Summary of login and authentication process

1단계: 사용자는 스마트카드 SC_i를 삽입하고 PID_i, 생체정보 BIO'_i, PWD_i를 입력한다. 스마트카드의 정보복구를 위해 퍼지추출기 $Rep(Bio'_i, \tau_i)$를 통해서 정상적인 σ'_i를 생성해 낸다. 입력된 정보를 사용하여 $h(PID_i \| PWD_i \| \sigma'_i)$을 계산하고 A_i와 비교한다. 비교하여 A_i와 일치하면 자신의 소유자 인증이 확인되었으므로 로그인정보 생성을 위해 임의의 수 R_{rand2}와 타임스탬프 T1을 선택한다. 사용자만의 패스워드와 생체정보로 SC_i에 대치되었던 파라미터들을 $R_i=R'_i \oplus h(PWD_i \| \sigma'_i)$, $K_i=K'_i \oplus h(PWD_i \| \sigma'_i)$, $TPID_i=TPID'_i \oplus h(PWD_i \| \sigma'_i)$로 계산하여 복구한다. 다음은 로그인 정보의 생성과정식 (1)이다.

$$
\begin{aligned}
&HID'_i=h(PID_i) \qquad (1)\\
&R_{rand2}=R_{rand2} \oplus HID'_i\\
&TPID''_i=TPID_i \oplus HID'_i\\
&T'1=T1 \oplus HID'_i\\
&W_i=h(HID'_i \| K_i \| T1)
\end{aligned}
$$

이와 같이 생성된 로그인 정보 $Msg1=(R_i, SID_j, R'_{rand2}, W_i, TPID''_i, T'1)$을 공개채널을 통해서 등록센터로 전송된다.

2단계: 등록센터는 Msg1을 수신하여 정상적인 등록 자인지를 확인하기 위해 등록센터의 비밀키로 R_i를 복호화하고 다음 식 (2)를 진행한다.

$$D_{KRC}[R_i]=[Auth_i,\ R_{rand1},\ HID_i] \quad (2)$$
$$T1=T'1 \oplus HID_i$$
$$|T1-T'1| \leq \triangle T$$

이와 같이 메시지의 적시성으로 $|T1 - Tc| \leq \triangle T$을 체크하여 조건이 만족하면 다음과 같이 정당한 사용자인지를 확인(식 (3))한다.

$$W_i=?h(HID_i \| h(HID_i \| K_{RC}) \| T1) \quad (3)$$
$$Auth_i=?h(K_{RC} \| HID'_i \| R_{rand1})$$

서버로 전송될 로그인정보를 위해 $TPID_i$, R_{rand2}를 복구한 다음 타임스탬프 T2를 선택한다.

$$TPID_i=TPID''_i \oplus HID_i \quad (4)$$
$$R_{rand2}=R'_{rand2} \oplus HID_i$$

등록센터는 다음과 같이 대칭키 K_j와 세션키 정보를 계산하여 G_{RC}, SID_j를 서버로 전송한다.

$$K_j=h(SID_j \| K_{RC}) \quad (5)$$
$$W_{RC}=h(K_j \| T2)$$
$$Y_{RC}=h(SID_j \| HID_i \| R_{rand2} \| T1)$$
$$G_{RC}=E_{Kj}[TPID_i,\ W_{RC}, Y_{RC}, T1, T2]$$

3단계: 서버는 등록센터로부터 G_{RC}, SID_j를 수신하고 공유비밀키를 사용하여 G_{RC}를 복호화한다. 등록센터를 인증할 정보와 세션키 생성정보, 서버를 인증할 수 있는 파라미터를 계산하는 과정은 식 (6)과 같다.

$$Ds_{privj}[G_{RC}]=TPID_i,\ W_{RC}, Y_{RC}, T1, T2 \quad (6)$$

메시지의 적시성을 $|T2-Tc| \leq \triangle T$로 확인하고 만족하면 등록센터를 인증하기 위해 아래와 같이 비교한다. 일치하면 다음단계를 진행하고 그렇지 않으면 종료시킨다.

$$W_{RC}=?h(S_{privj} \| T2) \quad (7)$$

서버는 타임스탬프 T3를 선택하여 세션키와 인증정보를 계산(식 (8))한다.

$$SK_{ij}=h(Y_{RC} \| SID_j \| T3) \quad (8)$$
$$W_{Sj}=h(SK_{ij} \| T1 \| T3)$$

서버는 사용자에게 W_{Sj}, T3, $TPID_i$을 전송한다.

4단계: 사용자는 W_{Sj}, T3, $TPID_i$을 수신하고 메시지의 적시성 $|T3 - Tc| \leq \triangle T$를 확인하여 조건이 맞으면 다음을 진행하고 다르면 종료시킨다.
사용자는 Y_i를 계산하고 세션키(SK'_{ij})를 생성한다.

$$Y_i=h(SID_j \| HID'_i \| R_{rand2} \| T1) \quad (9)$$
$$SK'_{ij}=h(Y_i \| SID_j \| T3)$$

다음 등록센터와 서버를 인증하기 위해 아래와 같이 해시값을 W_{Sj}와 비교하여 일치하면 성공적으로 로그인과 인증 및 세션키 생성이 종료된다.

$$W_{Sj}=?h(SK'_{ij} \| T1 \| T3) \quad (10)$$

III. Ali et al.'s 스킴의 분석

Ali et al'.s 스킴의 제안은 Barman et al'.s 스킴의 몇 가지 결점인 내부자공격, 알고리즘의 논리적 오류, 도난 검증자 공격, 사용자 위장공격 등을 해소하기 위해 대칭키 기반의 인증 및 키 동의 스킴을 제안하였다.

재분석결과 Ali et al'.s 스킴은 사용자의 ID를 사용하지 않고 등록센터에 의해 임시 ID가 부여되므로 익명과 내부자공격을 보장하고 스마트카드 소지자를 확인하기 위해 자기 자신을 인증 할 때만 패스워드를 사용하므로 오프라인 패스워드 추측공격은 고려사항이 되지 않는다.

그러나 우리는 Ali et al.'s 스킴이 등록과정에서 불필요한 정보를 생성하고 있는 점과 스마트카드 도난공격으로 인해 사용자의 합법적 위장이 이루어지고 있으며 전송정보 도청(중간자공격)으로 세션키가 노출되는 위험한 스킴임을 분석하였다.

3.1 중간자(도청) 공격에 의한 세션키 복원

공격자는 비밀리에 도청하거나 이동하는 트래픽을 가로채서 수정, 파괴, 통신방해를 일으킨다. Ali et al'.s스킴은 공격자가 올바른 로그인 요청 메시지를 비밀 매개 변수 {HID_i, R_{rand2}, K_i}와 함께 {R_i, SID_j, R'_{rand2}, W_i, $TPID''_i$, T'1}를 계산할 수 없기 때문에 스킴이 중간자 공격을 견딜 수 있다고 주장했다. 그러나 공격자는 $h(PWD_i \| \sigma'_i)=R_i \oplus R'_i$, $K_i=K'_i \oplus h(PWD_i \| \sigma'_i)$, $TPID_i=TPID'_i \oplus h(PWD_i \| \sigma'_i)$, $HID'_i=TPID''_i \oplus TPID_i$, $R_{rand2}=R_{rand2} \oplus HID'_i$, $T'1=T1 \oplus HID'_i$를 성공적으로 계산한다. 따라서 Ali et al'.s 스킴은 중간자 공격에 안전하지 않다.

또한 참조하여 공격자가 합법적인 사용자를 가장하고 다음과 같이 세션 키 $SK_{MA}=h(Y_{MA} \| SID_j \| T3)$를 계산할 수 있음을 보여준다.

중간 공격자는 SC_i에 저장된 비밀 매개 변수를 추출하고 공용 채널을 통해 사용자, 등록센터 및 서버 간에 전송 된 데이터를 가로챌 수 있다.

그렇다면 공격자는 $h(PWD_i \| \sigma_i)=R'_i \oplus R_i$, $TPID_i=TPID'_i \oplus h(PWD_i \| \sigma_i)$, $HID'_i=TPID_i \oplus TPID''_i$, $R_{rand2}=R_{rand2} \oplus HID'_i$, $T1=T'1 \oplus HID'_i$을 계산하고 의료서버로부터 W_{MA}, T3, $TPID_i$ 메시지를 받은 후 공격자는 $Y_i=h(SID_j \| HID'_i \| R_{rand2} \| T1)$ 및 $SK_{ij}=h(Y_i \| SID_j \| T3)$를 성공적으로 계산한다. 그 결과 공격자가 사용자와 의료서버 사이에 세션키 SK_{ij}를 생성할 수 있으므로 Ali et al'.s 스킴은 세션 키 노출 공격에 취약하다.

3.2 스마트카드 도난 공격과 위장공격

Ali et al'.s 스킴은 획득한 매개 변수에 대한 지식만으로는 악의적인 공격자가 합법적인 사용자를 가장하는 데 유용한 정보를 얻을 수 없어야 한다고 주장했다. 그러나 공격자는 합법적인 사용자로 가장하고 올바른 세션 키 $SK_{ij}=h(Y_i \| SID_j \| T3)$를 생성할 수 있다. 따라서 Ali et al'.s 스킴은 스마트카드 도난공격에 대해 안전하지 않다. 스마트카드 도난시 로그인 생성정보 $W_i=h(HID'_i \| K_i \| T1)$는 무력화된다.

Ali et al'.s 스킴은 합법적인 공격자라 하더라도 엔티티 K_i와 PID_i를 알고 있어야 식 (11)을 계산할 수 있다고 주장하고 있다.

$$R'_{rand2}=R'_{rand2} \oplus HID_i \quad (11)$$
$$W'_i=h(HID'_i \| K_i \| T'1)$$
$$TPID'_i=TPID_i \oplus HID_i$$

공격자는 로그인과 인증정보를 도청하여 아래와 같이 HID_i, R_{rand2}, $TPID_i$를 계산할 수 있다.

$$.HID_i=TPID_i \oplus TPID''_i \quad (12)$$
$$.R_{rand2}=R'_{rand2} \oplus HID'_i$$
$$.T1=T'1 \oplus HID'_i$$

또한 스마트카드 도난 시에는 식 (13)을 계산함으로써 위장공격에 취약하다.

$$.Y_{RC}=h(SID_j \| HID_i \| R_{rand2} \| T1) \quad (13)$$
$$.Y_i=h(SID_j \| HID'_i \| R_{rand2} \| T1)$$

3.3 상호인증

상호인증은 두 실체가 서로의 신분을 확인시켜주는 양방향 인증 방법으로 Ali et al'.s 스킴에서는 사용자, 등록센터, 의료서버 간의 상호인증이 이루어진다고 주장했다. 그러나 3.1절, 3.2절에서와 같이 공격자는 정확한 로그인 요청 메시지 R_i, SID_j, R'_{rand2}, W_i, $TPID''_i$, T'1과 인증 응답 메시지 W_{Sj}, T3, $TPID_i$를 성공적으로 계산할 수 있다. 따라서 Ali et al'.s 스킴은 안전한 상호 인증을 제공하지 못한다.

3.4 데이터베이스 불용

등록센터는 의료서버의 아이디 SID_j를 안전한 채널로 수신하여 등록센터의 비밀키가 포함된 해시값 $S_{privj}=h(SID_j||K_{RC})$를 계산하여 S_j로 전송하고 자신의 데이터베이스에 저장한다. 멀티서버 환경에서 다수의 서버 비밀키를 데이터베이스에 저장하고 있으나 로그인 정보는 사용자로부터 Msg1=(R_i, SID_j, R'_{rand2}, W_i, $TPID''_i$, T'1)에 의해 서버의 아이디 SID_j가 포함되어 $K_j=h(SID_j \| K_{RC})$를 계산할 때 서버의 아이디와

등록센터의 비밀키를 사용하므로 데이터베이스 사용이 불필요하다. 즉 서버의 아이디를 사용자로부터 수신을 받기 때문에 데이터베이스에 저장되어있는 각 서버와의 비밀키 저장은 무의미하다.

Ⅳ. 제안 스킴

3장에서 Ali et al'.s 스킴이 공격자의 중간자공격에 의한 세션 키 노출과 스마트카드 도난에 따른 위장공격, 상호인증의 부정확 등 스킴설계에 많은 취약점을 가지고 있음을 보였다. 따라서 Ali et al'.s 스킴의 이러한 보안위협을 해결하기 위한 개선이 필요하다. 일반적으로 합법적인 공격자가 인증 및 키 동의 단계에서 메시지를 쉽게 삽입, 삭제, 가로채고 수정할 수 있으므로 모든 참가자는 대칭키를 사용하여 메시지를 안전하게 암호화하고 전송하는 것이 안전하다. 또한 다른 엔티티를 활용한 다중채널, 다중요소 인증시스템으로 개선하여 사용자들의 안전성을 보장해야 한다. 세션 키 SK_{ij}는 임의의 난수 또는 등록센터에서 1회성으로 생성되는 비밀 값들을 매개 변수로 구성되어야 한다. 그리고 중간자 공격에 대응할 수 있는 인증방법으로 스마트 기기의 QR-code 인코딩(데이터를 코드화하고 압축하는)을 이용하여 인증하는 방법이다.

스마트카드를 분실하거나 도난당한 경우 악의적인 공격자는 합법적인 사용자로 위장하여 손쉽게 로그인 메시지를 생성할 수 있기 때문에 적법한 사용자와 서버만이 알거나 계산할 수 없는 비밀정보 값을 추가해야 한다. 또한 사용자의 PC와 스마트 기기를 활용한 두 가지 채널과 이중요소(2-channel, 2-factor)를 사용하는 인증시스템을 설계한다.

등록센터의 데이터베이스 활용으로 해당 트랜잭션의 섹션에서만 유효한 비밀파라미터를 임시 저장하는 저장소로 활용하면 가치를 높일 수 있다.

본 제안은 Ali et al'.s 스킴의 취약성을 개선할 목적으로 QR-code를 이용한 2중 채널과 대칭키 암호화를 기반으로 한 스킴이다. 본 제안스킴은 등록 프로세스, 로그인 및 인증, 키 동의 프로세스로 구성된다.

4.1 등록프로세스

등록프로세스는 사용자/환자(이하 U)들과 의료서버(이하 S)들이 등록센터(이하 RC)에 등록(그림 3, 4)하는 절차이다.

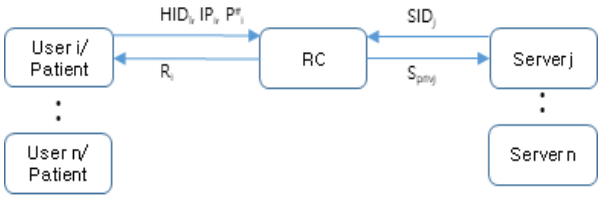

그림 3. 등록 프로세스
Fig. 3. Registration process

User(U_i) Registration centre(RC)

Selects PID_i, PWD_i compute
$HID_i=h(PID_i \| PWD_i)$
---------HID_i, $P^{\#}_i$, IP_i------->
secure channel Selects a random number R_{rand1},
$Auth_i=h(K_{RC} \| HID_i \| R_{rand1})$
$R_i=E_{KRC}[Auth_i, R_{rand1}, HID_i]$
Store $\{R_i\}$ into the SC_i
and IP_i, $P^{\#}_i$ in database
<----------(Smart card)---------
secure channel
imprint BIO_i Computes
$Gen(BIO_i)=(\sigma_i, \tau_i)$
$A_i=h(PID_i \| PWD_i \| \sigma_i)$
Finally SC_i contains $\{A_i, R_i, Gen(), Rep()\}$

그림 4. 사용자등록 프로세스
Fig. 4. User registration process

4.1.1 서버등록 프로세스

Ali et al'.s 스킴의 서버등록 프로세스는 2.1.1과 동일하다.

4.1.2 사용자등록 프로세스

모든 U들은 서비스를 이용하기 위해 RC에 등록해야 한다.

1단계 : U_i가 자신의 PID_i, PWD_i를 선택하여 $HID_i=h(PID_i \| PWD_i)$를 계산하고 U_i의 아이피(IP_i)와 모바일기기 번호($P^{\#}_i$)를 RC로 전송하여 등록

요청을 한다.

2단계: RC는 임의의 수 R_{rand1}을 선택한 후 식 (14)를 계산한다.

$$Auth_i=h(K_{RC} \| HID_i \| R_{rand1}) \quad (14)$$
$$R_i=E_{KRC}[Auth_i, R_{rand1}, HID_i]$$

RC는 안전한 채널로 U_i에게 스마트카드에 $\{R_i\}$를 저장하여 전송하고 자신의 데이터베이스에 사용자 U_i의 등록정보 $\{IP_i,P^{\#}_i\}$를 저장한다.

3단계: 사용자 U_i는 생체정보 BIO_i를 스캔하여 $Gen(BIO_i)=(\sigma_i, \tau_i)$과 $A_i=h(PID_i \| PWD_i \| \sigma_i)$를 계산하고 스마트카드에 $\{A_i, R_i, Gen(), Rep()\}$를 저장한다.

Mobile Device	Patient (U_i/SC_i)	Registration centre(RC)	Server(S_j)
	U_i inserts SC_i inputs PID_i, PWD_i		
	Imprints BIO'_i		
	Compute $Rep(BiO'_i, \tau_i)=\sigma'_i$		
	$A_i=?h(PID_i \| PWD_i \| \sigma'_i)$ else terminate		
	www.RC.or------>$TPID_i$ generate and DB temporary storage		
<----capture	<-------Res QR_Code--------- Encode($TPID_i$)		
Decode($TPID_i$)			
---------Res(IP_i, $TPID_i$)--------->Authentication (IP_i->$P^{\#}_i$)Nonce generate and DB temporary storage			
<------------Nonce----------			
$K_1=h(TPID_i \oplus Nonce \oplus HID_i)$			
	Generate R_{rand2}, T1 and compute		
	$Msg1=E_{K1}[R_{rand2}, TPID_i, SID_j]$		
	----------R_i, T1, Msg1---------->		
		$\|T1-T'1\| \leq \triangle T$	
		$D_{KRC}[R_i]=[Auth_i, R_{rand1}, HID_i]$	
		$Auth_i=?h(K_{RC} \| HID_i \| R_{rand1})$ //Ui authentication	
		$K_1=h(TPID_i \oplus Nonce \oplus \mathbf{HID}_i)$	
		$D_{K1}[Msg1]=(R_{rand2}, TPID_i, SID_j)$	
		Generate a timestamp T2	
		$W_{RC}=h(h(SID_j \| K_{RC}) \| T2)$	
		$Y_{RC}=h(SID_j \| HID_i \| R_{rand2} \| T1)$	
		$K_j=h(SID_j \| K_{RC})$	
		$Msg2=E_{Kj}[TPID_i, W_{RC}, Y_{RC}, T1, IP_i]$, **T2**	
		----------Msg2------->	
			$\|T2-Tc\| \leq \triangle T$
			$S_{privj}[G_{RC}]=[TPID_i, W_{RC}, Y_{RC}, T1, T2, IP_i]$
			$W_{RC}=?h(S_{privj} \| T2)$ //RC authentication
			Generate T3 timestamp
			$SK_{ij}=h(Y_{RC} \| SID_j \| T3 \| TPID_i)$
			$W_{Sj}=h(SK_{ij} \| T1 \| T3)$
		<----------W_{sj}, T3----------	
		$\|T3-Tc\| \leq \triangle T$	
		$Y_i=h(SID_j \| HID_i \| R_{rand2} \| T1)$	
		$SK_{ij}=h(Y_i \| SID_j \| T3 \| TPID_i)$	
		$W_{Sj}=?h(SK_{ij} \| T1 \| T3)$	

그림 5. 로그인 및 키 동의 프로세스
Fig. 5. Login and key agreement process

4.2 로그인과 키 동의 프로세스

U_i가 S_j에 로그인하기 위해 수행하는 단계(그림 5)이다.

1단계: U_i는 스마트카드 SC_i를 삽입하고 PID_i, PWD_i을 입력한다. 그 후 생체정보 BIO'_i를 스캔하여 $Rep(BiO'_i, \tau_i)=\sigma'_i$와 $h(PID_i \| PWD_i \| \sigma'_i)$를 계산하고 Ui의 스마트카드에 저장되어 있는 Ai와 비교($A_i=?h(PID_i \| PWD_i \| \sigma'_i)$)한다. 만약 두 값이 일치하지 않으면 로그인절차를 중단한다. U_i의 자체 인증이 성공하면 RC 메인페이지에 접속(QR_code 요청)한다. RC는 U_i의 IP주소를 통해서 데이터베이스에 등록된 스마트기기 번호를 확인한 후 사용자의 식별자 $TPID_i$를 선택하여 데이터베이스에 저장하고 QR_code로 인코딩($Encode(TPID_i)$)하여 사용자에게 전송한다. 사용자는 스마트기기로 웹 브라우저에 출력된 QR_code를 촬영하여 디코딩($Decode(TPID_i)$)한 후 자신의 IP_i와 $TPID_i$를 RC로 전송한다. RC는 수신한 IP_i와 $TPID_i$, $P^{\#}_i$를 통해 U_i를 확인하고 임의의 수 Nonce를 생성하여 사용자의 스마트기기로 전송한다. 사용자의 스마트기기는 로그인 정보를 암호화할 비밀키를 생성($K_i=h(TPID_i \oplus Nonce) \oplus \mathbf{HID_i}$)한다.

2단계: U_i는 R_{rand2}, T1을 선택하여 식 (15)를 계산하여 RC에 Msg1, T1, R_i를 전송한다.

$$Msg1=E_{Ki}[SID_j, R_{rand2}, TPID_i] \quad (15)$$

3단계: **RC**는 Msg1, T1, R_i를 수신하여 타임스탬프 조건 $|T1 - Tc| \leq \triangle T$을 체크하고 참이면 다음을 진행한다. RC의 비밀키로 Ri를 복호화($D_{KRC}[R_i]=[Auth_i, R_{rand1}, HID_i]$)하여 정상적인 등록자 확인을 위해 Authi, R_{rand1}, HID_i를 획득하고 $h(K_{RC} \| HID_i \| R_{rand1})$를 계산한다. 이 후 복호화된 파라미터 $Auth_i$와 비교($Auth_i=?h(K_{RC} \| HID_i \| R_{rand1})$)하여 일치하지 않으면 세션을 중단하고 일치하면 정상적인 등록자이므로 Msg1을 복호화한다.

$$K_i=h(TPID_i \oplus nonce) \quad (16)$$

$$D_{Ki}[Msg1]=[SID_j, R_{rand2}, TPID_i]$$

RC는 타임스탬프 T2를 선택하고 식 (17)을 계산한다.

$$K_j=h(SID_j \| K_{RC}) \quad (17)$$
$$W_{RC}=h(K_j \| T2)$$
$$Y_{RC}=h(SID_j \| HID_i \| R_{rand1} \| T1)$$
$$Msg2=E_{Kj}[TPID_i, W_{RC}, Y_{RC}, T1, IP_i]$$

RC는 S_j로 Msg2, T2를 전송한다. 이후 RC는 데이터베이스에 임시 저장한 $TPID_i$와 Nonce를 삭제한다.

4단계: S_j는 RC로부터 Msg2, T2를 수신하고 메시지 적시성을 위해 타임스탬프 조건 $|T2-Tc| \leq \triangle T$을 체크하여 참이면 식 (18)을 계산한다.

$$S_{privj}[Msg2]=[TPID_i, W_{RC}, Y_{RC}, T1, IP_i] \quad (18)$$

메시지의 적시성을 검증하고 $W_{RC}=?h(S_{privj} \| T2)$의 유효성 검사가 성공하면 S_j는 타임스탬프 T3을 선택하고 식 (19)를 계산한다.

$$SK_{ij}=h(Y_{RC} \| SID_j \| T3 \| TPID_i) \quad (19)$$
$$W_{Sj}=h(SK_{ij} \| T1 \| T3)$$

S_j는 W_{Sj}와 T3를 U_i로 전송한다.

5단계: 사용자 U_i가 W_{sj}, T3를 수신하고 메시지의 $|T3-Tc| \leq \triangle T$의 유효성 검사가 성공하면 세션키 생성과 서버 S_j의 확인을 위해 다음을 계산한다.

$$Y_i=h(SID_j \| HID_i \| R_{rand2} \| T1) \quad (20)$$
$$SK'_{ij}=h(Y_i \| SID_j \| T3 \| TPID_i)$$

$W_{Sj}=?h(SK'_{ij} \| T1 \| T3)$이 참이면 서버인증과 세션키 생성이 성공되었다.

Ⅴ. 제안스킴 보안분석 및 평가

본 스킴의 분석에서는 3장의 Ali et al'.s스킴에서

취약점을 보인 중간자 공격에 의한 세션키의 노출 문제와 스마트카드 도난공격에 따른 공격자의 위장 공격에 대해 보완하여 새로운 스킴의 진전된 프로세스의 분석이다.

5.1 중간자공격

공격자는 이 공격을 이용하여 개인정보나 로그인 정보의 수집에 중점을 두는 공격으로 온라인 뱅킹의 경우 사용자의 계좌나 송금액을 변경할 수 있는 위협이다. Ali et al'.s 스킴에서 로그인 정보 (Msg1=(R_i, SID_j, R'_{rand2}, W_i, TPID"$_i$, T'1))와 의료서버의 인증정보(W_{Sj}, T3, $TPID_i$))는 공개채널로 전송되어 공격자는 이 정보들을 도청. 캡쳐하여 인증을 확인받고 세션키를 생성해 내는 위험이 포함되어 있다.

제안 스킴에서는 2채널의 스마트기기를 사용하여 매개변수들을 교환하고 해시된 HIDi(PIDi와 PWDi)를 사용하여 암호키 K1=h(TPIDi⊕Nonce⊕HIDi)를 생성한다. 암호키 K1은 스마트기기에서 생성하고 웹브라우저에서 입력하여 암호문(Msg1)을 생성한다. 공개채널에서 Msg1, Msg2는 대칭키 암호문으로 공격자가 암호키 K1을 계산하기 위해서는 무선채널의 스마트기기 수신정보와 사용자의 아이디, 패스워드를 알고 있어야 한다. 또한 Ri와 Msg2는 등록센터의 비밀키를 알고 있어야 하므로 공격자는 이 공격을 사용할 수 없다.

5.2 스마트카드 도난공격

사용자의 스마트카드가 분실, 도난 또는 복사되었다고 가정하면 공격자는 전력분석 방법[17]으로든지 스마트카드 메모리로부터 저장된 정보 {Ai, Ri, Gen(), Rep()}를 추출한다. Ai=h(PIDi ‖ PWDi ‖ σ'i)는 스마트카드 소유자임을 증명하는 인자로 로그인 메시지 작성에 참여하지 않으며 Ri=EKRC[Authi, Rrand1, HIDi]는 공개채널에 노출되어 전송되고 있으나 등록센터의 비밀키로 암호화되어 해독이 불가능하다. 공격자는 스마트카드를 획득한다 해도 로그인 메시지 생성에 도움이 되지 않는다.

5.3 사용자 위장공격

공격자가 합법적 사용자로 위장하기 위해서는 정상적인 로그인 메시지를 생성할 수 있어야 한다. 정상적인 메시지를 생성하기 위해서는 파라미터 Ri, TPIDi, Nonce, HIDi가 필요하다. Ri는 스마트카드에 내장된 정보 또는 사용자의 로그인메시지를 도청하여 쉽게 얻을 수 있다. 그러나 TPIDi, Nonce는 이중 채널의 스마트기기로 전송되는 파라미터로 획득이 어려우며 만일 획득했더라도 HIDi를 알아야 조작된 위장메시지를 생성할 수 있다.

비밀키 K1=h(TPIDi⊕Nonce⊕HIDi)은 해시 값으로 합법적 사용자가 아니면 생성할 수 없는 구조이다. 특히 HIDi=h(PIDi ‖ PWDi)는 사용자의 아이디와 패스워드를 해시값으로 계산되어 공격자는 알아낼 수 없으며 또 다른 방법으로 Ri를 해독하려면 등록센터의 비밀키를 알아야 하기 때문에 위장공격은 불가능하다.

5.4 세션키 보안

세션키는 등록센터에서 정당한 사용자 확인 후 등록센터로부터 수신한 신뢰정보를 바탕으로 의료서버와 사용자간에 SKij를 생성한다. 세션키 생성을 위한 흐름은 Encoding된 QR_code의 TPIDi와 사용자의 임의의 수 Rrand2, 수신서버 SIDi, HIDi는 사용자와 등록센터간의 공통키인 비밀키 K1으로 암호화되었고 YRC 또한 등록센터와 의료서버의 공통키인 비밀키로 암호화되어 보호되고 있으며 TPIDi와 Rrand2, 타임스탬프 T3는 세션마다 값이 바뀌므로 이전의 세션키로 새로운 세션키를 유추할 수 없는 구조이다.

5.5 상호인증

제안 스킴에서 등록센터는 다음 3가지 조건으로 사용자를 인증한다. 타임스탬프의 신선도(|T1-T'1|≤ △T)를 체크하여 재전송여부를 확인하고 파라미터 Ri(=EKRC[Authi, Rrand1, HIDi])는 등록센터에서 발급한 것인지를 비밀키의 해독(DKRC[Ri]=[Authi, Rrand1, HIDi])으로 알 수 있으며 해독된 파라미터

들과 등록센터의 비밀키를 해시한 값 Authi=?h(KRC ‖ HIDi ‖ Rrand1)를 계산하여 사용자를 확인한다.

또한 공통키 K1=h(TPIDi⊕Nonce⊕HIDi)을 계산할 수 있는 사용자는 정당하게 등록센터에 등록한 개체로 스마트기기로 전송된 정보와 사용자가 해시값으로 등록할 때의 아이디와 패스워드 소지자(HIDi=h(PIDi ‖ PWDi))만이 생성할 수 있다.

5.6 Reply 공격

등록센터의 데이터베이스는 각 세션마다 새로운 TPIDi와 Nonce, timestamp가 생성되어 Reply 공격을 차단한다. 공격자가 Msg1을 재전송했을 때 RC의 데이터베이스에는 TPIDi와 Nonce가 삭제되어 Msg1을 해독할 수 없다.

5.7 도난 검증자 공격

도용된 검증자공격은 악의적인 사용자가 서버에 저장된 검증데이터인 암호 등을 훔치거나 수정하는 것을 의미한다. 제안된 방식에서 등록센터는 데이터베이스에 사용자의 패스워드, 생체인식 등 확인정보를 유지하지 않고 있다. IPi와 P#i는 이중채널을 사용하므로 동일한 스마트기기번호를 사용할 수 없으므로 무의미하고 TPIDi와 Nonce는 한 세션동안 만 사용되고 데이터베이스에서 0으로 다시 세트된다. 따라서 제안된 기법은 도용된 검증자공격에 안전하다.

VI. 효율성 분석

이 장에서는 다중서버기반 인증방식인 Ali et al'.s 스킴에 대한 기능 및 비용과 관련하여 제안된 방식을 평가한다.

제안된 스킴에 대하여 Ali et al'.s 스킴과 비교하여 재분석결과가 표 2와 같다. Ali et al'.s는 F#1(사용자익명성)부터 F#10의 완전순방향 기밀성까지 보안의 안전기능을 완벽하게 설계하였다고 주장하였으나 본 논문에서 재분석한 결과 Ali et al'.s 스킴은 사용자의 아이디 대신에 등록센터에 의해 임시 아이디가 부여되므로 익명과 내부자공격은 보장한다. 또한 스마트카드 소지자를 확인하기 위해 자기 자신을 인증 할 때만 패스워드를 사용하므로 오프라인 패스워드 추측공격은 고려사항이 되지 않는다는 장점이 있다. 그러나 Ali et al'.s 스킴은 사용자위장공격, 상호인증, 중간자공격, 도난 스마트카드공격, 완전 순방향 기밀성에 대한 다양한 공격에 취약함을 보였고 본 논문에서 이에 대응하는 개선된 스킴을 설계하여 필요한 모든 보안 요구 사항을 충족하고 다중 서버 환경에서 다양한 공격에 대해 안전함을 보였다.

안전한 스킴설계에 주요연산으로 이중채널에 의한 QR_code와 대칭키 암호기법의 비밀키 암호화(TE)와 복호화(TD) 연산, 퍼지추출(Tfe) 연산으로 평가하였다.

표 3의 계산비용[18]은 서버기준으로 대칭키 암호화/복호화(AES 256bit) 시간비용은 0.8ms, 해시함수 시간비용은 0.01ms, 퍼지추출 시간비용은 2.23ms 이다.

표 3. 개략연산시간
Table 3. Approximate time required for various operations

Notation	Description	Approx. execution time(in ms)
Th	Hash function	0.01ms
TE/D	Symmetric enc/dec	0.8ms
Tfe	Fuzzy extractor	2.226ms

표 2. 보안속성의 재분석 결과
Table 2. Result of re-analysis of security characteristics

Attack Type	F#1	F#2	F#3	F#4	F#5	F#6	F#7	F#8	F#9	F#10
Ali et al.'s	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Re_analysis result	✓	✓	✓	x	✓	x	✓	x	x	x
Proposed scheme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

F#1: 사용자 익명성 F#2: 내부자공격 F#3: 오프라인패스워드추측공격 F#4: 사용자 위장공격 F#5: 서버위장공격
F#6: 상호인증 F#7: 재생공격 F#8: 중간자공격 F#9: 도난 스마트카드공격 F#10: 완전 순방향 기밀성

표 4. 연산시간비교
Table 4. Comparison of computation costs

Scheme	MD	User	RC	Server	Time(ms)
Ali et al'.s		6Th+1Tfe	2TE/D+6Th	3Th+1TE/D	≈4.766ms
Our	1TE/D+1Th	4Th+1TE/D+1Tfe	4TE/D+4Th	3Th+1TE/D	≈7.946ms

표 4는 제안스킴이 모바일기기의 디코딩과 로그인메시지의 암호화의 필요성으로 Ali et al'.s 스킴보다 약2배 정도의 시간지연이 발생한다는 것으로 보여준다. 통신에서 Ali et al'.s 스킴의 로그인 및 인증 메시지에 대한 도청(중간자)공격을 회피하기 위해 모바일기기를 이용한 QR_code와 인증자 교환으로 총 4라운드의 통신을 추가로 필요로 한다. 표 4는 제안된 방식의 계산비용이 Ali et al'.s 보다 높음을 보여주지만 제안된 방식이 다른 방식보다 견고하고 안전함을 알 수 있다.

Ⅶ. 결 론

Ali et al'.s 는 Barman et al'.s 스킴의 논리적 설계오류, 사용자 위장공격 등을 해결하기 위해 대칭키 기반의 인증 및 키 동의 스킴으로 개선하여 제안하였다.

재분석한 결과 Ali et al'.s 스킴은 사용자의 아이디를 대신하여 등록센터에 의해 일시적 아이디가 발급되어 익명성과 오프라인 패스워드 추측공격은 고려사항이 되지 않는 장점을 갖는 반면에 중간자 공격에 의한 세션키 노출과 및 스마트카드 도난 공격에 이은 사용자 위장공격에 취약하고 상호 인증을 보장하지 않는 것으로 분석하였다. 등록과정에서 불필요한 정보의 생성으로 인해 사용자의 합법적 위장이 이루어지며 전송정보 도청(중간자공격)으로 세션키가 노출되는 위험한 스킴임을 알 수 있었다. 이러한 취약점을 해결하기 위해 본 논문에서는 QR-code를 이용한 2중 채널과 2-factor를 사용하는 대칭키 기반의 인증스킴을 제안하였다. 그 결과 도청에 의한 중간자 공격이 되지 않기에 세션키의 안전성이 확보되고 이로 인해 완전 순방향기밀성이 보호되며 이중채널로 인해 스마트카드가 도난 되더라도 사용자의 위장공격이 될 수 없다. 이러한 제안된 방식은 향후 다중서버 환경에서 원격의료, 헬스케어, 온라인뱅킹 등에서 인증 및 키 동의 설계에 활용될 것이다.

References

[1] Y. Park, K. Park, K. Lee, H. Song, and Y. Park: "Security analysis and enhancements of an improved multi-factor biometric authentication scheme", International Journal of Distributed Sensor Networks, Vol. 13, No. 8, pp. 1-15, Aug. 2017. http://dx.doi.org/10.1177/1550147717724308.

[2] Y. Zhang, L. Sun, H. Song, and X. Cao, "Ubiquitous wsn for healthcare:Recent advances and future prospects", IEEE Internet of Things Journal, Vol. 1, No. 4, pp. 311-318, Aug. 2014. https://doi.org/10.1109/JIOT.2014.2329462.

[3] U. Gogate and J. Bakal, "Refining healthcare monitoring system using wireless sensor networks based on key design parameters", in Information and Communication Technology for Intelligent Systems, pp. 341-349, 2019. https://doi.org/10.1007/978-981-13-1742-2_33.

[4] S. Barman, H. P. Shum, S. Chattopadhyay, and D. Samanta, "A secure authentication protocol for multi-server-based e-healthcare using a fuzzy commitment scheme", IEEE Access, Vol. 7, pp. 1-18, 2019. https://doi.org/10.1109/ACCESS.2019.2893185.

[5] S. H. Li, C. Y. Wang, W. H. Lu, Y. Y. Lin, and D. C. Yen, "Design and implementation of a telecare information platform", Journal of medical systems, Vol. 36, No. 3, pp. 1629-1650, Jun. 2012. https://doi.org/10.1007/s10916-010-9625-6.

[6] S. A. Chaudhry, H. Naqvi, and M. K. Khan, "An enhanced lightweight anonymous biometric based authentication scheme for tmis", Multimedia Tools and Applications, Vol. 77, No. 5, pp. 5503-5524,

Mar. 2018. https://link.springer.com/article/10.1007/s11042-017-4464-9.

[7] K. Mahmood, J. Arshad, S. A. Chaudhry, and S. Kumari, "An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure", International Journal of Communication Systems, Vol. 32, No. 16, pp. 1-16, Nov. 2019. http://dx.doi.org/10.1002/dac.4137.

[8] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ecc-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks", Computers & Electrical Engineering, Vol. 69, pp. 534–554, Jul. 2018. https://doi.org/10.1016/j.compeleceng.2017.08.003.

[9] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards", Journal of Network and computer applications, Vol. 33, No. 1, pp. 1–5, Jan. 2010. http://dx.doi.org/10.1016/j.jnca.2009.08.001.

[10] Q. Pu, J. Wang, and R. Zhao, "Strong authentication scheme for telecare medicine information systems", Journal of medical systems, Vol. 36, No. 4, pp. 2609–2619, Aug. 2012. https://doi.org/10.1007/s10916-011-9735-9.

[11] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment", IEEE Systems Journal, Vol. 9, No. 3, pp. 816–823, Sep. 2015. https://doi.org/10.1109/JSYST.2014.2301517.

[12] Wang, X. Zhang, Z. Zheng, and M. K. Khan, "Cryptanalysis and improvement of a biometric-based multi-server authentication and key agreement scheme", PLoS ONE, Vol. 11, No. 2, pp. 1-25, Mar. 2016. https://dx.doi.org/10.1371%2Fjournal.pone.0149173.

[13] Kumari, X. Li, F. Wu, A. K. Das, K. K. R. Choo, and J. Shen, "Design of a provably secure biometrics-based multi-cloud-server authentication scheme", Future Generation Computer Systems, Vol. 68, pp. 320–330, Mar. 2017. http://dx.doi.org/10.1016/j.future.2016.10.004.

[14] R. Ali and A. K. Pal, "An efficient three factor-based authentication scheme in multiserver environment using ECC", International Journal of Communication Systems, Vol. 31, No. 4, pp. 1-22, Mar. 2018. https://doi.org/10.1002/dac.3484.

[15] K. C. Shin, "A Robust Authentication Scheme Based on ECC and Dynamic ID for Remote Telecare Medical Information Systems", The Journal of Korean Institute of Information Technology, Vol. 17, No. 6, pp. 123-132, Jun. 2019. http://dx.doi.org/10.14801/jkiit.2019.17.6.123.

[16] Z. Ali, S. Hussain, R. H. U. Rehman, A. Munshi, M. Liaqat, N. Kumar, and S. A. Chaudhry, "ITSSAKA-MS: An improved three-factor symmetric-key based secure AKA scheme for multi-server environments", IEEE Access, Vol. 8, pp. 107993-108003, Jun. 2020. https://doi.org/10.1109/ACCESS.2020.3000716.

[17] T. Messerges, E. Dabbish, and R. Sloan, "Examining Smart-card Security under the Threat of Power Analysis Attacks", IEEE Trans. Comput. Vol. 51, No. 5, pp. 541-552, May 2002. https://doi.org/10.1109/TC.2002.1004593.

[18] S. Adhikari, S. Ray, Gosta P. Biswas, and Mohammad S. Obaidat, "Efficient and secure business model for content centric network using elliptic curve cryptography", Sharmistha Adhikari, Sangram Ray, Gosta P. Biswas, Mohammad S. Obaidat, pp. 1-26, Oct. 2018. https://doi.org/10.1002/dac.3839.

저자소개

신 광 철 (Kwang-Cheul Shin)

1985년 2월 : 서울과학기술대학교 전자계산학과(공학사)
1990년 12월 : 국방대학원 전자계산학과(공학석사)
2003년 8월 : 성균관대학교 대학원 정보공학과(공학박사)
2004년 3월 ~ 현재 : 성결대학교 산업경영공학과 부교수
관심분야 : 정보보호, 프로젝트관리, 소프트웨어 표준화