Journal of KIIT. Vol. 17, No. 6, pp. 123-132, Jun. 30, 2019. pISSN 1598-8619, eISSN 2093-7571 123
http://dx.doi.org/10.14801/jkiit.2019.17.6.123

원격 의료정보시스템을 위한 ECC와 동적 ID기반의 강력한 인증스킴

신 광 철*

A Robust Authentication Scheme Based on ECC and Dynamic ID for Remote Telecare Medical Information Systems

Kwang-Cheul Shin*

요 약

원격 의료 정보 시스템(TMIS)에 대한 인증 체계는 안전하고 인증된 접근을 보장해야 한다. 식별자 및 패스워드기반의 인증방식은 도청 및 위장공격에 취약하며 특히 TMIS에서 중요한 민감한 개인정보의 익명성이 보장되지 않는다. 최근에는 사용자의 개인정보를 효율적으로 보호하기 위해 TMIS에 대한 동적 ID 기반 원격 사용자 인증 체계가 제시되고 있으나 기존의 동적 ID 기반 인증 방식의 대부분은 입력 검증 조건을 무시하고 있다. 이로 인해 로그인 및 암호 변경 단계가 비효율적이며 암호 변경 단계에서 입력이 잘못되었을 때 서비스 거부 공격을 유발할 수 있다. 이러한 약점을 극복하기 위해 난수의 강도를 높이기 위해 ECC 기반의 새로운 동적 ID 기반 인증 방식을 제안했다. 제안된 기법은 사용자의 익명성과 사용자 및 서버의 위장공격에 안전한 강력한 인증스킴을 제안한다.

Abstract

The certification system for the telecare medicine information system(TMIS) should ensure secure and authorized access. Identifier and password-based authentication methods are vulnerable to eavesdropping and spoofing attacks, and TMIS does not protect the anonymity of sensitive personal information. Recently, a dynamic ID-based remote user authentication scheme for TMIS has been proposed to efficiently protect user's personal information. However, most of the existing dynamic ID-based authentication schemes ignore input validation conditions. This can lead to a denial of service attack when the login and password change phases are inefficient and the input in the password change phase is incorrect. To overcome these drawbacks, we proposed a new dynamic ID-based authentication scheme using ECC to increase the strength of random numbers. The proposed scheme proposes a robust authentication scheme that is robust against user anonymity and user and server spoofing attacks.

Keywords
TMIS, biometrics, mutual authentication, impersonation attack, anonymity

* 성결대학교 산업경영공학부
- ORCID: http://orcid.org/0000-0003-2375-0640

· Received: Mar. 09, 2019, Revised: May 03, 2019, Accepted: May 06, 2019
· Corresponding Author: Kwang-Cheul Shin
Department of Industrial Management Engineering, Sungkyul University, 53 Sungkyul University-ro Manan-gu, Anyang-si, Gyeonggi-do, 14097, Korea.
Tel.: +82-2-820-0908, Email: skcskc12@sungkyul.ac.kr

Ⅰ. 서 론

지난 몇 년간 기술의 발달로 의료산업의 패러다임이 변화를 겪으며 환자중심의 능동적인 의료서비스가 도래하였다. 가장 중요한 부분으로 의료정보의 디지털화인데 그 중심에 있는 TMIS는 사용자 친화적이고 환자 중심의 응용프로그램으로 더 편리한 환자서비스 제공, 진료예약, 진행사항 확인, 전자처방전 등이 포함된다. 이러한 시스템을 갖추기 위해서 기본적으로 의료데이터 보안과 개인정보보호의 침해에 대한 대책이 필요하다. 인터넷의 편리성과 접근성은 의료 서비스를 위한 유연한 플랫폼을 제공한다. TMIS는 의료 관련 서비스의 질을 높이기 위해 원격 사용자에게 전자기록을 지원하는 의료정보시스템이다. 환자는 공공 네트워크를 통해서 의료정보서비스를 받을 수 있으므로 개인정보보호는 TMIS에서 매우 중요한 문제이다.

지금까지 TMIS에는 공개키 암호화와 비교하여 더 작은 크기의 키로 동일한 보안을 제공하는 타원곡선 암호시스템을 도입하여 인증과 세션키 동의 스킴이 제안되어 왔다[1]-[3]. TMIS 프로토콜의 대부분은 안전한 세션키 동의 스킴을 설계하는 것이 어려운 학문적 주제이다.

표 1에서와 같이 2013년 Lin[4]과 Xie et al.'s[5]는 Chen et al.'s[6] 스킴이 스마트카드 도난 시 패스워드를 도출할 수 있으며 사용자의 식별이 사전공격으로 취약하다는 것을 증명하고 사전공격 차단과 익명성을 보호하는 개선된 스킴을 제안했으나 입력검증 조건이 누락되어 로그인 및 패스워드 변경단계가 비효율적이다. Xie et al.'s은 Lin 스킴이 입력검증 조건이 포함되지 않아서 로긴 및 패스워드 수정단계의 비효율성으로 귀착되고 서비스거부공격(DoS)에 취약하며 스마트카드 도난 시 패스워드추측공격에 취약하다는 것을 증명했다.

2013년 Xu et al.'s[7]은 동적식별자와 익명성에 안전한 TMIS를 위한 ECC기반의 안전하고 효율적인 인증 및 키동의 스킴을 제안했다. 그러나 Islam et al.'s[8]은 Xu et al.'s 스킴이 인증결여와 재생공격에 취약함을 증명하고 ECC를 기반으로 익명으로 입증된 이중 인증 프로토콜을 제안했다. 그러나 2015년 Chaudhry et al.'s[9]은 Islam et al.'s 스킴이 사용자 가장 및 서버 도용 공격에 취약함을 입증하고 개선된 스킴을 제안했다.

Awasthi et al.'s[10]는 난수와 Xor 연산, 해시 함수를 사용하는 효율적인 TMIS 생체인식 기반 인증스킴을 제시하였으나 반사공격과 사용자의 익명성을 제공하지 못한다는 사실을 밝혀졌다.

2014년 Arshad et al.'s[11]은 서비스 거부(Denial of Service)공격 및 재생공격에 안전한 타원형 곡선 암호화 시스템(ECC)을 기반으로 한 스킴을 제시했다. 최근, Lu et al.'s 스킴[12]은 Arshad et al.'s 스킴의 보안 취약점을 제시하고 타원 곡선 암호화 시스템을 사용하는 생체 인식 기반 인증 방법을 제안했다. 그러나 K. C. Shin[13]의 분석에서 환자(User's)들의 익명성을 보호하지 못하고 합법적인 사용자가 다른 합법적인 사용자 및 서버의 위장공격에 취약함을 보였다.

표 1. 보안특징(속성) 비교
Table 1. Comparison of security features

	Islam et al.'s [8]	Lu et al.'s [12]	Xu et al.'s [7]	Chaudhry et al.'s [9]	Qui et al.'s [14]	Lin [4]	Chen et al.'s [6]	Arshad et al.'s [11]
s1	√	×	√	√	√	√	√	√
s2	×	×	√	×	√	√	×	×
s3	×	×	√	×	√	√	×	×
s4	√	√	×	√	√	√	√	√
s5	×	√	×	×	√	√	√	√
s6	×	×	√	√	√	√	√	√
s7	√	√	√	√	√	√	×	×
s8	-	×	-	×	×	×	×	√

* s1: 익명성, s2: 사용자위장공격, 3: 서버위장공격, s4: 재생공격, s5: 중간자(도청, 수정)공격, s6: 상호인증, s7: 전방향보안, s8: 서비스거부공격

또한 Qui et al.'s[14]는 Chaudhry et al.'s 스킴이 오프라인 패스워드 추측공격과 서버 및 사용자 위장공격, 중간자공격에 취약함을 지적하고 퍼지 검증자(Fuzzy-verifier)를 사용하여 개선된 스킴을 제안했다. 그러나 표 1에서는 표기하지 않았으나 내부자공격과 서비스거부공격에 취약함을 보였다. 표 1에서 보안 속성에 대해 공격을 저지하거나 속성을 만족시키는 요소는 √로 표시하고 그렇지 못한 경우는 x로 표시하였다. 지금까지의 연구에서 공통으로 발견되는 취약성으로는 위장공격, 서비스 거부공격, 사용자익명성, 재생공격, 패스워드추측공격, 도청공격, 내부자공격, 중간자공격 등이다.

본 논문에서는 TMIS 인증스킴의 속성 중 가장 중요한 익명성보호와 사용자와 서버간 강력한 인증설계, 후속통신을 보호하기 위한 안전한 세션키 동의 및 위장공격과 도청공격에 안전한 스킴을 제안한다. 또한 서버의 관여없이 사용자의 간단하고 안전한 패스워드변경과 사용자의 패스워드와 생체정보의 잘못된 입력에 의한 불일치를 신속하게 검출하며 계산비용을 최소화한다.

II. 제안스킴

본장에서는 TMIS를 위한 ECC를 기반으로 향상된 상호 인증스킴을 제안한다. 제안된 스킴은 익명성과 효율적인 인증단계를 설계하는데 중점을 두었고 재생 공격, 위장공격을 회피하기 위해 ECC 생성자인 난수를 사용하기 때문에 사용자와 서버 간 동기화를 위한 타임스탬프를 사용하지 않는다. 새로운 사용자는 서버에 식별자와 비밀파라미터로 등록하고 스마트카드를 획득한다.

Chaudhry et al.'s, Islam et al.'s 스킴의 사용자/서버 위장공격과 중간자공격의 단점을 보완할 뿐만 아니라 상호 인증 및 다양한 공격에 대응할 수 있다. 제안된 스킴은 등록 단계, 인증 및 키 동의 단계, 암호 변경 단계의 세 단계로 구성된다. 제안된 프로토콜의 표기는 표 2에, 등록 및 인증 프로세스는 그림 1에 제시되어있다.

표 2. 약어표기 및 정의
Table 2. Notations used in this paper

Notation	Definition
U, S	User(Patient), Server
ID_i, pw_i, Bio_i	Identifier of User i, password, Biometric
G	Generator of Cyclic group Z_p
x	Private Key of Server
y	Number of secret
p	1024bit prime
⊕, ‖	Exclusive-or Operation, Concatenation

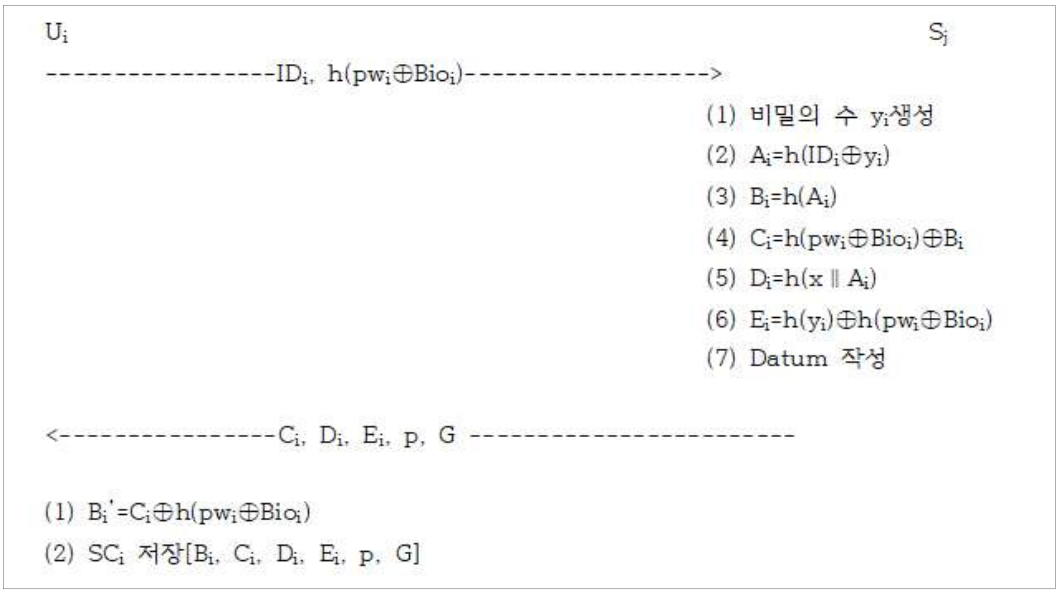

그림 1. 제안 등록단계
Fig. 1. Registration phase of proposed scheme

2.1 등록단계

사용자 i는 ID_i와 $h(pw_i \oplus Bio_i)$를 안전한 채널을 사용하여 서버 S_j의 등록단계를 필요로 한다. 서버는 사용자가 서버와 상호인증 할 수 있는 정보 값을 계산하고 타원곡선 암호를 사용할 수 있는 파라미터를 정보를 사용자에게 보낸다. 절차는 다음과 같다.

(1) 환자 U_i는 패스워드 pw_i, 생체정보 Bio_i를 이용하여 $h(pw_i \oplus Bio_i)$를 계산한다.

(2) U_i는 $h(pw_i \oplus Bio_i)$, 자신의 식별자 ID_i와 함께 안전한 채널을 통해 서버 S_j로 전송한다.

(3) 서버 S_j는 ID_i의 비밀번호 y_i를 생성하여 다음을 계산한다.

. $A_i=h(ID_i \oplus y_i)$

. $B_i=h(A_i)$

. $C_i=h(pw_i \oplus Bio_i) \oplus B_i$

. $D_i=y_i \oplus A_i \oplus h(y_i)$

. $E_i=h(y_i) \oplus h(pw_i \oplus Bio_i)$

(4) 서버 S_j는 스마트카드에 인증파라미터[C_i, D_i, E_i, p, G]를 저장하여 안전한 채널로 사용자 U_i에게 전송한다.

(5) 사용자 U_i는 $B'_i=C_i \oplus h(pw_i \oplus Bio_i)$를 계산하고 스마트카드에 [$B'_i$, C_i, D_i, E_i, p, G]를 저장한다.

(6) 서버 S_j는 판별식별자인 A_i와 로긴메시지 인증시에 추출된 ECC 생성자를 공란으로, 상태비트를 0으로 데이터베이스에 보관한다.

판별식별자	ECC생성자	상태비트
A_i	r'_i	0 or 1
A_j	r'_j	0 or 1
:	:	:

2.2 로긴단계

사용자가 서버에 등록을 완료하면 로긴메시지를 보낼 수 있다. 스마트카드는 사용자의 식별자, 패스워드, 생체정보를 사용하여 즉시 합법성을 검사한다. 절차는 그림 2와 같다.

(1) 사용자는 스마트카드를 리더기에 삽입하고 ID_i, pw_i를 입력한 다음 센서를 사용하여 생체정보 Bio_i를 입력한다.

(2) 스마트카드는 $B_i=C_i \oplus h(pw_i \oplus Bio_i)$를 계산하여 스마트카드의 B_i'와 비교하고 일치 여부를 점검한다. 일치하면 E_i를 사용하여 $h(y_i)$를 추출해 낸다.

(3) 스마트카드는 랜덤넘버 $r_i \in Z^*_p$를 선택하고 $r'_i=r_iG$를 생성하여 다음을 계산한다.

. $M_1=h(B_i) \oplus r'_i \oplus h(y_i)$, $AID_i=h(r'_i) \oplus ID_i \oplus h(y_i)$

. $M_2=h(r'_i \| AID_i \| D_i \| SID_j)$

(4) 스마트카드는 로긴메시지 [M_1, M_2, D_i]를 서버 S_j로 전송한다.

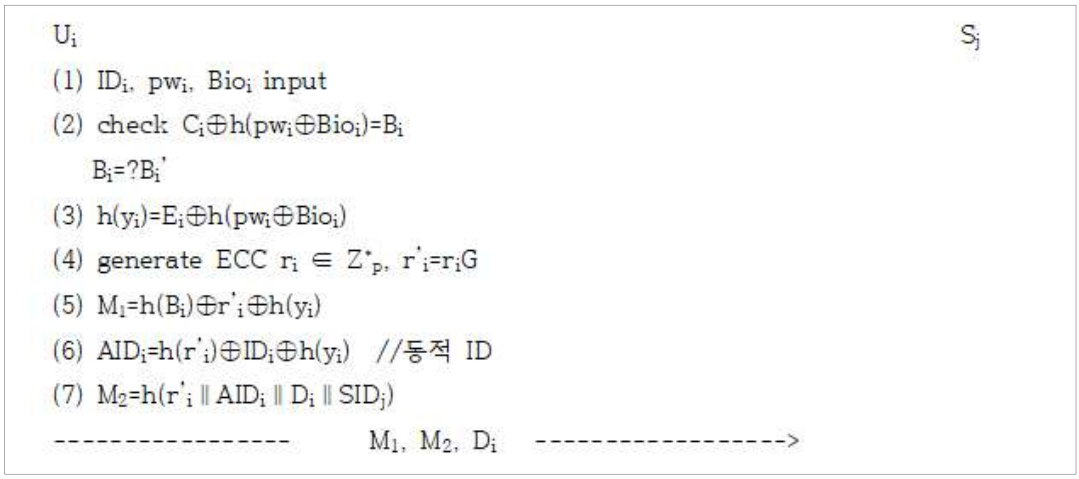

그림 2. 제안 로긴단계

Fig. 2. Login phase proposed scheme

2.3 인증 단계

(1) 그림 3에서와 같이 로긴메시지 [M_1, M_2, D_i]를 수신한 서버 S_j는 비밀키 x와 데이터베이스 리스트에 저장된 datum을 사용하여 $D'_i=h(x \| A_i)$를 계산하고 수신한 D_i와 D'_i의 일치여부를 확인한다. 일치한 D_i는 사용자의 식별자를 포함하므로 ID_i를 검색해 낼 수 있다.

(2) 검색된 ID_i와 로긴메시지 M_1를 이용하여 $r'_i=M_1 \oplus h2(A_i) \oplus h(y_i)$와 $AID_i=h(r'_i) \oplus ID_i \oplus h(y_i)$를 계산한다. 사용자의 ECC생성자($r'_i$)는 데이터베이스에 저장하고 상태비트를 0에서 1로 변환하여 재생공격과 세션유지에 사용한다.

(3) 사용자를 인증하기 위해서 서버는 검색 및 산출한 정보를 이용하여 $M'2=h(r'_i \| AID_i \| D_i \| SID_j)$를 계산하고 수신한 M_2와 비교하여 일치하면 사용자는 인증된다.

(4) 서버는 랜덤넘버 $r_s \in Z^*_p$를 선택하고 $r'_s=r_sG$를 생성하여 세션키 $SK_{ji}=h(ID_i \| r'_i \| r'_s \| SID_j)$와 $M_3=r'_s \oplus h(r'_i) \oplus h(y_i)$, $M_4=h(SID_j \| r'_s \| AID_i)$를 계산한다.

(5) 인증메시지 [M_3, M_4]를 사용자에게 전송한다.

(6) [M_3, M_4]를 수신한 사용자는 $r'_s=M_3 \oplus h(r'_i) \oplus h(y_i)$를 산출하고 합법적 서버인지 비교하기 위해 $M'_4=h(SID_j \| r'_s \| AID_i)$를 계산한다. 계산된 M'_4와 수신한 M_4가 일치하면 사용자는 서버를 인증하고 세션키 $SK_{ji}=h(ID_i \| r'_i \| r'_s \| SID_j)$를 계산한다.

2.4 패스워드 변경단계

그림 4는 합법적인 사용자가 서버의 참여 없이 스마트카드에 의한 패스워드를 변경한다. 카드리더기에 스마트카드를 삽입하고 현재의 패스워드와 식별자를 입력한다. 스마트카드는 식별자가 정확히 입력되면 생체정보를 입력받는다.

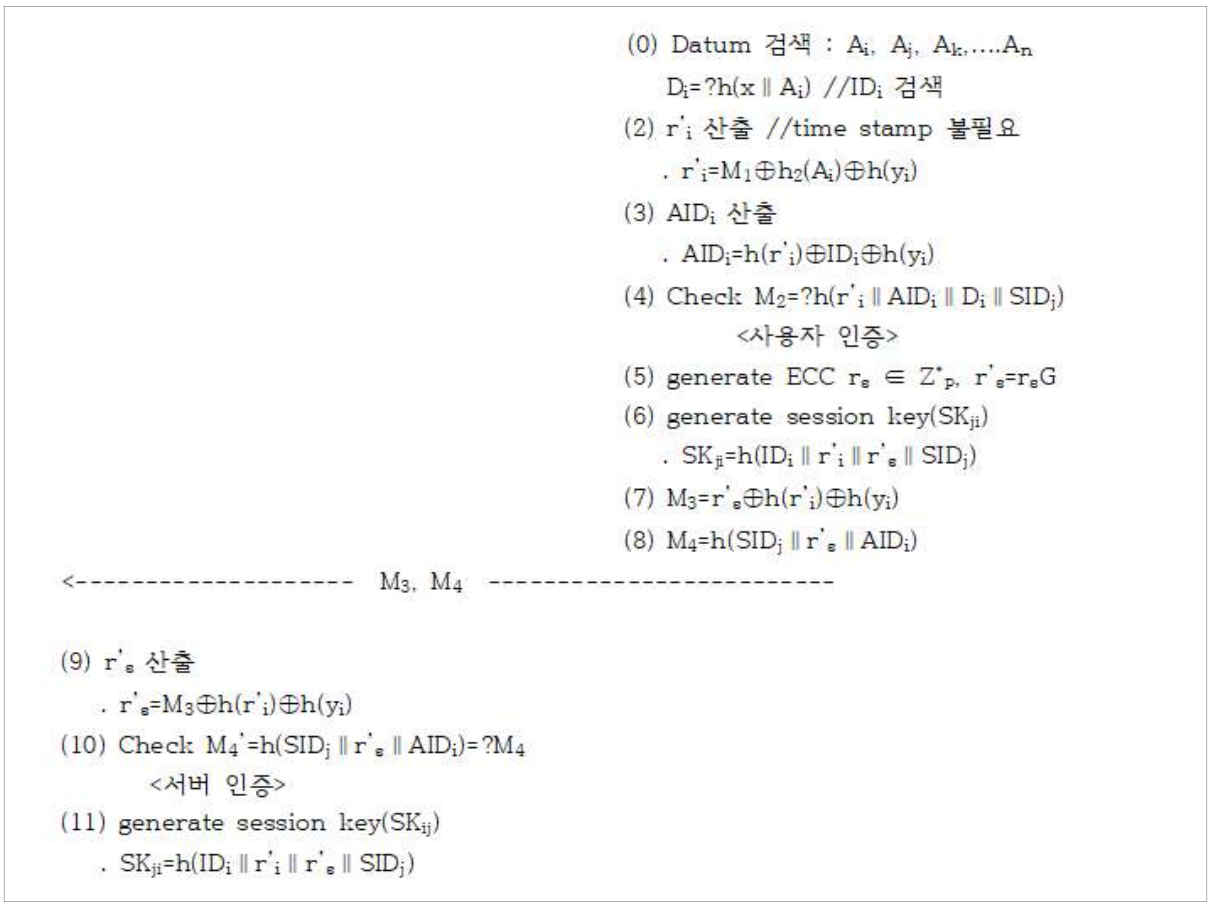

그림 3. 제안 인증 단계
Fig. 3. Authentication phase of proposed scheme

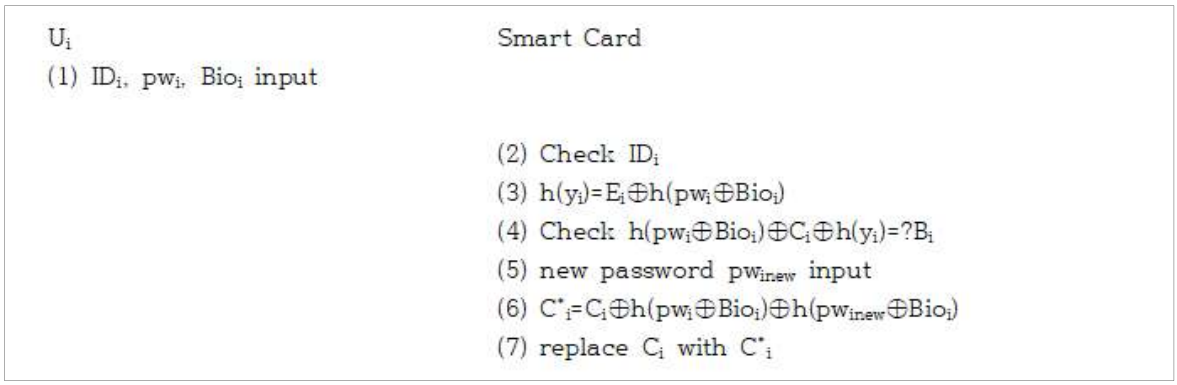

그림 4. 제안 패스워드 변경단계
Fig. 4. Password exchange phase of proposed scheme

스마트카드는 합법적 소유자의 정당성을 체크하면 새로운 패스워드를 요구하여 업데이트하는 단계로 다음과 같다.

(1) 합법적 사용자의 ID_i, pw_i를 입력한다.

(2) 사용자의 식별자 ID_i를 체크하고 생체정보를 입력받아 합법적인 사용자인지 체크한다.

.$h(y_i)=E_i \oplus h(pw_i \oplus Bio_i)$, $h(pw_i \oplus Bio_i) \oplus C_i \oplus h(y_i) = ?B_i$

(3) 새로운 패스워드 pw_{inew}를 입력하고 C^*_i를 계산하여 C_i로 교체한다.

.$C^*_i = C_i \oplus h(pw_i \oplus Bio_i) \oplus h(pw_{inew} \oplus Bio_i)$

III. 제안스킴 분석

익명의 서버 인증 키 동의 스킴은 보안속성과 공격에 대한 저항 및 효율성의 세 가지 중요한 요구사항을 가지므로 이를 사용하여 제안된 스킴을 분석한다. 이 절에서는 제안된 스킴이 요구사항에 어떻게 만족되는지를 설명하고 제안된 스킴을 다른 인증스킴과 비교[표 1, 4, 5]한다.

3.1 보안분석

3.1.1 보안 속성

(1) 익명성(Anonymity) : 제안된 방식에서, 사용자의 실제 신원은 항상 $AID_i=h(r'_i) \oplus ID_i \oplus h(y_i)$를 사용하여 변환되기 때문에 합법적 제3자는 $h(r'_i)$, $h(y_i)$없이 사용자의 실제 신원 ID_i를 계산할 수 없다. 서버가 y_i를 가지고 있으므로 제3자가 [M_1, M_2, D_i]와 [M_3, M_4]를 도청해도 $A_i=h(ID_i \oplus y_i)$, $D_i=y_i \oplus A_i \oplus h(y_i)$의 y_i를 알지 못하므로 식별자를 추출해 낼 수 없다.

따라서 인가 된 서버만이 사용자의 ID_i를 확인한다. 결과적으로, 제3자는 사용자의 실제 신원을 얻을 수 없지만 합법적인 사용자는 서버로부터 익명으로 인증 받을 수 있다.

(2) 상호 인증 : 상호 인증은 두 당사자가 서로를 인증하는 것으로 제안된 기법에서 서버는 비밀키 x를 사용하여 등록단계의 $A_i=h(ID_i \oplus y_i)$를 datum으로 해시화하여 사용자의 식별자를 확인하는 방법으로 r'_i와 AID_i를 계산하여 M_2가 올바른지 체크한다.

. $M_2 = ?h(r'_i \| AID_i \| D_i \| SID_j)$

사용자의 서버에 대한 인증은 M_4를 사용하여 서버가 자신의 동적 ID인 AID_i를 계산할 수 있는지의 여부를 확인하는 체크를 한다.

. $M_4' = h(SID_j \| r'_s \| AID_i) = ?M_4$

제3자가 메시지를 가로채서 합법적인 사용자/서버로 위장하려 해도 정확한 값을 계산할 수 없으므로 사용자/서버에 유효한 응답 메시지를 보낼 수 없다. 이것은 제3자가 비밀 키 x, 비밀번호 y_i 및 랜덤 넘버 r'_i와 r'_s를 알지 못하기 때문이다.

(3) 세션 키 동의 : 제안된 방식에서 사용자와 서버는 인증 단계 후에 세션 키($h(ID_i \| r'_i \| r'_s \| SID_j)$)를 공유한다. r'_i과 r'_s는 매 세션마다 변경되므로 각 세션마다 세션 키가 다르다. 따라서 제3자는 도청된 메시지로부터 세션 키를 계산하는 것은 어렵다.

(4) 완전한 순방향 보안 : 서버의 비밀키 x가 손

상되고 제3자는 ID_i, PW_i, Bio_i, r_i를 획득하였다면 [M_1, M_2, M_3, M_4]를 계산할 수 있다. 그러나 이전의 세션 키 $h(ID_i \| r'_i \| r'_s \| SID_j)$를 계산하기 위해서는 제3자는 r_i와 r_s를 알아야 한다. r'_i로부터 r_i를 계산하거나 r'_s로부터 r_s를 계산하기 위해서는 ECC의 난해함으로 인해 r'_s, r'_i를 계산하는 것이 불가능하다.

제안된 기법은 사용자와 서버 간의 세션 키를 다음과 같이 계산한다.

. $r'_i=M_1 \oplus h_2(A_i) \oplus h(y_i)$

. $r'_s=M_3 \oplus h(r'_i) \oplus h(y_i)$

. $SK_{ji}=h(ID_i \| r'_i \| r'_s \| SID_j)$

공격자는 $h(y_i)$와 y_i를 계산할 수 없기 때문에 r'_i 또는 r'_s를 계산할 수 없으며 그것은 사용자와 서버 사이의 세션 키를 생성 할 수 없다. 따라서 제안된 기법은 완전한 순방향 보안을 달성한다.

3.1.2 기능적 분석

데이터베이스에는 $A_i=h(ID_i \oplus y_i)$와 사용자 로그인이 성공하면 세션 유지동안 인증정보인 사용자의 비밀난수 r'_i가 저장된다. 서버 S_j가 로긴메시지[M_1, M_2, D_i]를 수신하면 $D_i=h(x \| A_i)$ 파라미터와 일치여부로 등록된 합법적인 사용자인 식별자를 구분해야 한다. 합법적인 제3자가 데이터베이스를 해킹하고 사용자 i의 로긴메시지를 도청하였다 해도 서버 S_j의 인증을 통과할 수 없다. 서버는 D_i'에 자신의 비밀키 x를 사용하고 데이터베이스의 A_i과 연접시켜 해시값을 계산, 비교(D_i=?D_i')하므로 합법적인 제3자는 서버의 비밀키 x를 모르고는 검증단계를 통과할 수 없다. 그렇다면 합법적인 제3자가 비교(D_i=?D_i'), 검증단계를 생략하고 위장서버로 행동한다고 해도 사용자의 비밀난수 r'_i를 찾을 수 없다. $A_i=h(ID_i \oplus y_i)$의 y_i값은 모든 사용자마다 다르며 y_i를 알기 위해서는 정당한 사용자의 ID_i와 pw_i를 알아야 한다. 그러므로 데이터베이스가 해킹되어도 안전하다.

(1) 재생 공격 저항 : 제안된 기법은 비밀번호 r_i, r_s 및 양방향 시도응답 메커니즘을 사용하여 재생공격에 안전하다. 제3자가 로그인 요청메시지 [M_1, M_2, D_i]를 재생하면 각 세션에서 사용된 비밀번호 r_i가 재생된 r'_i가 다르므로 검증테스트를 통과하지 못하고 서버 S_j가 세션을 중단시킨다. 또한 제3자는 각 세션마다 r_s가 다르므로 응답메시지 [M_3, M_4]를 재생할 수 없다.

(2) 수정 공격 및 중간자 공격(Man-in-middle Attack) 저항 : 등록을 원하는 모든 사용자에게는 서버가 고유의 비밀의 수(임의난수)를 생성하여 A_i를 계산하므로 하나의 식별자에게만 사용되는 유일한 비밀의 수이다. 합법적 다른 사용자의 y와 다르다. 공격자는 인증 메시지를 가로챌 수 있고 불법적인 인증을 위해 이를 수정하려고 시도 할 수 있다. 제안된 기법은 단방향 해시 함수를 사용하여 인증 정보가 수정되었는지 여부를 확인한다. 제3자는 y_i, $h(y_i)$ 또는 비밀번호를 얻을 수 없으므로 적법한 인증 메시지를 계산할 수 없다. 따라서 서버와 사용자는 인증 메시지가 공격자에 의해 수정되는지 아닌지를 확인할 수 있다. 따라서 제안된 기법은 변경 등 중간자공격에 대해 안전하다.

(3) 오프라인 추측 공격 저항 : 상대방은 SPA[15] 또는 DPA[16]와 같은 측면 채널 공격을 사용하여 스마트카드에 저장된 정보를 추출 할 수 있다. 그래서 제3자는 [B_i, C_i, D_i, E_i, p, G]를 알 수 있지만 $h(y_i)$, y_i, Bio_i는 알려지지 않았기 때문에 사용자의 패스워드를 알아낼 수 없다. 제안된 방식에서 사용자의 패스워드는 단방향 해시 함수($h(pw_i \oplus Bio_i)$)로 보호되어 항상 사용자의 생체인식과 함께 사용된다. 따라서 생체 정보가 높은 엔트로피를 가지기 때문에 사용자의 패스워드를 계산할 수 없다. 또한 어떤 두 사람이 동일한 생체 인식 템플릿을 가질 수 없기 때문에 생체 인식을 파악할 수 없다. 따라서 제안된 기법은 오프라인 추측 공격에 대해서 안전하다.

(4) 사용자 위장공격(User Impersonation Attack Resistance) 저항 : 합법적인 사용자를 위장하기 위해 제3자는 사용자의 ID_i, pw_i를 획득하거나 [M_1, M_2, D_i]를 구성해야 하는데 (3) 오프라인 추측 공격 저항에 따라 Ui의 올바른 식별자와 패스워드, 생체 정보를 추측하는 것이 불가능하다. 그 다음 [M_1,

M_2, D_i]를 구성하기 위해 사용자의 생체정보와 사용자마다 다른 $A_i=h(ID_i \oplus y_i)$, $D_i=y_i \oplus A_i \oplus h(y_i)$이므로 서버의 비밀번호 $h(y_i)$를 모른 채로 [M_1, M_2, D_i]를 복원하는 것은 불가능하다.

(5) DoS 공격 저항 : 서비스거부 공격은 응용서버의 다운, 서비스의 정지, 네트워크의 기능을 마비시키는 등 여러 형태로 나타나는데 로긴 정보를 대량으로 생산, 복제하여 ping of death와 같은 기법을 사용하여 동시에 많은 로그인 사용자들의 공격에 대하여 S_j는 동시에 다수의 사용자들의 접속에 대해 로그인을 승인하여야 한다. 제안스킴에서는 로그인 메시지 [M_1, M_2, D_i]에서 정당한 서버만이 datum을 디코드하여 ID_i를 알아낸 후 데이터베이스에 한 세션(log out까지)동안 만 ECC로 생성된 임의난수를 저장하고 세션이 끝나면 "0"으로 세팅한다. 즉, 한 세션동안 동일한 ID 식별자로 동시에 다량의 메시지를 보낼 때 서버는 세션을 거절한다.

(6) 서버 위장공격(Server Impersonation Attack Tesistance) 저항 : 제3자가 서버로 위장하여 정당한 사용자 U_i를 속일 수 없다. 제3자가 서버로 속이기 위해서 U_i의 등록정보인 A_i를 서버의 비밀키 x로 엔코딩한 것을 보유하거나 정당한 서버의 datum을 검색할 수 있어야 한다. 로긴 메시지 [M_1, M_2, D_i]를 수신하여 정당한 서버의 비밀번호 y_i를 알지 못하고는 ID_i와 r'_i, AID_i를 계산할 수 없으므로 응답메시지 [M_3, M_4]를 생성할 수 없다.

3.2 보안성능 분석

효율성 측정에는 단일 등록, 간단하고 안전한 암호 변경, 빠른 오류 감지 및 낮은 계산 비용이 포함된다. 성능에서, 제안된 기법은 Qui et al.'s의 스킴보다 작게 계산된다. Qui et al.'s의 스킴은 제안된 스킴보다 약간 높은 계산 비용을 갖지만 다양한 공격에 강력하다. 제안된 기법은 계산비용을 줄이면서 Qui et al.'s의 스킴보다 더 강력하여 문제를 해결한다.

Xu et al.'s, Islam et al.'s, Chaudhry et al.'s, Qui et al.'s의 스킴들과 계산상의 복잡성을 비교하기 위해 배타적 논리합 연산과 문자열 연결과 같은 간단한 연산을 무시한다.

표 3과 같이 수행된 실험 결과에 따르면 각각 Tpa, Tpm, Tme 및 Th는 클럭 속도 36MHz의 Philips Hiper-smart 카드에서 100ms, 130ms, 380ms 및 1ms 걸리는 실행 시간을 나타낸다.

클럭 속도 3GHz의 서버 측 펜티엄 IV 프로세서의 경우 이러한 작업은 각각 0.1ms, 1.17ms, 3.16ms, 0.3ms 및 0.01ms가 소요된다.

표 3. 암호연산시간
Table 3. Time of executing cryptographic operations[17]

	Tpa	Tpm	Tme	Th
server	0.1ms	1.17ms	3.16ms	0.01ms
User/Client	100ms	130ms	380ms	1ms

• Tpa : 타원 곡선 연산 실행시간, • Tpm : 포인트 곱셈 연산 실행시간, • Tme : 지수 연산 실행시간, • Th : 해시함수연산 실행시간.

표 4. 계산복잡도 비교
Table 4. Comparison of computation complexity

	Xu et al.'s[7]	Islam et al.'s[8]	Chaudhry et al.'s[9]	Qui et al.'s[14]	Lu et al.'s [12]	Proposed scheme
User	6Th+3Tpm	6Th+3Tpm+1Tpa	5Th+4Tpm+1Tpa	8Th+2Tpm	8Th+1Tpm+1Tpa	6Th+1Tpm+1Tpa
Server	5Th+3Tpm	4Th+3Tpm	4Th+3Tpm+1Tpa	5Th+2Tpm	4Th+1Tpm+2Tpa	6Th+1Tpm+1Tpa
Complexity	≈399.56ms	≈499.55ms	≈628.85ms	≈270.4	≈239.31	≈237.33

표 5. 제안스킴의 보안속성
Table 5. Security features of proposed scheme

s1	s2	s3	s4	s5	s6	s7	s8
√	√	√	√	√	√	√	√

제안 프로토콜은 [7]-[14]보다 성능이 좋으며 계산비용은 237.33ms에 불과하다. 따라서 효율성 측면에서 제안된 프로토콜이 가장 우수한 성능을 발휘한다. 표 5에서는 각 스킴들의 보안 요소가 부족하고 제안된 스킴보다 보안 문제가 더 많다는 것을 알 수 있다.

Chaudhry et al.'s의 스킴은 Islam et al.'s 스킴의 중간자공격을 개선하여 제안했으나 그들의 스킴 또한 서버와 사용자 위장공격 및 중간자공격에 취약할뿐만 아니라 오프라인 신원 추측 공격에 취약하다는 점을 지적한다. 제안된 프로토콜에서 오프라인 정체성 추측 공격에 저항하기 위해 퍼지 검증 자(fuzzy-verifiers)[18] 기법을 사용한다.

표 1의 보안문제를 보완할 뿐만 아니라 표 4, 5와 같은 모든 장점을 유지한다. 제안된 스킴은 안전성 측면에서 뛰어나고 대응 방안에 비해 많은 우수한 기능을 가지고 있다.

Ⅳ. 결 론

TMIS는 PC나 스마트 폰의 기능을 사용해 건강상태를 모니터링하며 이러한 결과는 의사에게 전달되고 의사가 후속조치를 함으로써 시간과 비용을 절약하고 환자에게 높은 독립성과 적극참여를 유도할 수 있는 장점을 갖는다. 원활한 TMIS를 실현하기 위해서는 개인정보보호를 위한 상호인증과 익명성 보장이 중요하다. 그동안 TMIS의 이전의 스킴 표 1에서 살펴본 바와 같이 제3자의 다양한 공격에 취약함을 드러냈다. 본 논문은 이러한 취약점을 보완하기 위해 해시함수와 ECC난수, 생체정보를 사용하여 동적 ID(AIDi) 기반의 상호인증과 키교환 스킴을 제안했다. 또한 제3자의 로긴 메시지 도청이 이루어져도 해독이 불가능하도록 서버의 비밀키 x와 각 사용자에게 비밀의 수 y_n을 사용하여 합법적인 사용자가 아니라면 정당한 로그인 메시지를 생성할 수 없도록 설계되었다. TMIS의 기본적인 요구조건인 익명성을 보장하고 강력한 상호인증으로 위장공격 등 다양한 공격에 보안성을 충족하는 메커니즘으로 저비용계산의 안전한 스킴이다.

References

[1] E. J. Yoon and K. Y. Yoo, "Cryptanalysis of DS-SIP authentication scheme using ECDH", in Proc. Int. Conf. New Trends Inf. Service Sci., pp. 642-647, July. 2009.

[2] T. H. Chen, H. L. Yeh, P. C. Liu, H. C. Hsiang, and W. K. Shih, "A secured authentication protocol for SIP using elliptic curves cryptography", in Proc. FGIT-FGCN, Vol. 1. pp. 46-55. Dec. 2010.

[3] M. S. Farash and M. A. Attari, "An Enhanced authenticated key agreement for session initiation protocol", Inf. Technol. Control, Vol. 42, No. 4, pp. 333-342, Oct. 2014.

[4] Lin, H. Y, "On the security of a dynamic id-based authentication scheme for telecare medical information systems", J. Med. Syst. Vol. 37, No. 2, pp. 1-5, April. 2013.

[5] Q. Xie, J. Zhang, and N. Dong, "Robust anonymous authentication scheme for telecare medical information systems", J. Med. Syst. Vol. 37, No. 2, pp. 1-8, Jan. 2013.

[6] H. M. Chen, J. W Lo, and C. K. Yeh, "An efficient and secure dynamic id-based authentication scheme for telecare medical information systems", J. Med. Syst. Vol. 36, No. 6, pp. 3907-3915, June. 2012.

[7] X. Xu, P. Zhu, Q. Wen, Z. Jin, H. Zhang, and L. He, "A secure and efficient authentication and key agreement scheme based on ECC for Telecare medicine information systems", J. Med. Syst., Vol. 38, No. 1, pp. 1-17, Nov. 2013.

[8] S. Islam and M. Khan, "Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems" J. Med. Syst., Vol. 38, No. 10, pp. 1-13, Sep. 2014.

[9] S. A. Chaudhry, H. Naqvi, T. Shon, M. Sher, and M. S. Farash, "Cryptanalysis and

improvement of an improved two factor authentication protocol for telecare medical information systems", J. Med. Syst., Vol. 39, No. 6, pp. 1-11, Apr. 2015.

[10] A. K. Das and A. Goswami, "An enhanced biometric authentication scheme for telecare medicine information systems with nonce Using Chaotic Hash Function", Journal of Medical Systems, Vol. 37, No. 12, pp. 9964-9976, June. 2014.

[11] Arshad. H, and Nikooghadam. M., "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems", J. Med. Syst. Vol. 38, No. 12, pp. 1-12, Oct. 2014.

[12] Y. Lu, L. Li, H. Peng, and Y. Yang, "An enhanced biometric-based authentication scheme for telecare medicine information system using elliptic curve cryptosystem", Journal of Medical Systems, Vol. 39, No. 32, pp. 1-9, Feb. 2015.

[13] K. C. Shin, "Cryptanalysis of Biometric-based to Remote User Authentication Scheme", Journal of KIIT, Vol. 17, No. 2, pp. 133-141, Feb. 2019.

[14] Shuming Qiu, Guoai Xu, Haseeb Ahmad, and Licheng Wang, "A Robust Mutual Authentication Scheme Based on Elliptic Curve Cryptography for Telecare Medical Information Systems", IEEE Access, Vol. 6, pp. 7452-7463, Mar. 2018.

[15] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis", in Advances in Cryptology RYPTO, Lecture Notes in Computer Science, Springer, Berlin, Germany, pp. 388-397, Dec. 1999.

[16] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks", IEEE Transactions on Computers, Vol. 51, No. 5, pp. 541-552, May. 2002.

[17] D. He, "An efficient remote user authentication and key agreement protocol for mobile client-server environment from pairings", Ad Hoc Netw., Vol.10, No. 6, pp. 1009-1016, Aug. 2012.

[18] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound", IEEE Trans. Depend. Sec. Comput., to be published. [Online]. Available: https://doi.org/10.1109/TDSC.2016.2605087, doi: 10.1109/TDSC.2016. 2605087.

저자소개

신 광 철(Kwang-Cheul Shin)

1985년 : 서울과학기술대학교 (공학사)
1990년 : 국방대학원(공학석사)
2003년 : 성균관대학교(공학박사)
2004년 3월 ~ 현재 : 성결대학교 산업경영공학부 부교수
관심분야 : 네트워크보안, 정보보호론