JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 30 No. 3, pp. 83-93, March 2025
https://doi.org/10.9708/jksci.2025.30.03.083

Vulnerability Analysis and Enhancement 'Improved of ECC-based Three-Factor Multiserver Authentication Scheme'

Mi-Og Park*

*Professor, Dept. of Computer Engineering, Sungkyul University, Anyang, Korea

[Abstract]

Due to the rapid increase of Internet users, a lot of authentication schemes in multi-server environments have been proposed, and in this paper, we analyze the authentication scheme for multi-server environments proposed by Wu et al. in 2021 and propose a new authentication scheme that improves it. The Wu authentication scheme analyzed in this paper has problems such as the lack of user anonymity and un-traceability due to smart-card theft attack, and such as failure to establish the same session key due to design issue, identifier duplication, and user-unfriendly password change. The improved authentication scheme proposed in this paper is analyzed to ensure secure user anonymity, and is safe for various attacks such as smart-card theft attack, offline password guessing attack, and user impersonation attack, privileged insider attack, perfect forward security and so on. In addition, the proposed authentication scheme shows relatively efficient results in terms of computational complexity and communication cost, so it can be said to be an authentication scheme suitable for a multi-server environment.

▸ **Key words**: Smart-card theft attack, User anonymity, Multiserver, Authentication, ECC

[요 약]

인터넷 사용자의 급속한 증가로 인하여 멀티서버 환경의 여러 인증 스킴들이 제안되고 있으며, 본 논문에서는 2021년에 Wu 등이 제안한 멀티서버 환경을 위한 인증 스킴에 대한 분석과 이를 개선한 새로운 인증 스킴을 제안한다. 본 논문에서 분석한 Wu 인증 스킴은 스마트카드 분실 공격으로 인한 사용자 익명성과 추적불가능성의 부족, 그리고 설계문제로 인한 동일한 세션키 설정 실패, 식별자 중복성, 그리고 사용자 비친화적인 패스워드 변경 등의 문제가 있다. 본 논문에서 제안한 개선된 인증 스킴은 안전한 사용자 익명성을 보장하고, 스마트카드 도난 공격, 오프라인 패스워드 추측 공격, 사용자 가장 공격, 특권을 가진 내부자 공격, 전방향 안전성 등 여러 공격에 안전한 것으로 분석되었다. 또한 제안 인증스킴은 계산 복잡도와 통신 비용면에서도 상대적으로 효율적인 결과를 나타내어, 멀티서버 환경에 적합한 인증 스킴이라고 할 수 있다.

▸ **주제어**: 스마트카드 도난 공격, 사용자 익명성, 멀티서버, 인증, ECC

• First Author: Mi-Og Park, Corresponding Author: Mi-Og Park
*Mi-Og Park (mopark777@daum.net), Dept. of Computer Engineering, Sungkyul University
• Received: 2025. 01. 31, Revised: 2025. 03. 02, Accepted: 2025. 03. 20.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

IT 기술은 현재 클라우드 컴퓨팅, IoT, 엣지(edge) 컴퓨팅 등으로 발전하고 있으며, 이러한 발전은 더 많은 서버를 필요로 한다. 이러한 변화를 반영하듯 멀티서버(multi-server) 환경을 위한 많은 인증 스킴들이 제안되고 있으며, 2018년에 Ali 등이 제안한 멀티서버 인증 스킴[1]은 Li 인증 스킴[2]이 패스워드 추측 공격(password guessing attack), 사용자 가장 공격(user impersonation attack), 내부자 공격(privileged insider attack), 스마트카드 도난 공격(smart-card theft attack)에 안전하지 않고, 사용자 익명성(user anonymity)을 제공하지 못한다고 지적하였다. 이와 같이 멀티서버 환경의 인증 스킴들도 싱글 서버 환경의 인증 스킴들과 마찬가지로 다양한 공격에 안전해야 한다. 또한 여러 사이트에서 동일한 식별자(ID)를 자주 사용하는 사용자들때문에 사용자 익명성이나 추적 불가능성 등의 기능을 멀티서버 환경에서도 제공해야 한다.

2015년에 제안된 Li 인증 스킴은 Pippal 인증 스킴[3]을 개선한 멀티서버 인증 스킴으로, Pippal 인증 스킴의 사용자 가장 공격, 내부자 공격, 인증 단계의 잘못된 설계, 새로운 서버의 확장 불가의 문제가 있다고 지적하였다. 이 두 인증 스킴은 모듈러 지수 연산을 이용한 2-factor 인증 스킴이고, Li 인증 스킴을 개선한 Ali 인증 스킴은 ECC(elliptic curve cryptography)와 비밀키 암호를 이용한 3-factor 인증 스킴으로, 자신들의 인증 스킴은 여러 공격에 안전하고 상호 인증과 안전한 세션 키를 보장한다고 주장하였다.

그러나 2019년 Wang 인증 스킴[4]은 Ali 인증 스킴이 사용자 가장 공격, 서버 가장 공격, 내부자 공격, 서비스 거부 공격, 그리고 전방향 안전성 공격에 안전하지 않다고 지적하면서, ECC와 비밀키 암호방식을 이용한 3-factor 인증 스킴을 제안하였다. Wang 인증 스킴은 자신들의 인증 스킴이 여러 공격에 안전하고, 성능과 안전성 비교에서도 관련 인증 스킴들보다 우수하다고 주장하였다. 그러나 2021년 Wu 인증 스킴[5]은 Wang 인증 스킴이 사용자 가장 공격, 서버 가장 공격, 임시 비밀 누출 공격(ephemeral secret leakage attack)에 안전하지 않다고 지적하면서, 이 문제를 개선하기 위하여 ECC와 비밀키 암호방식을 이용한 3-factor 멀티서버 인증 스킴을 제안하였고, 그들이 제시한 안전성과 성능 비교가 자신들의 인증 스킴에 대한 안전성과 효율성을 증명한다고 주장하였다.

2022년 Tanveer 인증 스킴[6]은 원격의료정보시스템(Telecare Medical Information System)을 위한 인증 스킴을 제안하면서, Ali 인증 스킴이 사용자 가장 공격, 내부자 공격, 서버 가장 공격에 안전하지 않고, 사용자 익명성을 제공하지 못한다고 지적하였다. 또한, Tanveer 인증 스킴은 Ali 인증 스킴의 안전성 분석 외에도 Wang 인증 스킴의 사용자 가장 공격, 서버 가장 공격, 임시 비밀 누출 공격에 대한 문제점을 지적하였다. Wu 인증 스킴의 문제점은 2022년 Mirsaraei 인증 스킴[7]의 비교실험에서도 제시하고 있으며, 2024년에 Jha 인증 스킴[8]도 Mirsaraei 인증 스킴이 지적한 Wu 인증 스킴의 문제점들 즉, 데이터 무결성과 데이터 비밀성, 그리고 안전한 패스워드 업데이트(secured password updating) 문제를 간단히 언급하였다. Mirsaraei 인증 스킴에서 언급한 안전한 패스워드 업데이트란 사용자의 패스워드 업데이트 시에 서버의 도움을 받아야 하는 문제를 지적한 것으로, Wu 인증 스킴은 패스

Table 1. The Summary of Authentication Schemes

Reference	Year	Features	Vulnerabilities
Ali[1]	2018	-Utilized ECC -Three-factor scheme -Based on data encryption scheme	-Does not resist impersonation attack, privileged insider attack, perfect forward secrecy, user anonymity, ephemeral secret leakage attack
Wang[4]	2019	-Utilized ECC -Three-factor scheme -Based on data encryption scheme	-Does not resist impersonation attack, ephemeral secret leakage attack, user anonymity, user untraceability
Wu[5]	2021	-Utilized ECC -Three-factor scheme -Based on data encryption scheme	-Does not resist smart card theft attack, user anonymity, user untraceability
Tanveer [6]	2022	-Telecare Medical Information System -Utilized ECC and chaotic map -Three-factor scheme	-Does not resist privileged insider attack, smart card theft attack, offline password guessing attack, ephemeral secret leakage attack, perfect forward secrecy, impersonation attack
Mirsaraei [7]	2022	-Three-factor scheme -Utilized ECC -Three-factor scheme	-Does not resist smart card theft attack, user impersonation attack, perfect forward secrecy, user anonymity, user untraceability

워드 업데이트 단계는 제시하지 않았다. 2023년에 Li 인증 스킴[9]도 Mirsaraei 인증 스킴이 전방향 안전성과 추적 불가능성을 제공하지 못한다고 지적하였다.

2023년에 Salem 인증 스킴[10]은 Wu 인증 스킴과 Wang 인증 스킴 모두 등록 센터에서 높은 계산량의 오버헤드를 가진다고 간단히 지적하였다. 본 논문에서 Wu 인증 스킴을 분석한 결과, 이 인증 스킴은 그들의 주장과 달리 평문으로 저장한 난수로 인하여 스마트카드 도난 공격에 의한 사용자 익명성을 보장하지 못한다. 또한, 매 세션마다 동일한 동적 ID를 사용하여 사용자 추적 불가능성도 보장하지 못한다. 본 논문에서는 이러한 Wu 인증 스킴의 문제를 해결하기 위하여 개선된 사용자 익명성 제공 인증 스킴을 제안한다.

본 논문은 2장과 3장에서 Wu 인증 스킴의 각 단계를 리뷰하고, 그에 대한 문제들을 분석한다. 4장에서는 문제 해결을 위한 개선된 인증 스킴을 제안하고, 그에 대한 안전성 분석과 계산 복잡도, 통신 비용 등을 5장에서 제시한다. 마지막으로 6장은 결론을 내리고 본 고를 마친다.

II. Review of Wu et al.'s Scheme

Wu 인증 스킴의 등록 단계, 로그인 단계, 그리고 인증 단계는 다음과 같으며, 패스워드 변경 단계는 제시하지 않았다. 본 논문에서 사용하는 기호들은 다음과 같다.

P_{pub}: RC(registration center)의 공개키
x : 서버 s의 비밀키(secret key)
ID_i : i번째 사용자의 식별자(identity)
PW_i : i번째 사용자의 패스워드(password)
b_i : i번째 사용자의 생체정보
$E_{key}()/D_{key}()$: 비밀키 암호방식의 암、복호화
$h()$: 단방향 해시함수(one-way hash function)
$H()$: 바이오 해시함수(Bio-hash function)
$\oplus$: XOR 연산
$\|$: 연접(concatenation) 연산

1. Registration phase

사용자와 서버는 다음과 같은 과정을 진행하여 등록 센터에 등록한다.

1.서버 $server_j$는 자신의 ID인 SID_j를 선택하여 등록 센터 RC에 안전하게 전송한다.
2.메시지를 받은 RC는 난수 e_j를 선택하여 $SM_j = H(SID_j \| x \| e_j)$를 계산하고 $\{SID_j, e_j\}$를 저장한 후 서버 $server_j$에 SM_j를 전송한다.
3.메시지를 받은 서버 $server_j$는 데이터베이스에 SM_j를 저장한다.
4.사용자는 자신의 ID_i와 패스워드 PW_i을 선택하고, 자신의 생체정보 b_i를 입력한다.
5.사용자는 난수 r_i를 선택하여 $P_i = h(PW_i \| H(b_i) \| r_i)$와 $DID_i = h(ID_i \oplus r_i)$을 계산한 후 $\{DID_i, ID_i, P_i\}$를 RC에 전송한다.
6.메시지를 받은 RC는 난수 d_i를 선택하여 다음 값들을 계산한다.

$$A_i = h(x \| DID_i \| ID_i \| d_i)$$
$$B_i = A_i \oplus P_i$$
$$V_i = h(P_i \oplus h(DID_i)) \bmod n$$

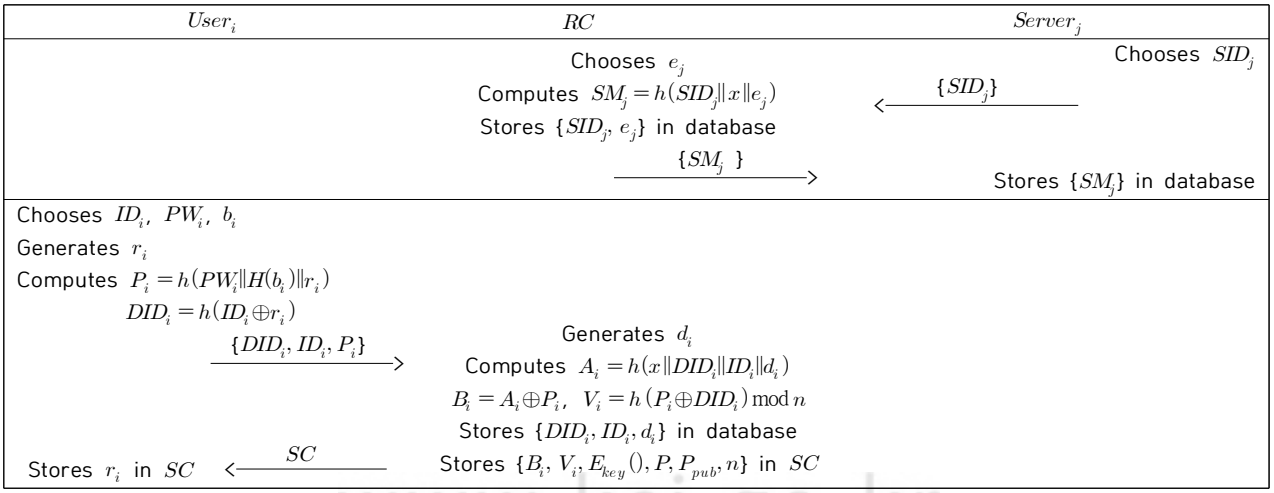

Fig. 1. Wu et al.'s Registration Phase

여기서 n은 $2^4 \le n \le 2^8$이며, RC는 $\{DID_i,\ ID_i,\ d_i\}$를 데이터베이스에 저장하고, $\{B_i, V_i, E_{key}(), P, n\ P_{pub}\}$는 스마트카드 SC에 저장하여 사용자에게 안전하게 보낸다.

7.사용자는 난수 r_i를 SC에 저장하고 등록 단계를 마친다.

2. Login and authentication phase

1.사용자 $user_i$가 자신의 ID_i와 PW_i, 그리고 b_i을 입력하여 스마트카드 SC에 로그인하면 SC는 다음을 계산한다.

$$P_i' = h(PW_i \| H(b_i) \| r_i)$$
$$DID_i' = h(ID_i \oplus r_i)$$
$$V_i' = h(P_i' \oplus h(DID_i')) \bmod n$$

만약 V_i'과 V_i가 동일하면 난수 N_1을 생성하여 다음 값들을 계산한 후, $M_1 = \{D_i, DID_i', L_i\}$을 RC에 전송한다.

$$A_i' = B_i \oplus P_i'$$
$$D_i = h(A_i' \oplus DID_i') \oplus N_1$$
$$G_i = h(N_1 \oplus A_i' \oplus DID_i')$$
$$R_i = G_i P$$
$$C_i = h(G_i P_{pub})$$
$$L_i' = E_{c_i}(DID_i' \| A_i' \| SID_j)$$

2.등록 센터 RC는 데이터베이스에서 $\{DID_i', ID_i\}$를 검색하여 다음 값들을 계산한다.

$User_i$	RC	$Server_j$
Inputs $ID_i,\ PW_i,\ b_i$		
Computes $P_i' = h(PW_i \| H(b_i) \| r_i)$		
$DID_i' = h(ID_i \oplus r_i)$		
$V_i' = h(P_i' \oplus h(DID_i')) \bmod n$		
Compares $V_i' ? = V_i$		
Chooses N_1		
Computes $A_i' = B_i \oplus P_i'$		
$D_i = h(A_i' \oplus DID_i') \oplus N_1$		
$G_i = h(N_1 \oplus A_i' \oplus DID_i')$		
$R_i = G_i P,\ C_i = h(G_i P_{pub})$		
$L_i' = E_{c_i}(DID_i' \| A_i' \| SID_j)$		
$M_1 = \{D_i, DID_i', L_i\}$ ---------->	Retrieves $\{DID_i', ID_i\}$	
	Computes $A_i'' = h(x \| DID_i' \| ID_i \| d_i)$	
	$N_1' = D_i \oplus h(A_i'' \oplus DID_i')$	
	$G_i' = h(N_1' \oplus A_i'' \oplus DID_i')$	
	$R_i' = G_i' P,\ C_i' = h(x R_i')$	
	$(DID_i' \| A_i' \| SID_j) = D'_{c_i}(L_i)$	
	Compares $A_i' ? = A_i''$	
	Computes $SM_j = h(SID_j \| x \| e_j)$	
	$Y_i = h(SID_j \| SM_j)$	
	$M_i = E_{SM_j}(DID_i' \| R_i' \| Y_i \| h(A_i' \| C_i'))$	
	$M_2 = \{M_i\}$ ---------->	Computes $(DID_i' \| R_i' \| Y_i \| h(A_i' \| C_i')) = D_{SM_j}(M_i)$
		$Y_i' = h(SID_j \| SM_j)$
		Compares $Y_i' ? = Y_i$
		Chooses N_2
		Computes $R_s = N_2 P,\ E_i = N_2 R_i'$
		$SK_j = h(E_i \| h(A_i' \| C_i'))$
		$F_i = h(DID_i' \| SK_j \| R_s \| SID_j)$
	$M_3 = \{R_s, F_i\}$ <----------	
Computes $E_i' = N_1 R_s$		
$SK_i = h(E_i' \| h(A_i' \| C_i))$		
$F_i' = h(DID_i' \| SK_i \| R_s \| SID_j)$		
Compares $F_i' ? = F_i$		

Fig. 2. Wu et al.'s Login and Authentication Phase

$$A_i'' = h(x \| DID_i' \| ID_i)$$
$$N_1' = D_1 \oplus h(A_i'' \oplus DID_i')$$
$$G_i' = h(N_1' \oplus A_i'' \oplus DID_i')$$
$$R_i' = G_i' P,\ C_i' = h(xR_i')$$
$$(DID_i' \| A_i' \| SID_j) = D'_{c_i}(L_i)$$

만약 A_i''과 A_i'이 동일하면 $SM_j = h(SID_j \| x \| e_j)$, $Y_i = h(SID_j \| SM_j)$, $M_i = E_{SM_j}(DID_i' \| R_i' \| Y_i \| h(A_i' \| C_i'))$을 계산하고 $M_2 = \{M_i\}$를 서버에게 전송한다.

3.서버 $server_j$는 M_i를 복호화하여 $Y_i' = h(SID_j \| SM_j)$를 계산한 후 Y_i'과 Y_i가 동일한지 비교한다. 만약, 두 값이 동일하면 서버는 난수 N_2를 생성하여 다음을 계산한 후 $M_3 = \{R_s, F_i\}$를 사용자에게 전송한다.

$$R_s = N_2 P,\ E_i = N_2 R_i'$$
$$SK_j = h(E_i \| h(A_i' \| C_i'))$$
$$F_i = h(DID_i' \| SK_j \| R_s \| SID_j)$$

4.메시지 M_3을 받은 $user_i$는 다음을 계산하여 F_i'과 F_i가 동일하면 서버를 인증하고 SK_i를 세션키로 사용한다.

$$E_i' = N_1 R_s$$
$$SK_i = h(E_i' \| h(A_i' \| C_i))$$
$$F_i' = h(DID_i' \| SK_j \| R_s \| SID_j)$$

III. Vulnerability of Wu et al.'s Scheme

본 장에서는 Wu 인증 스킴에 대한 본 논문의 분석결과 제시로, 분석결과는 안전성 문제와 설계상의 문제 순으로 서술한다.

1. Security Vulnerability

Smart-card theft attack

Wu 인증 스킴은 DID_i로 사용자 익명성을 개선하였다고 주장하였으나, 공격자가 스마트카드 SC를 획득할 경우 난수 r_i를 기존의 wang 인증 스킴과 동일하게 SC에 평문으로 저장하기 때문에, 전송 메시지 DID_i를 $ID_i' = DID_i \oplus r_i$와 같이 계산하여 사용자의 ID_i를 쉽게 계산할 수 있다. 그러므로 Wu 인증 스킴의 사용자 익명성은 안전하지 않다.

User untraceability attack

Wu 인증 스킴은 스마트카드 SC의 난수 r_i를 매번 변경하지 않기 때문에 매 세션마다 항상 동일한 DID_i를 사용한다. 그러므로 공격자가 사용자의 정확한 ID_i를 모른다 할지라도 항상 동일한 DID_i를 사용하는 동일한 사용자라는 것을 알 수 있다. 그러므로 이 인증 스킴은 안전한 추적 불가능성을 보장하지 못한다.

Mutual authentication

Wu 인증 스킴의 사용자 E_i'과 서버의 E_i 계산은 $E_i' = N_1 R_s$와 $E_i = N_2 R_i'$으로 이 두 수식의 계산 값이 일치하지 않는다. 이러한 문제는 사용자와 서버 간의 상호 인증에 실패하고 동일한 세션키를 생성할 수 없다.

2. Design Vulnerability

Unconfirmed Identity format

등록 단계의 RC는 사용자가 제출한 ID_i나 DID_i의 타당성 확인 없이, 사용자가 제출한 자료를 가지고 곧바로 등록 과정을 진행한다. 그러므로 이 인증 스킴은 사용자의 중복성 문제를 해결할 수 없어 안전한 인증 스킴이라고 할 수 없다.

User-unfriendly password change phase

Wu 인증 스킴은 패스워드 변경단계를 미제시하였고, 본 논문에서 분석한 결과 사용자가 패스워드를 변경하려면 사용자와 RC와의 DID_i 값의 일치성 때문에 등록 센터 RC와의 통신이 필요하다. 그러므로 이 인증 스킴은 사용자 친화적인 패스워드 변경단계가 아니다.

IV. Improved Authentication Scheme

본 장에서는 Wu 인증 스킴의 문제를 해결한 개선된 사용자 익명성 제공 인증 스킴을 제안한다.

4.1 Registration phase

제안 인증 스킴의 등록 단계는 Fig. 3과 같이, 기존의 등록 단계와 거의 동일하며, 다른 점은 등록 단계에서 서버 $server_j$의 식별자 SID_j와 사용자 ID_i의 타당성을 검증하는 것이다. 그리고 등록 단계의 마지막 과정에서 난수 r_i를 $R_i = h(ID_i \oplus H(b_i)) \oplus r_i$로 계산하여 스마트카드에 안전하게 저장한다.

4.2 Login and authentication phase

1.사용자 $user_i$가 자신의 ID_i, PW_i, 생체정보 b_i을 입력하면 스마트카드 SC는 $F_i = H(b_i)$를 계산한 후, 저장된 R_i와 V_i를 사용하여 다음을 진행한다.

$$r_i' = h(ID_i \oplus F_i) \oplus R_i$$
$$P_i' = h(PW_i \| F_i \| r_i')$$
$$V_i' = h(P_i' \oplus ID_i') \bmod n$$
$$DID_i' = h(ID_i \oplus r_i')$$

계산한 V_i'과 V_i가 동일하면 SC는 난수 N_1과 새로운 난수 r_i^n을 생성하여 다음 값들을 계산한 후, $M_1 = \{DID_i', D_i, L_i\}$을 등록 센터 RC에 전송한다.

$$A_i' = B_i \oplus P_i'$$
$$DID_i^n = h(ID_i \oplus r_i^n)$$
$$R_i^n = h(ID_i \oplus F_i) \oplus r_i^n$$
$$D_i = h(ID_i \oplus N_1 \oplus DID_i' \oplus A_i' \oplus SID_j \oplus DID_i^n)$$
$$L_i' = E_{A_i}(ID_i \| N_1 \| DID_i' \| A_i' \| SID_j \| DID_i^n)$$

2.등록 센터 RC는 데이터베이스에서 $\{DID_i', ID_i\}$를 검색하여 다음 값들을 계산한다.

$$A_i'' = h(x \| DID_i' \| ID_i \| d_i)$$
$$N_1' = D_i \oplus h(A_i'' \oplus DID_i')$$
$$D_{A_i}(L_i) = (ID_i \| N_1 \| DID_i' \| A_i' \| SID_j \| DID_i^n)$$
$$D_i' = h(ID_i \oplus N_1 \oplus DID_i' \oplus A_i' \oplus SID_j \oplus DID_i^n)$$

만약 A_i''과 A_i', D_i'과 D_i의 각각의 값이 동일하지 않으면 세션을 종료하고, 그렇지 않을 경우, RC는 기존의 DID_i'를 DID_i^n으로 업데이트한 후, 다음을 계산하여 $M_2 = \{M_i\}$를 서버에 전송한다.

$$A_i^n = h(x \| DID_i^n \| ID_i \| d_i)$$
$$T_i = h(N_1' \oplus h(A_i'')) \oplus A_i^n$$
$$SM_j = h(SID_j \| x \| e_j)$$
$$Y_i = h(SID_j \| SM_j)$$
$$M_i = E_{SM_j}(N_1' \| DID_i' \| T_i \| Y_i \| h(A_i'' \oplus ID_i))$$

3.서버 $server_j$는 메시지 M_i를 복호화($D_{SM_j}(M_i)$)한 후 $Y_i' = h(SID_j \| SM_j)$를 계산하여 Y_i'과 Y_i가 동일한 지 비교한다. 만약, 두 값이 동일하면 서버는 난수 N_2를 생성하여 다음 값들을 계산한 후, $M_3 = \{R_s, Z_i, C_i\}$를 사용자에게 전송한다.

$$Y_i' = h(SID_j \| SM_j)$$
$$R_s = N_2 P$$
$$E_i = N_1' R_s$$
$$Z_i = E_i \oplus T_i$$
$$SK_j = h(N_1' \| E_i \| h(A_i'' \oplus ID_i))$$
$$C_i = h(DID_i' \| SK_j \| R_s \| Z_i \| SID_j)$$

4.메시지 M_3을 받은 $user_i$는 다음을 계산하여 C_i'과 C_i가 동일하면 서버를 인증하고 다음 계산을 진행하여 새로운 값들, B_i^n와 V_i^n을 업데이트한다. 만약 두 값이 동일하지 않으면 세션을 종료한다.

$$E_i' = N_1 R_s$$
$$SK_i = h(N_1 \| E_i' \| h(A_i \oplus ID_i))$$
$$C_i' = h(DID_i' \| SK_i \| R_s \| Z_i' \| SID_j)$$
$$T_i' = Z_i \oplus E_i'$$
$$A_i^n = T_i' \oplus h(N_1 \oplus h(A_i))$$
$$P_i^n = h(PW_i \| F_i \| r_i^n)$$
$$B_i^n = A_i^n \oplus P_i^n$$
$$V_i^n = h(P_i^n \oplus ID_i) \bmod n$$

$User_i$		RC
Chooses ID_i, PW_i, b_i and generates r_i Computes $F_i = H(b_i)$, $P_i = h(PW_i \| F_i \| r_i)$ $DID_i = h(ID_i \oplus r_i)$	$\{DID_i, ID_i, P_i\}$ →	Checks the validity of ID_i and generates d_i Computes $A_i = h(x \| DID_i \| ID_i \| d_i)$, $B_i = A_i \oplus P_i$ $V_i = h(P_i \oplus ID_i) \bmod n$ Stores $\{DID_i, ID_i, d_i\}$ in database
Computes R_i and saves in SC $R_i = h(ID_i \oplus F_i) \oplus r_i$	← SC	Stores $\{B_i, V_i, E_{key}(), P, P_{pub}, n\}$ in SC

Fig. 3. Proposed Registration Phase

4.3 Password change phase

패스워드를 변경하기 원하는 사용자는 다음 과정을 진행하여 자신의 패스워드를 변경할 수 있다.

1.사용자 $user_i$는 자신의 ID_i, PW_i, 생체정보 b_i를 입력하여 $F_i = H(b_i)$를 계산한 후 다음 과정을 진행한다.

$$r_i' = h(ID_i \oplus F_i) \oplus R_i$$
$$P_i' = h(PW_i \| F_i \| r_i')$$
$$V_i' = h(P_i' \oplus ID_i') \bmod n$$

2.만약 V_i'과 V_i가 동일하면 새로운 난수 r_i^n을 생성하여 다음을 계산한 후 R_i, R_i^n, V_i^n, B_i^n을 각각 저장한다. 그렇지 않을 경우에는 세션을 종료한다.

$$A_i' = B_i \oplus P_i'$$
$$R_i^n = h(ID_i \oplus F_i) \oplus r_i^n$$
$$P_i{}^n = h(PW_i \| F_i \| r_i^n)$$
$$DID_i^n = h(ID_i \oplus r_i^n)$$
$$V_i^n = h(P_i^n \oplus DID_i^n) \bmod n$$
$$B_i^n = A_i' \oplus P_i^n$$

$User_i$	RC	$Server_j$
Inputs ID_i, PW_i, b_i		
Computes $F_i = H(b_i)$		
$r_i' = h(ID_i \oplus F_i) \oplus R_i$, $P_i' = h(PW_i \| F_i \| r_i')$		
$V_i' = h(P_i' \oplus ID_i) \bmod n$, $DID_i' = h(ID_i \oplus r_i')$		
Checks $V_i' ? = V_i$ and chooses N_1, r_i^n		
Computes $A_i' = B_i \oplus P_i'$, $DID_i^n = h(ID_i \oplus r_i^n)$		
$R_i^n = h(ID_i \oplus F_i) \oplus r_i^n$		
$D_i = h(ID_i \oplus N_1 \oplus DID_i' \oplus A_i' \oplus SID_j \oplus DID_i^n)$		
$L_i = E_{A_i}(ID_i \| N_1 \| DID_i' \| A_i' \| SID_j \| DID_i^n)$		
$M_1 = \{DID_i', D_i, L_i\}$ ---------->	Retrieves $\{DID_i', ID_i\}$	
	Computes $A_i'' = h(x \| DID_i' \| ID_i \| d_i)$	
	$N_1' = D_i \oplus h(A_i'' \oplus DID_i')$	
	$D_{A_i''}(L_i) = (ID_i \| N_1 \| DID_i' \| A_i' \| SID_j \| DID_i^n)$	
	$D_i' = h(ID_i \oplus N_1 \oplus DID_i' \oplus A_i' \oplus SID_j \oplus DID_i^n)$	
	Checks $A_i'' ? = A_i'$ and $D_i' ? = D_i$	
	Replaces DID_i' with DID_i^n	
	Computes $A_i{}^n = h(x \| DID_i^n \| ID_i \| d_i)$	
	$T_i = h(N_1' \oplus h(A_i'')) \oplus A_i^n$	
	$SM_j = h(SID_j \| x \| e_j)$, $Y_i = h(SID_j \| SM_j)$	
	$M_i = E_{SM_j}(N_1' \| DID_i' \| T_i \| Y_i \| h(A_i'' \oplus ID_i))$	
	$M_2 = \{M_i\}$ ---------->	Computes $D_{SM_j}(M_i)$
		$Y_i' = h(SID_j \| SM_j)$
		Checks $Y_i' ? = Y_i$
		Generates N_2
		Computes $R_s = N_2 P$
		$E_i = N_1' R_s$, $Z_i = E_i \oplus T_i$
		$SK_j = h(N_1' \| E_i \| h(A_i'' \oplus ID_i))$
		$C_i = h(DID_i' \| SK_j \| R_s \| Z_i \| SID_j)$
Computes $E_i' = N_1 R_s$	$M_3 = \{R_s, Z_i, C_i\}$ <----------	
$SK_i = h(N_1 \| E_i' \| h(A_i \oplus ID_i))$		
$C_i' = h(DID_i' \| SK_i \| R_s \| Z_i' \| SID_j)$		
Checks $C_i' ? = C_i$		
Computes $T_i' = Z_i \oplus E_i'$		
$A_i^{n\,\prime} = T_i' \oplus h(N_1 \oplus h(A_i))$		
$P_i{}^n = h(PW_i \| F_i \| r_i^n)$, $B_i^n = A_i^n \oplus P_i^n$		
$V_i^n = h(P_i^n \oplus ID_i) \bmod n$		

Fig. 4. The Proposed Login and Authentication Phase

V. Analysis of The Proposed Scheme

본 장에서는 제안 인증 스킴의 안전성 분석과 계산 복잡도, 그리고 통신 비용의 복잡도를 비교·분석한다. 여기서 계산 복잡도는 각 연산의 횟수를 의미하고, 통신 비용의 복잡도는 각 개체 간에 필요한 전송 메시지의 길이를 의미한다. 그러므로 두 복잡도는 값이 작을수록 더 빠른 실행 속도와 더 빠른 통신이 가능하다.

1. Security Analysis

Offline password guessing attack

공격자가 사용자의 패스워드 추측 공격에 성공하려면 $P_i' = h(PW_i \| F_i \| r_i')$와 난수 r_i를 알아야 한다. 기존의 Wang이나 Wu 인증 스킴은 난수 r_i를 평문으로 저장하였으나 제안 인증 스킴은 $R_i = h(ID_i \oplus F_i) \oplus r_i$와 같이 사용자의 ID_i와 생체정보 b_i를 알아야 한다. 공격자가 사용자의 ID_i를 획득하였다 할지라도 높은 엔트로피의 생체정보는 계산해내기 어렵다. 또한 $P_i'(P_i' = B_i \oplus A_i)$을 획득하려면 A_i와 B_i의 두 값을 알아야 하는데, B_i는 스마트카드의 저장정보이나 A_i는 스마트카드의 저장정보가 아니다. 그러므로 제안 인증 스킴은 공격자에 의한 P_i' 획득이 불가하여 오프라인 패스워드 추측 공격에 안전하다.

Smart-card theft attack

스마트카드를 획득한 공격자는 난수 r_i를 계산할 수 없고, B_i의 계산은 $A_i \oplus P_i$이므로 $A_i(A_i = h(x \| DID_i \| (ID_i \| d_i))$와 P_i를 각각 알아야 하고, 이 두 값을 계산하려면 서버의 비밀키 x, 서버의 난수 d_i, 사용자의 생체정보, 그리고 사용자의 난수 r_i를 알아내야 한다. 그러므로 앞의 오프라인 패스워드 추측 공격 절에서 분석한 것처럼 해시연산한 높은 엔트로피의 이 값들을 공격자가 계산해내기 힘들다.

User anonymity

제안 인증 스킴은 매 세션마다 새로운 난수를 사용하여 동적 DID_i를 계산하고, 새로운 난수 $r_i = h(ID_i \oplus F_i) \oplus F_i) \oplus R_i$와 같이 계산하여 저장하므로 공격자는 사용자의 생체정보를 획득해야 만이 매 세션마다 변경되는 난수 r_i를 알아낼 수 있다. 그러므로 제안 인증 스킴은 안전한 사용자 익명성뿐만 아니라 추적 불가능성도 함께 제공한다.

Privileged insider attack

내부 공격자가 등록 단계의 $\{DID_i, ID_i, P_i\}$를 획득하여 패스워드 추측 공격에 성공하려면 사용자의 생성 난수 r_i와 생체정보 b_i를 알아야 한다. 그러나 해시 연산한 P_i로부터 높은 엔트로피의 r_i와 b_i를 계산해내기 어렵다. 그러므로 제안 인증 스킴은 내부자 공격에 안전하다.

Ephemeral secret leakage attack

공격자가 난수 N_1과 같이 일시적으로 사용하는 값들을 획득하였다고 가정할 경우, 세션 키 $SK_i = h(N_1 \| E_i' \| h(A_i \oplus ID_i))$를 계산하기 위해서는 A_i와 E_i를 알아야 한다. 그러나 A_i는 식 $h(x \| DID_i' \| ID_i \| d_i)$나 $A_i = B_i \oplus P_i$와 같이 서버의 비밀키 x를 알거나 B_i와 P_i를 모두 알아야 한다. B_i는 SC_i에 저장되어 있으나 P_i는 저장되지 않는 값이고, 이 값을 계산해내려면 사용자의 PW_i와 생체정보 b_i를 알아야 한다. 그러므로 공격자는 획득한 난수만으로 세션 키 SK를 계산하기 어렵다.

Table 2. Analysis of the Security Features and Design of Related Schemes

	Ali[1]	Wang[4]	Wu[5]	Mirsaraei[7]	Jha[8]	Saini[11]	Proposed
User anonymity	O	X	X	X	X	O	O
User untraceability	O	X	X	X	X	O	O
Smart-card theft attack	O	O	X	X	X	O	O
Offline password guessing attack	O	O	O	O	O	X	O
Privileged insider attack	O	O	O	O	O	O	O
User impersonation attack	X	X	O	X	O	X	O
Server impersonating attack	X	X	O	O	O	O	O
Replay attack	O	O	O	O	X	O	O
Ephemeral secret leakage attack	X	X	O	X	X	O	O
Perfect forward security	X	O	O	X	X	O	O
Design defects	X	X	X	X	X	X	O

Perfect forward security

공격자가 서버의 비밀키 x를 안다고 가정할 경우, 세션키를 계산하려면 A_i, E_i, 그리고 난수 d_i, N_1, N_2를 각각 알아야 한다. 또한, 제안 인증 스킴은 매 세션마다 난수 N_1, N_2를 새롭게 생성한다. 그러므로 공격자가 서버의 비밀키를 안다고 할지라도 함께 사용하는 난수들을 획득하지 못하는 한 제안 인증 스킴은 전방향 안전성을 보장한다.

Replay attack

제안 인증 스킴은 매 세션마다 다른 난수 r_i를 사용하여 DID_i를 계산하고, 매번 새로운 DID_i는 D_i와 L_i에 포함되어 계산한다. 또한, 새로운 DID_i^n는 RC에 저장하므로, 공격자가 보낸 기존의 DID_i와 새로운 DID_i^n이 일치하지 않아 공격자는 재전송 공격에 성공할 수 없다.

User impersonation attack

공격자가 사용자로 가장하려면 사용자의 패스워드와 생체정보를 획득해야 한다. 그러나 스마트카드 분실 공격 절에서 분석한 바와 같이 공격자는 사용자의 PW_i와 생체정보 b_i를 획득하기 어렵다. 그러므로 제안 인증 스킴은 사용자 가장 공격에 안전하다.

Confirmed Identity format

제안 인증 스킴은 등록 단계에서 사용자의 ID_i와 서버의 SID_j에 대한 타당성을 검증한다. 그러므로 사용자와 서버의 식별자에 대한 중복성 문제는 발생하지 않는다.

User-friendly password change phase

제안한 패스워드 변경단계는 서버의 도움 없이 사용자가 패스워드를 자유롭게 변경할 수 있으므로, 제안 인증 스킴은 사용자 친화적인 패스워드 변경단계를 지원한다.

2. Performance Analysis

제안 인증 스킴과 관련 인증 스킴들에 대한 계산 복잡도는 table 3과 같고, Wu 인증 스킴[5]은 복잡도 계산에 해시함수 연산을 배제하였으나, 제안 인증 스킴에서는 해시함수를 포함하여 더 정확한 계산 복잡도를 제시한다.

Table 3의 T_h는 해시함수, T_s는 비밀키 암호 방식, T_m은 ECC 곱셈 연산, T_p는 ECC point addition, 그리고 T_f는 퍼지 추출 연산을 나타내며, 각각의 실행속도는 0.0023ms, 0.0046ms, 2.26ms, 0.0288ms, 2.226ms이다[10][13]. Fig. 5에서 보듯이 Ali의 실행속도는 대략 25ms이고, Wang, Wu, Saini는 13~15ms, Mirsaraei, Jha, 그리고 제안 인증 스킴은 6.7~6.8ms이다. 그러므로 제안 인증 스킴의 실행속도가 상대적으로 빠르다는 것을 알 수 있다.

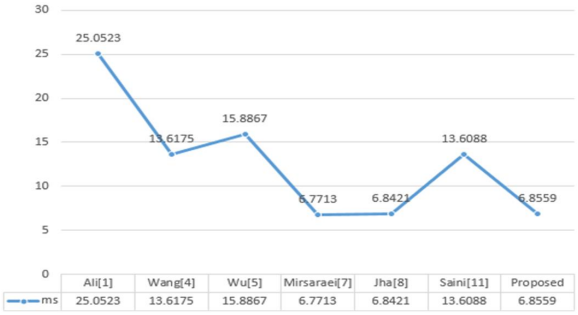

Fig. 5. Comparison of Execution Time

Table 4의 통신 비용은 제안 인증 스킴이 1760 bits로, Wu 인증 스킴의 문제를 개선하기 위하여 전송 메시지가 약간 증가하였으나, 이러한 증가는 Ali나 Jha 인증 스킴에 비하여 매우 작은 전송비용으로, 적은 메시지를 전송하므로 더 빠르게 전송할 수 있다는 것을 의미한다. 그러므로 제안 인증 스킴은 여러 공격에 안전하고 효율적인 실행속도를 나타내므로 모든 면을 고려할 때 제안 인증 스킴은 안전한 인증 스킴이라고 할 수 있다.

Table 3. Comparison of the Computational Complexity of Related Schemes

Schemes	User-side	Server-side	RC-side	Total computational complexity
Ali[1]	$6T_h+4T_m+2T_p$	$4T_h+4T_m+1T_s+2T_p$	$3T_h+3T_m+3T_s+1T_p$	$13T_h+11T_m+4T_s+5T_p$
Wang[4]	$9T_h+3T_m+1T_s$	$4T_h+2T_m+1T_s$	$4T_h+1T_m+2T_s$	$17T_h+6T_m+4T_s$
Wu[5]	$11T_h+3T_m+1T_s$	$3T_h+2T_m+1T_s$	$7T_h+2T_m+2T_s$	$21T_h+7T_m+4T_s$
Mirsaraei[7]	$5T_h+1T_m+1T_f$	$6T_h+1T_m$	-	$11T_h+2T_m+1T_f$
Jha[8]	$9T_h+2T_m$	$5T_h$	$13T_h+1T_m$	$27T_h+3T_m$
Saini[11]	$13T_h+3T_m+1T_f$	$6T_h$	$12T_h+2T_m$	$36T_h+5T_m+1T_f$
Proposed	$14T_h+1T_m+1T_s$	$3T_h+2T_m+1T_s$	$8T_h+2T_s$	$25T_h+3T_m+4T_s$

Table 4. Comparison of the Communication Cost

	Communication cost	Massage rounds
Ali[1]	3712 bits	4
Wang[4]	1664 bits	4
Wu[5]	1600 bits	3
Mirsaraei[7]	1792 bits	2
Jha[8]	3808 bits	4
Saini[11]	1792 bits	2
Proposed scheme	1760 bits	3

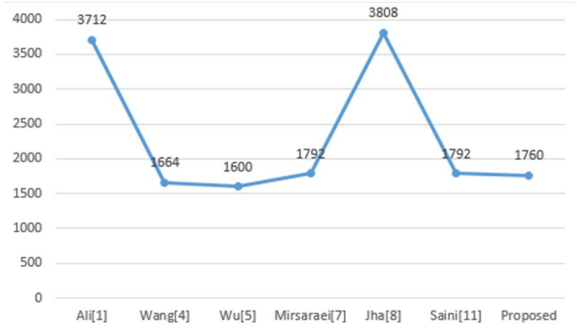

Fig. 6. Comparison of the Communication Cost

VI. Conclusions

본 논문에서 Wu 인증 스킴을 분석한 결과, 이 인증 스킴은 스마트카드 도난 공격으로 인한 사용자 익명성과 추적 불가능성을 제공하지 못하고, 설계상의 문제로 인하여 사용자와 서버 간에 동일한 세션 키를 생성하지 못한다. 또한, 식별자 미검증으로 인한 중복성 문제가 존재하며, 패스워드 변경단계를 미제안하였고, 이 단계를 제안하였다 할지라도 사용자 비친화적인 패스워드 변경단계이다.

본 논문에서는 이러한 문제를 해결한, 개선된 사용자 익명성 제공 인증 스킴을 제안하였다. 제안 인증 스킴의 분석 결과, 스마트카드 도난 공격, 오프라인 패스워드 추측 공격, 사용자 가장 공격, 특권을 가진 내부자 공격, 전방향 안전성, 세션 키 노출 공격 등 다양한 공격에 안전하였고, 관련된 다른 인증 스킴들과의 복잡도 비교에서도 상대적으로 빠른 실행속도를 나타내었다. 또한, 통신 비용에서도 큰 증가 없이 효율적인 결과를 나타내었다. 그러므로 제안 인증 스킴은 여러 공격에 대한 안전성뿐만 아니라 효율적인 복잡도를 제공하여 멀티서버 환경에 적합한 인증 스킴이다.

REFERENCES

[1] 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. DOI: 10.1002/dac.3484

[2] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, "An enhancement of a smart card authentication scheme for multi-server architecture," Wireless Personal Communications, Vol. 80, No. 1, pp. 175-192, 2015. DOI:10.1007/s11277-014-2002-x

[3] R. S. Pippal, C. D. Jaidhar, and S. Tapaswi, "Robust smart card authentication scheme for multiserver architecture," Wireless Personal Communications, Vol. 72, No. 1, pp. 729-745, Mar. 2013. DOI:10.1007/s11277-013-1039-6

[4] F. Wang, G. Xu, C. Wang, and J. Peng, "A provably secure biometrics-based authentication scheme for multiserver environment," Security and Communication Networks, Vol. 2019, pp. 1-15, June 2019. DOI: 10.1155/2019/2838615

[5] T. Y. Wu, L. Yang, Z. Lee, C. M. Chen, J. S. Pan, and S. H. Islam, "Improved ECC-based three-factor multiserver authentication scheme," Security and Communication Networks, Vol. 2021, pp. 1-14, Jan. 2021. DOI: 10.1155/2021/6627956

[6] M. Tanveer, A. U. Khan, A. Alkhayyat, S. A. Chaudhry, Y. B. Zikria and S. W. Kim, "REAS-TMIS: Resource-Efficient Authentication Scheme for Telecare Medical Information System," in IEEE Access, Vol. 10. pp. 23008-23012, 2022. DOI: 10.1109/ACCESS.2022.3153069

[7] A. G. Mirsaraei, A. Barati, H. Barati, "A secure three-factor authentication scheme for IoT environments," Journal of Parallel and Distributed Computing 169, pp. 87-105, June 2022. DOI: 10.1016/j.jpdc.2022.06.011

[8] K. Jha, A. Jain, and S. Srivastava, "A Secure Biometric-Based User Authentication Scheme for Cyber-Physical Systems in Healthcare," Vol. 39, pp. 154-169, May 2024. DOI: 10.52756/ijerr.2024.v39spl.012

[9] Y. Li, "A secure and efficient three-factor authentication protocol for IoT environments," Journal of Parallel and Distributed Computing, Vol. 179, Article 104714, pp. 1-16, Sep. 2023. DOI:10.1016/j.jpdc.2023.104714

[10] F. M. Salem, M. Safwat, R. Fathy, and S. Habashy, "AMAKAS Anonymous Mutual Authentication and Key Agreement Scheme for securing multi-server environments," Journal of Cloud Computing, Vol. 12 No. 1, pp. 1-13, Aug. 2023. DOI: 10.1186/s13677-023-00499-3

[11] K. K. Saini, D. Kaur, D. Kumar, B. Kumar, "An efficient three factor authentication protocol for wireless healthcare sensor networks," Multimedia Tools and Applications, Vol. 83. pp. 63699-63721, 2024. DOI: 10.1007/s11042-024-18114-1

[12] Z. Mahmood, Z. Ashraf, M. Iqbal, B. Farooq, "User-trust centric

lightweight access control for smart IoT crowd sensing applications in healthcare systems," Personal and Ubiquitous Computing, pp. 1-14, May 2024. DOI: 10.1007/s00779-024-01803-x

[13] A. M. Dariush, O. S. Arezou, and N. Morteza, "Novel Anonymous Key Establishment Protocol for Isolated Smart Meters," in IEEE Transactions on Industrial Electronics, Vol. 67, No. 4, pp. 2844-2851, April 2020. DOI:10.1109/TIE.2019.2912789

Authors

Mi-Og Park received the M.S. and Ph.D. degrees in Computer Science and Engineering from Soongsil University, Korea, in 1993 and 2004, respectively. Dr. Park joined the faculty of the Department of Computer Engineering at Sungkyul University, Korea, in 2005. She is interested in mobile security, security protocol and IoT security.