JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 30 No. 11, pp. 151-159, November 2025
https://doi.org/10.9708/jksci.2025.30.11.151

A Secure and Efficient User Authentication Scheme for Cyber-Physical System in Healthcare

Mi-Og Park*

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

[Abstract]

This paper analyzes the user authentication scheme for healthcare systems proposed by Jha et al. in 2024. The analysis reveals that Jha et al.'s authentication scheme is vulnerable to session key computation attacks caused by smart card loss, and it lacks user anonymity, perfect forward secrecy, and contains design flaws. To address these issues, this paper proposes a secure authentication scheme that supports anonymity. The security analysis demonstrates that the proposed scheme is resistant to various attacks, including smart-card lost attack, perfect forward secrecy, insider attack, user anonymity, offline password guessing attack, and sensor node capture attack. In addition, a comparative analysis of the computational and communication costs with related authentication schemes shows that the proposed scheme achieves superior performance in both aspects. Therefore, the proposed authentication scheme is suitable for secure and efficient user authentication in healthcare systems.

▸ **Key words**: Smart-card lost attack, Perfect forward secrecy, Session key, User anonymity, Healthcare

[요 약]

본 논문에서는 2024년에 Jha et al.이 제안한 헬스케어 시스템상에서의 사용자 인증 방식을 분석한다. 본 논문에서 분석한 결과, Jha et al.의 인증 방식은 스마트카드 분실 공격에 의한 세션 키 계산이 가능하고, 사용자 익명성, 전방향 안전성, 설계상의 취약점이 존재한다. 본 논문에서는 이러한 문제 해결을 위해 익명성을 지원하는 안전한 인증 방식을 제안하고, 안전성 분석결과, 스마트카드 분실 공격, 내부자 공격, 전방향 안전성, 사용자 익명성, 오프라인 패스워드 추측 공격, 센서노드 캡처 공격 등 다양한 공격에 안전하였다. 또한, 계산 비용과 전송 비용을 관련 인증 방식들과 비교·분석한 결과 계산 비용과 전송 비용의 두 가지 측면에서도 우수한 결과를 나타내었다. 따라서 제안 인증 방식은 헬스케어 시스템상에서의 안전하고 효율적인 사용자 인증 방식에 적합하다.

▸ **주제어**: 스마트카드 분실 공격, 전방향 안전성, 세션 키, 사용자 인증, 헬스케어

• First Author: Mi-Og Park, Corresponding Author: Mi-Og Park
*Mi-Og Park (mopark777@daum.net), Dept. of Computer Engineering, Sungkyul University
• Received: 2025. 10. 15, Revised: 2025. 10. 31, Accepted: 2025. 11. 14.

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

I. Introduction

코로나19로 인한 전 세계적 봉쇄 조치 이후, 의료 서비스의 패러다임이 기존의 치료·병원 중심에서 예방 및 소비자 중심으로 변화하면서 헬스케어(Healthcare)의 중요성이 부상하고 있다. 헬스케어는 말 그대로 건강 상태의 유지 혹은 향상 등 건강 관리를 포괄하는 산업 전반을 의미하며, 스마트폰, IoT, 웨어러블 디바이스, 클라우드 컴퓨팅, 인공지능 등 기존 의료 시스템 외부의 디지털 기술들이 빠르고 광범위하게 의료 분야에 접목되고 있다. 그러나 헬스케어 시스템은 개인의 건강 정보를 다루는 특성상 프라이버시 보호가 핵심 요소로 작용하며, 이를 반영하듯 의료 데이터는 관련 법령상 민감정보로 분류되는 중요한 정보로 보호되어야 한다. 헬스케어와 관련된 다양한 인증 방식 중, Jha 인증 방식[1]은 IoT 환경에서의 헬스케어 시스템을 위한 인증 방식을 제안하였다. 2024년에 제안된 이 방식은 원격의료시스템의 특성에 따라, 일반적인 인증 방식의 필수 요건 외에도 사용자 익명성과 같은 요소의 보장을 필수적으로 요구한다.

Jha 인증 방식은 2022년에 제안된 Mirsaraei 인증 방식[2]를 언급하고 있으며, 2023년에 발표된 Y. Li 인증 방식[3]에서는 Mirsaraei 인증 방식이 추적 불가능성(untraceability), 전방향 안전성(forward secrecy), 그리고 KCI(Key Compromise Impersonation) 공격에 취약하다고 분석하고, 이를 개선한 IoT 환경 기반의 인증 방식을 제안하였다. Mirsaraei 인증 방식은 블록체인(blockchain) 기반의 IoT 인증 방식으로, 자신들의 인증 방식이 안전하다고 주장하면서, 2021년의 Wu 인증 방식[4]이 데이터 기밀성, 데이터 무결성, 그리고 사용자 비친화적인 패스워드 업데이트 단계 등의 문제점을 가진다고 지적하였다. Mirsaraei 인증 방식에서 분석한 Wu 인증 방식은 Wang 인증 방식[5]이 사용자 가장 공격, 서버 가장 공격, 세션 기반 임시 정보 공격(KSSTI, known session-temporary information attack)의 취약점을 지적하였으며, 이러한 문제를 해결하기 위해 제안된 3-factor 인증 방식이다.

Wu 인증 방식에서 분석한 Wang 인증 방식은 2019년에 멀티서버 환경에서의 인증 방식을 제안한 것으로, Ali 인증 방식[6]의 문제점을 개선한 것이다. Wang 인증 방식이 지적한 Ali 인증 방식의 취약점으로는 전방향 안전성, 사용자 가장 공격, 서버 가장 공격, 서비스 거부 공격, 내부자 공격, KSSTI 공격 등이 있으며, Wang 방식은 자신들의 인증 방식이 보안성과 성능 측면에서 관련된 기존 방식들보다 우수하다고 주장하였다. 2023년의 Salem 인증 방식[7]은 멀티서버 환경에서 사용자 익명성을 지원하는 방식으로, Wu 인증 방식과 Wang 인증 방식이 등록 센터에서의 계산량의 오버헤드가 높다고 평가하였다. 그러나 2024년 차량 애드혹 네트워크(VANETs, Vehicular Ad-Hoc Networks) 환경을 대상으로 한 Awais 인증 방식[8]은 Salem 인증 방식도 높은 계산 비용(computational cost)을 가진다고 평가하였다. 본 논문에서도 Salem 인증 방식을 분석하였고, 그 결과 해당 방식이 안전한 사용자 익명성을 충분히 보장하지 못함을 확인하였다.

본 논문에서는 사용자 익명성이 필수적인 Jha 인증 방식을 분석하였으며, 해당 인증 방식은 스마트카드 분실 시 세션 키가 쉽게 노출되는 취약점이 있음을 확인하였다. 헬스케어 시스템은 사용자들의 건강 정보를 처리하는 특성상, 이러한 정보가 유출될 경우 개인의 프라이버시 침해뿐만 아니라 보험료 상승 등 신체적, 경제적인 중대한 문제로 이어질 수 있다. 또한, 본 논문에서는 Jha 인증 방식이 분석하지 않은 전방향 안전성 항목에 대해 추가적으로 분

Table 1. Summary of Related Authentication Schemes

	Features	Security weaknesses
Mirsaraei et al.[2]	-Authentication scheme for the IoT -ECC -Three-factor	-Does not provide perfect forward secrecy -Does not provide user untraceability attack -Does not provide KCI attack
Wu et al.[4]	-Multi-server environment -Symmetric encryption and ECC -Three-factor	-Does not resist user/server impersonation attacks -KSSTI attack
Wang[5]	-Multi-server environment, -Symmetric encryption and ECC -Three-factor	-Does not resist impersonation attacks -Does not resist KSSTI attack
Ali et al.[6]	-Multi-server authentication scheme -Symmetric encryption and ECC -Three-factor	-Doesnot resist user/server impersonation attacks -Does not resist privileged insider attack -Does not provide perfect forward secrecy -Does not resist KSSTI attack

석하였으며, 그 결과 해당 방식이 전방향 안전성 또한 만족하지 못함을 확인하였다. 이에 따라 본 논문에서는 Jha 인증 방식에 대한 리뷰를 통하여 보안상의 문제점을 제시하고, 이를 개선한 새로운 인증 방식을 제안한다.

본 논문의 구성은 다음과 같다. 제2장에서는 Jha 인증 방식의 절차를 단계별로 분석하며, 제3장에서는 해당 방식에 대한 안전성 분석 결과를 제시한다. 제4장과 제5장에서는 개선된 인증 방식을 제안하고, 안전성 분석 및 비용 효율성 평가를 수행한다. 마지막으로 제6장에서는 제안된 인증 방식에 대한 결론을 제시한다.

II. Jha et al.'s Authentication Scheme

Jha et al. 인증 방식은 시스템 초기화 단계, 센서 노드의 등록 단계, 사용자 등록 단계, 로그인 단계와 인증 단계, 그리고 패스워드 변경 단계를 제안하였다. 각 단계에서 사용한 기호의 의미는 다음과 같다.

x : 게이트웨이 GW의 비밀키(secret key)
$X = x \cdot P$: 게이트웨이 GW의 공개키(public key)
SN_j : j번째 센서 노드
ID_i : i번째 사용자의 식별자(identity)
PW_i : i번째 사용자의 패스워드
b_i : i번째 사용자의 생체정보
$H()$: 바이오 해싱 함수(bio-hashing function)
$h()$: 안전한 단방향 해쉬함수
$\|, \oplus$: 연결(concatenation)과 XOR 연산

• System initialization phase

게이트웨이 GW는 유한체 F_p에 대한 가산군(additive group)으로 G를 선택한 후, 비밀키(secret key)로 난수 $x \in Z_n^*$와 공개키(public key) $X = x \cdot P$를 계산한다. x는 비밀로 유지하고, 1024 비트의 마스터 키 K_{GW}를 선택한 후, 파라미터 $\{E(F_p), G, P, X\}$를 전송한다.

• Sensor node registration phase

게이트웨이 GW는 센서 노드 SN_j의 식별자 SID_j를 선택하고, 센서 노드의 비밀키 $K_{SN} = h(SID_j \| K_{GW})$를 계산하여 저장한 후 센서 노드 N_j에 $\{SID_j, K_{SN}\}$을 배포한다.

• User registration phase

1.사용자 U_i는 사용자의 ID_i와 PW_i, 그리고 난수 a_i를 생성하여 $MP_i = h(a_i \| PW_i)$를 계산하고 생체정보 b_i를 입력하여 $F_i = H(b_i)$를 계산한다. 계산한 $\{ID_i, F_i, MP_i\}$는 안전한 채널을 통하여 게이트웨이 GW에게 전송한다.

2.게이트웨이 GW는 $A_i = H(ID_i \| F_i \| MP_i)$, $B_i = h(F_i \| MP_i) \oplus h(ID_i \| K_{GW})$를 계산하여 $\{A_i, B_i, h(), H(), X, P\}$를 스마트카드 SC_i에 저장하여 사용자에게 안전하게 전달한다.

• Login phase

1.사용자 U_i가 자신의 ID_i와 패스워드 PW_i, 그리고 자신의 생체정보 b_i를 입력하면, 스마트카드는 $F_i' = H(b_i')$, $a_i' = V_i \oplus F_i'$, $MP_i' = h(a_i' \| PW_i)$를 계산하여 $A_i' = h(ID_i \| F_i' \| MP_i')$과 A_i가 같은지 비교한다. 만약 비교 결과가 다르면 세션을 종료하고, 그렇지 않으면 다음 과정을 계속 진행한다.

2.스마트카드 SC_i는 $C_i = B_i \oplus h(F_i' \| MP_i') = h(ID_i \| K_{GW})$를 계산한 후, 난수 r과 $U_{sk} \in Z_n^*$을 선택하여 $M_0 = r \cdot P$, $M_1 = r \cdot x \cdot P$, $M_2 = ID_i \oplus M_1$, $M_3 = SID_j \oplus h(C_i \| M_1)$, $M_4 = h(C_i \| SID_j \| M_1 \| T_1)$, $M_5 = U_{sk} \oplus h(M_1) \oplus C_i$를 계산하여, $\{M_0, M_2, M_3, M_4, M_5, T_1\}$을 GW에게 전송한다.

• Authentication phase

1.메시지를 받은 게이트웨이 GW는 타임스탬프 T_1의 $(T_2 - T_1) \le \triangle T$를 조사하여 타당할 경우, $M_1' = x \cdot M_0$, $ID_i' = M_2 \oplus M_1'$, $C_i' = h(ID_i' \| K_{GW})$, $SID_j' = M_3 \oplus h(C_i' \| M_1')$, $M_4' = h(C_i' \| SID_j' \| M_1' \| T_1)$를 계산하여, M_4'과 M_4가 동일하지 않으면 세션을 종료한다. 그렇지 않을 경우에는 $U_{sk}' = M_5 \oplus h(M_1') \oplus C_i'$, $TD_i = h(h(ID_i') \| T_1)$, $M_6 = TD_i \oplus h(h(SID_i' \| K_{GW}) \| T_3)$을 계산한 후, 난수 $G_{sk} \in Z_n^*$를 생성하고 M_7, M_8, M_9를 계산하여 $\{T_3, M_6, M_7, M_8, M_9\}$를 센서 노드 SN_j에 전송한다.

$$M_7 = G_{sk} \oplus TD_i$$
$$M_8 = G_{sk} \oplus U_{sk}'$$

$M_9 = h(G_{sk}\|U_{sk}'\|h(SID_j'\|K_{GW})\|TD_i\|T_3)$

2.센서 노드 SN_j는 타임스탬프 T_4의 $(T_4 - T_3) \leq \triangle T$를 계산하여 타당할 경우, $TD_i' = M_6 \oplus h(K_{SN}\|T_3)$, $G_{sk}' = M_7 \oplus TD_i'$, $U_{sk}' = M_8 \oplus G_{sk}'$, $M_9' = h(G_{sk}'\|U_{sk}'\|K_{SN})\|TD_i'\|T_3)$을 계산하여 M_9'과 M_9가 동일한지 비교한다. 동일하지 않으면 세션을 종료하고, 그렇지 않을 경우에 난수 $S_{sk} \in Z_n^*$를 생성하여 SK_j, M_{10}, M_{11}을 계산한 후, $\{T_5, M_{10}, M_{11}\}$을 GW에게 전한다.

$SK_j = h(TD_i\|SID_j\|U_{sk}'\|G_{sk}'\|S_{sk})$

$M_{10} = S_{sk} \oplus h(G_{sk}'\|K_{SN})$

$M_{11} = h(G_{sk}'\|S_{sk}\|U_{sk}'\|TD_i\|T_5)$

3.게이트웨이 GW는 타임스탬프 T_6의 $(T_6 - T_5) \leq \triangle T$를 계산하여 타당하지 않을 경우, 세션을 종료한다. 그렇지 않을 경우에 $S_{sk}' = M_{10} \oplus h(G_{sk}\|h(SID_j'\|K_{GW}))$, $M_{11}' = h(G_{sk}\|S_{sk}'\|U_{sk}'\|TD_i\|T_5)$을 계산하여 M_{11}'과 M_{11}이 동일한지 비교한다. 만약 결과가 동일하지 않으면 세션을 종료하고, 그렇지 않을 경우에는 $SK_g = h(TD_i\|SID_j\|U_{sk}'\|G_{sk}'\|S_{sk})$, $M_{12} = G_{sk} \oplus M_1'$, $M_{13} = S_{sk}' \oplus TD_i$을 계산한 후 타임스탬프 T_7를 생성하여 $M_{14} = h(G_{sk}\|S_{sk}'\|U_{sk}'\|TD_i\|T_7)$을 계산한다. 그런 다음 $\{T_7, M_{12}, M_{13}, M_{14}\}$를 사용자 U_i에게 전송한다.

4.사용자 U_i는 T_8의 $(T_8 - T_7) \leq \triangle T$를 계산하여 타당하지 않으면 세션을 종료하고, 그렇지 않을 경우 $G_{sk}' = M_{12} \oplus M_1$, $S_{sk}' = M_{13} \oplus TD_i$, $SK_j = h(TD_i\|SID_j\|U_{sk}\|G_{sk}'\|S_{sk}')$, $M_{14}' = h(G_{sk}'\|S_{sk}'\|U_{sk}\|TD_i\|T_7)$을 계산하여 M_{14}'과 M_{14}가 동일한지 비교한다. 동일하지 않으면 세션을 종료하고, 그렇지 않을 경우 서버를 인증한다.

• Password change phase

1.사용자 U_i가 자신의 ID_i와 패스워드 PW_i, b_i를 입력하면 스마트카드는 $F_i' = H(b_i')$, $a_i' = V_i \oplus F_i'$, $MP_i' = h(a_i'\|PW_i)$, $A_i' = h(ID_i\|F_i'\|MP_i')$을 계산하여 A_i'과 A_i가 같은지 비교하여, 비교 결과가 다르면 세션을 종료하고 그렇지 않으면 다음 과정을 진행한다.

2.스마트카드는 $MP_i^n = h(a_i'\|PW_i^n)$, $A_i^n = h(ID_i\|F_i'\|MP_i^n)$, $B_i^n = B_i \oplus h(MP_i\|F_i') \oplus h(MP_i^n\|F_i')$을 계산하여 A_i와 B_i를 A_i^n와 B_i^n으로 각각 업데이트한다.

III. Analysis of Jha et al.'s Authentication Scheme

본 장에서는 본 논문에서 분석한 Jha et al. 인증 방식의 보안 취약점으로, 스마트카드 분실 공격에 의한 세션키 노출과 전방향 안전성 등의 문제를 살펴본다.

3.1 Smart-card lost attack

스마트카드와 공개정보 T_1, M_2, M_7, M_8, M_{13}을 획득한 공격자는 Table 2의 공격 시나리오에 의하여 세션키 SK_i를 계산할 수 있다. 여기서 사용자의 ID_i는 추측 공격하여 사용하는 것으로 하며 아래 시나리오가 성공할 경우 공개정보 M_{11}과 M_{14}도 계산할 수 있다.

Table 2. The procedure of smart-card lost attack

1. $M_1' = ID_i' \oplus M_2$
2. $TD_i' = h(h(ID_i')\|T_1)$
3. $G_{SK}' = M_7 \oplus TD_i'$
4. $U_{SK}' = M_8 \oplus G_{SK}'$
5. $S_{SK}' = M_{13} \oplus TD_i'$
6. $SK_i' = h(TD_i'\|SID_j\|U_{SK}'\|G_{SK}'\|S_{SK}')$

3.2 Perfect forward secrecy

Jha 인증 방식에서는 전방향 안전성 항목을 분석하지 않았으며, 본 논문에서 이 항목을 분석한 결과 해당 인증 방식은 전방향 안전성을 보장하지 못한다. 이에 대한 과정은 Table 3과 같다.

Table 3. The procedure of perfect forward secrecy

1. $TD_i' = M_6 \oplus h(h(SID_i'\|K_{GW})\|T_3)$
2. $G_{SK}' = M_7 \oplus TD_i'$
3. $U_{SK}' = M_8 \oplus G_{SK}'$
4. $S_{SK}' = M_{13} \oplus TD_i'$
5. $SK_j' = h(TD_i'\|SID_j\|U_{SK}'\|G_{SK}'\|S_{SK}') = SK_i'$

3.3 Design problem

Jha et al. 인증 방식은 사용자 등록 단계에서 사용자의

ID_i 타당성을 확인하지 않으며, 이로 인하여 사용자 ID_i 중복 문제가 존재한다.

IV. A New Authentication Scheme

본 장에서는 스마트카드 분실 공격에 의한 세션 키 노출 문제와 전방향 안전성 문제를 해결하고 사용자 익명성을 지원하는 개선된 인증 방식을 제안한다. 제안 인증 방식의 시스템 초기화 단계는 시스템의 안전성을 위하여 난수 s_j를 K_{SN} 계산(K_{SN}=$h(SID_j||K_{GW}||s_j)$)에 추가하여 계산한 것을 제외하면 기존의 초기화 단계와 거의 동일하다.

4.1 User registration phase

1.사용자 U_i는 자신의 ID_i, 패스워드 PW_i, 난수 a_i를 생성하여 $MP_i = h(a_i||PW_i)$를 계산하고 생체정보 b_i를 이용하여 $F_i = H(b_i)$를 계산한 후, $\{ID_i, F_i, MP_i\}$를 안전한 채널을 통하여 게이트웨이에게 전송한다.

2.게이트웨이 GW는 사용자 ID_i의 타당성을 확인한 후, 타당할 경우 난수 c_i를 생성하여 $A_i = H(ID_i||F_i||MP_i)$, $B_i = h(MP_i||F_i) \oplus h(ID_i||K_{GW}||c_i)$를 계산하여 $\{A_i, B_i, h(), H(), X, P\}$를 스마트카드에 저장한 후 사용자에게 안전하게 전달한다.

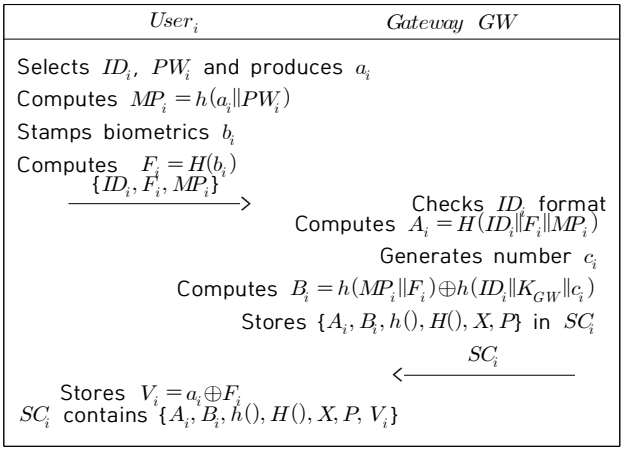

Fig. 1. Proposed Registration Process

4.2 Login phase

1.사용자 U_i가 자신의 ID_i와 패스워드 PW_i, 그리고 자신의 생체정보 b_i를 입력하면, 스마트카드는 다음의 $F_i' = H(b_i')$, $a_i' = V_i \oplus F_i'$, $MP_i' = h(a_i'||PW_i)$를 계산하여 $A_i' = h(ID_i||F_i'||MP_i')$과 A_i가 같은지 비교한다. 만약 결과 값이 다르면 세션을 종료하고, 그렇지 않으면 다음 과정을 진행한다.

2.스마트카드는 $C_i = B_i \oplus h(F_i'||MP_i')$을 계산하고 난수 r과 $U_{sk} \in Z_n^*$을 선택하여 $M_0 = r \cdot P$, $M_1 = r \cdot X$, $M_2 = E_{M_1}(ID_i||SID_j||T_1)$, $M_2 = E_{M_1}(ID_i||SID_j||T_1)$, ,$M_3 = h(C_i||SID_j||M_1||T_1)$ $M_4 = U_{sk} \oplus h(M_1 \oplus C_i \oplus T_1)$을 계산하여, $\{T_1, M_0, M_2, M_3, M_4\}$를 게이트웨이 GW에게 전송한다.

4.3 Authentication phase

1.메시지를 받은 게이트웨이 GW는 타임스탬프 T_1의 $(T_2 - T_1) \leq \triangle T$를 조사하여 타당할 경우, $M_1' = x \cdot M_0$, $D_{M_1'}(M_2) = (ID_i||SID_j||T_1)$, $C_i' = h(ID_i'||K_{GW}||c_i)$, $M_3' = h(C_i'||SID_j'||M_1'||T_1)$을 계산하여 M_3'과 M_3이 동일하지 않으면 세션을 종료한다. 그렇지 않을 경우 $U_{sk}' = M_4 \oplus h(M_1 \oplus C_i' \oplus \oplus T_1)$와 $K_{SN} = h(SID_j'||K_{GW}||s_j)$을 계산하고 타임스탬프 T_3, 난수 M_{sk}, $G_{sk} \in Z_n^*$를 생성하여 $M_5 = TD_i \oplus h(K_{SN}||T_3)$, $M_6 = G_{sk} \oplus TD_i$, $IM_1 = h(TD_i||K_{SN}||T_3)$, $M_7 = U_{sk}' \oplus IM_1, M_8 = h(G_{sk}||U_{sk}'||K_{SN}||TD_i||T_3)$을 계산하여 센서 노드 SN_j에 $\{T_3, M_5, M_6, M_7, M_8\}$을 전송한다.

2.센서 노드 SN_j는 타임스탬프 T_4의 $(T_4 - T_3) \leq \triangle T$를 조사하여 타당하지 않으면, 세션을 종료하고, 그렇지 않을 경우 $TD_i' = M_5 \oplus h(K_{SN}||T_3)$, $G_{sk}' = M_6 \oplus TD_i'$, $IM_1' = h(TD_i'||K_{SN}||T_3)$, $U_{sk}' = M_7 \oplus IM_1'$, $M_8' = h(G_{sk}'||U_{sk}'||K_{SN}||TD_i'||T_3)$를 계산하여 M_8'과 M_8이 동일한지 비교한다. 만약 두 값이 동일하지 않으면 세션을 종료하고, 그렇지 않을 경우 난수 $S_{sk} \in Z_n^*$를 생성하여 $SK_j = h(TD_i'||SID_j||IM_1'||U_{sk}'||G_{sk}'||S_{sk})$, $M_9 = S_{sk} \oplus h(G_{sk}'||K_{SN}||T_5)$, $M_{10} = h(G_{sk}'||S_{sk}||U_{sk}'||TD_i'||T_5||IM_1')$을 계산한 후, $\{T_5, M_9, M_{10}\}$을 게이트웨이에게 전송한다.

3.게이트웨이 GW는 타임스탬프 T_6의 $(T_6 - T_5) \leq \triangle T$를 계산하여 타당하지 않으면, 세션을 종료하

고 그렇지 않을 경우, S_{sk}'과 M_{11}'을 계산하여 M_{11}'과 M_{11}이 동일한지 비교한다. 동일하지 않으면 세션을 종료하고 그렇지 않을 경우, SK_g, M_{11}, M_{12}, IM_2, M_{13}을 계산하여 $\{T_7, M_{11}, M_{12}, M_{13}, IM_2\}$를 사용자에게 전송한다.

$$S_{sk}' = M_9 \oplus h(G_{sk} \| K_{SN} \| T_5)$$
$$M_{11}' = h(G_{sk} \| S_{sk}' \| U_{sk}' \| TD_i \| T_5 \| IM_1)$$
$$SK_g = h(TD_i' \| SID_j \| IM_1' \| U_{sk}' \| G_{sk} \| S_{sk}')$$
$$M_{11} = G_{sk} \oplus M_1'$$
$$M_{12} = S_{sk}' \oplus TD_i$$
$$IM_2 = TD_i' \oplus IM_1$$
$$M_{13} = h(G_{sk} \| S_{sk}' \| U_{sk}' \| TD_i \| T_7 \| IM_2)$$

4.사용자 U_i는 T_8의 $(T_8 - T_7) \leq \Delta T$를 계산하여 타당하지 않으면 세션을 종료하고, 그렇지 않을 경우, $G_{sk}' = M_{11} \oplus M_1$, $TD_i' = h(ID_i \| U_{sk}) \oplus h(M_1 \| G_{sk}')$, $S_{sk}' = M_{12} \oplus TD_i$, $IM_1' = IM_2 \oplus TD_i'$, $SK_i = h(TD_i \| SID_j \| IM_1' \| U_{sk} \| G_{sk}' \| S_{sk}')$, $M_{13}' = h(G_{sk}' \| S_{sk}' \| U_{sk} \| TD_i \| T_7 \| IM_2')$을 계산한 후, M_{13}'과 M_{13}이 동일한지 비교한다. 만약 동일하지 않으면 세션을 종료하고 그렇지 않을 경우 서버를 인증한다.

4.4 Password change phase

1.스마트카드는 사용자 U_i가 ID_i, 패스워드 PW_i, b_i를 입력하면 $F_i' = H(b_i')$, $a_i' = V_i \oplus F_i'$, $MP_i' = h(a_i' \| PW_i)$ $A_i' = h(ID_i \| F_i' \| MP_i')$을 계산하여 A_i'과 A_i가 같은지 비교한다. 비교 결과가 다르면 세션을 종료하고 그렇지 않으면 다음 과정을 진행한다.

2.스마트카드는 새로운 난수 a_i^n와 새로운 패스워드 PW_i^n을 생성하여 $V_i^n = a_i^n \oplus F_i'$, $MP_i^n = h(a_i^n \| PW_i^n)$, $A_i^n = h(ID_i \| F_i' \| MP_i^n)$, $B_i^n = B_i \oplus h(MP_i \| F_i') \oplus h(MP_i^n \| F_i')$을 계산한 후, A_i, B_i, V_i를 새로운 A_i^n, B_i^n, V_i^n으로 업데이트한다.

V. Analysis of The Proposed Scheme

본 장에서는 제안 인증 방식의 안전성과 계산 비용, 그리고 전송 비용을 기존의 관련 인증 방식들과 비교 분석함으로써, 제안 인증 방식의 안전성과 효율성을 입증한다. 비교분석 결과는 Table 4와 같으며, 'O'는 해당 공격에 대해 안전하거나 해당 기능을 보장한다는 것이고, 'X'는 그 반대의 의미를 나타낸다.

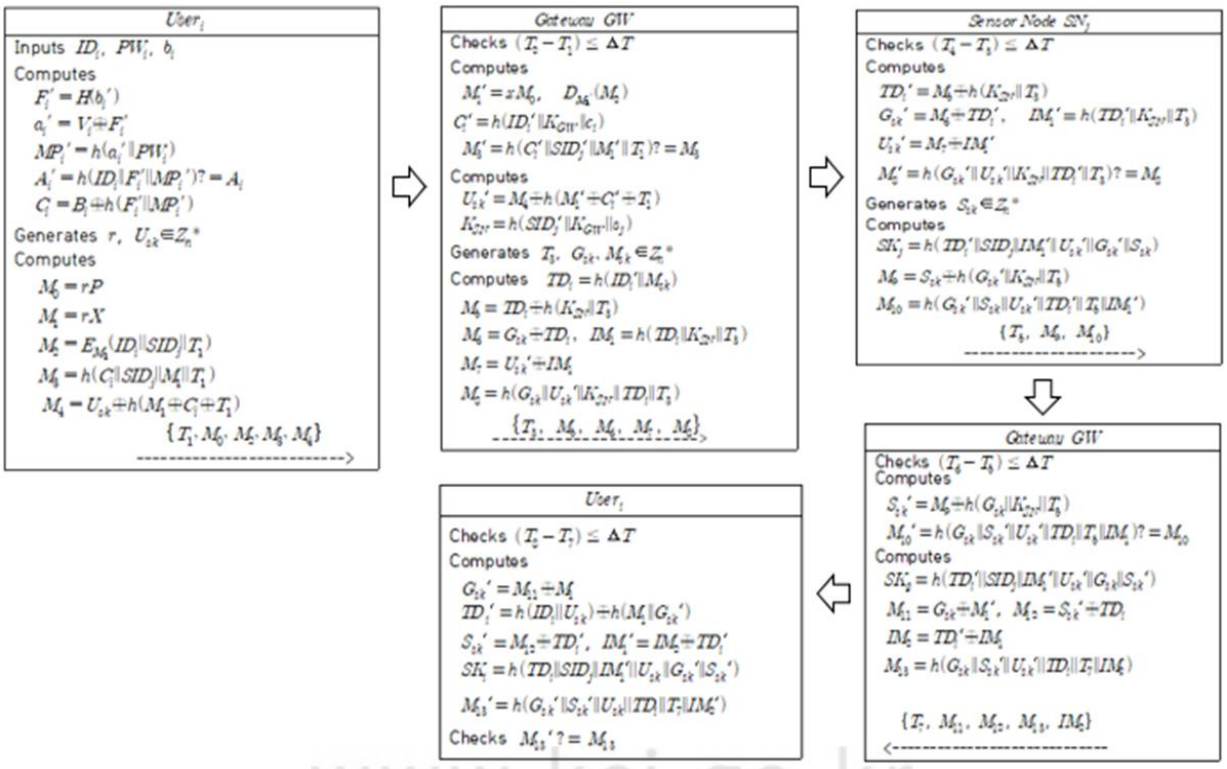

Fig. 2. The Proposed Login and Authentication Process

1. Security analysis

Perfect forward secrecy

공격자가 게이트웨이의 비밀키 x를 안다고 가정할 경우, 공격자는 $M_1' = x \cdot M_0$을 계산하여 전송 메시지 M_2를 복호화할 수 있다. 그러나 다음 과정의 $C_i' = h(ID_i' \| K_{GW} \| c_i)$를 계산해내려면 난수 c_i와 마스터 키 K_{GW}를 알아야 한다. 그러므로 공격자는 게이트웨이의 비밀키를 안다고 할지라도 다음 과정을 통과할 수 없다. 또한, 다음 과정들 중 $M_4 = U_{sk} \oplus h(M_1 \oplus C_i \oplus T_1)$를 계산하는 부분의 C_i도 난수 c_i와 마스터 키 K_{GW}를 알아야 하고, 이 식에서 사용한 다른 난수 U_{sk}도 알아야 한다. 그러므로 이 값들을 획득하지 못한 공격자는 다음 과정을 진행할 수 없어, 전방향 안전성을 깰 수 없다.

Smart-card lost attack

공격자가 사용자의 패스워드를 획득하려면 난수 a_i를 알아야 하고 이 난수는 $V_i = a_i \oplus F_i$로부터 획득할 수 있다. 그러나 난수 a_i와 생체정보를 계산한 $F_i = H(b_i)$는 저장되지 않는다. 또한, 저장정보 A_i를 사용하여 정보를 획득하려면 사용자 ID_i와 F_i, MP_i가 필요하나 이 값들 또한 저장되지 않는다. 그러므로 제안 인증 방식은 스마트 카드 분실 공격에 안전하다.

Sensor node capture attack

공격자는 센서 노드 SN_j의 저장정보 SID_j와 $K_{SN} = h(SID_j \| K_{GW} \| s_j)$를 탈취할 수 있다. 그러나 게이트웨이가 생성한 센서 노드의 식별자 SID_j와 난수 s_j를 사용하여 계산한 K_{SN}은 각 센서 노드마다 모두 다른 값이다. 그러므로 공격자가 센서 노드 SN_j의 정보를 탈취하였다 할지라도 다른 정상적인 센서 노드들과 사용자 U_i간의 세션 키를 계산하는 데에는 도움이 되지 않는다.

Privileged insider attack

ID_i, F_i, MP_i를 획득한 내부 공격자가 MP_i로부터 사용자의 패스워드를 획득하려면 사용자의 생성 난수 a_i'를 알아야 한다. 그러나 난수의 높은 엔트로피의 특성으로 인하여 특권을 가진 내부 공격자는 패스워드 추측 공격에 성공하기 어렵다.

User anonymity

사용자의 ID_i는 전송 메시지 $M_2 = E_{M_1}(ID_i \| SID_j \| T_1)$와 같이 M_1으로 암호화하여 서버에 전송한다. 그러므로 M_1 값을 알아야 만이 사용자의 ID_i를 획득할 수 있다. M_1값은 $M_1 = r \cdot X$나 $M_1' = x \cdot M_0$와 같이 계산하며 매번 다른 난수 r을 생성하여 계산한다. 그러므로 난수 r이나 서버의 비밀키 x를 획득해야 만이 사용자의 ID_i를 계산해 낼 수 있다.

Replay attack

제안 인증 방식은 모든 메시지 전송에 T_1부터 T_8까지 8개의 타임스탬프를 사용하며, 타임스탬프의 시간 간격에 대한 타당성을 먼저 검증한 후에 다음 과정을 진행한다. 그러므로 제안 인증 방식은 재전송 공격에 안전하다.

Design problems

제안 인증 방식은 사용자 등록 단계에서 사용자의 ID_i 형식을 검증한다. 이에 따라, 제안된 인증 방식은 기존의 Jha 인증 방식에서 발생할 수 있는 사용자 중복 문제를 방지할 수 있다. 특히 헬스케어 시스템은 그 특성상 사용자 중복이 심각한 문제를 초래할 수 있으므로, 이를 해결하는 것은 필수적인 설계 요소로 간주된다.

Table 4. Comparison of Security Functions and Design Defects

	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12
Jha et al.[1]	X	O	O	X	O	O	O	X	X	X	O	X
Mirsaraei et al.[2]	O	X	O	X	O	O	O	X	X	X	O	X
Y. Li[3]	X	X	X	X	O	O	O	X	X	X	O	X
Salem et al.[7]	X	O	O	X	O	O	O	X	X	X	-	X
Saini et al..[9]	O	X	O	O	O	X	O	O	O	O	X	X
W. Huang[10]	O	X	X	O	X	O	O	O	O	O	X	O
Proposed	O	O	O	O	O	O	O	O	O	O	O	O

F1:User anonymity, F2:User impersonation attack, F3:Server spoofing attack, F4:Smart-card lost attack, F5:Privileged insider attack, F6:Offline password guessing attack, F7:Replay attack, F8:Perfect forward secrecy, F9:Session key disclosure, F10:User un-traceability, F11:Sensor node capture attack, F12: Design problems

Table 5. A Comparative Analysis of Computational Costs in Related Schemes

	Registration phase	Authentication phase	Total cost
Jha et al.[1]	$6T_h$	$27T_h+3T_m$	$27T_h+3T_m$
Mirsaraei et al.[2]	$7T_h+1T_f$	$11T_h+2T_m+1T_f$	$18T_h+2T_m+2T_f$
Y. Li[3]	$7T_h+1T_{em}+1T_f$	$21T_h+1T_m+1T_f$	$28T_h+2T_m+2T_f$
Salem et al.[7]	$7T_h+3T_m$	$15T_h+4T_m$	$21T_h+7T_m$
Saini et al.[9]	$12T_h+2T_{pm}+1T_f$	$31T_h+5T_m+2T_{pm}+1T_f$	$36T_h+5T_m+2T_{pm}+2T_f$
W. Huang[10]	$8T_h+3T_m+1T_{pm}+1T_f$	$40T_h+9T_m+2T_{pm}+1T_f$	$48T_h+12T_m+3T_{pm}+2T_f$
Arpitha et al.[11]	$5T_h+1T_f$	$9T_h+7T_m+6T_s+1T_f$	$14T_h+7T_m+6T_s+2T_f$
Manickam et al.[12]	$16T_h+1T_m+8T_s$	$22T_h+5T_m$	$38T_h+6T_m+8T_s$
Proposed	$6T_h$	$28T_h+3T_m+2T_s$	$34T_h+3T_m+2T_s$

2. Computation Overhead

본 절에서 비교·분석한 제안 인증 방식의 계산 비용은 Table 5와 같다. Table 5에서 사용한 T_h, T_m, T_f, T_s, T_{pm}는 각각 해시함수의 연산, ECC에서의 곱셈 연산, 퍼지 추출 연산, 비밀키 암호방식의 암호화 및 복호화, 모듈러 지수승(modular exponentiation) 연산을 의미한다. 각 연산의 대략적인 실행시간은 순서대로 0.0026ms, 1.989ms, 1.989ms, 0.00325ms이며[10], 이에 근거하여 계산한 실행시간은 Fig. 3과 같다.

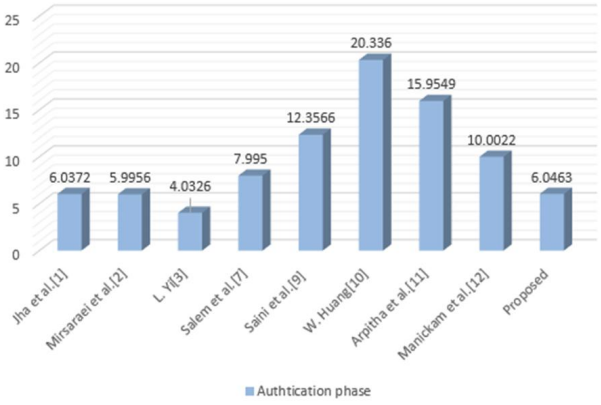

Fig. 3. Computational Cost Comparison

Fig. 3에서 W. Huang[10]의 실행시간은 20.336ms로 관련 인증 방식들 중 가장 많은 실행시간을 나타내었다. 다음으로 Arpitha 인증 방식[11]은 15.9549ms의 실행시간을 나타내어 두 번째로 많은 시간이 필요하다. Arpitha 인증 방식은 자신들의 인증 방식이 빠르다고 주장하였으나 본 논문에서 분석한 결과, T_m 연산의 누락으로 인하여 발생한 잘못된 계산 결과값이었다. Saini[9]와 Manickam 인증 방식[12]는 각각 $36T_h+5T_m+1T_f$와 $38T_h+6T_m+8T_s$의 계산 비용으로 대략 12.3566ms와 10ms의 실행시간을 나타내었다.

가장 빠른 실행시간은 4.0326ms의 Y. Li 인증 방식이고, 제안 인증 방식과 Mirsaraei, Jha 인증 방식은 대략 6ms의 실행시간을 나타내어 관련 인증 방식들 중 두 번째로 빠른 실행시간을 나타내었다.

Table 6은 전송 비용을 비교·분석한 결과로, ECC 포인트의 길이는 512비트, 해시함수는 256비트, 비밀키 암호 알고리즘은 AES-128, 그리고 기타 식별자, 난수, 타임스탬프 등의 길이는 128비트로 가정한다. Table 6의 전송 비용을 분석한 결과, 전송 비용이 낮은 편에 속한 관련 인증 방식들은 송수신 측이 사용자나 서버 등 두 개의 주체로 구성된 경우에 나타났고, 센서 노드가 포함된 3개의 송수신 주체인 경우는 Saini[9], W. Huang[10], 제안 인증 방식으로 송수신 주체가 증가한 만큼 전송 비용이 증가한 것을 알 수 있다.

Table 6. Communication Cost Comparison

	Communication cost	Massage rounds
Jha et al.[1]	4,608 bits	4
Mirsaraei et al.[2]	2,048 bits	2
Y. Li[3]	2,048 bits	2
Salem et al.[7]	2,304 bits	2
Saini et al.[9]	3,840 bits	4
W. Huang[10]	7,168 bits	4
Arpitha et al.[11]	2,176 bits	4
Manickam et al.[12]	2,176 bits	2
Proposed	4,096 bits	4

센서 노드가 포함된 3개의 통신 주체를 가진 환경에서 가장 적은 전송 비용은 3,840비트로 Saini 인증 방식이고, Jha 인증 방식은 4,608비트, 제안 인증 방식은 4,096비트이다. 가장 많은 전송 비용은 W. Huang 인증 방식으로 7,168비트이다. 그러므로 제안 인증 방식은 기존의 Jha 인증 방식의 전송 비용보다 더 감소하여 전송 비용면에서 더 효율적인 것을 알 수 있다.

VI. Conclusions

본 논문에서 분석한 Jha et al. 인증 방식은 스마트카드 분실 공격에 의한 세션 키 노출과 전방향 안전성, 그리고 설계 문제의 취약점이 있음을 확인하였다. 본 연구에서는 기존 인증 방식의 취약점을 개선하기 위한 새로운 인증 방식을 제안하였고, 안전성 분석 결과, 스마트카드 분실 공격, 전방향 안전성, 사용자 익명성, 추적 불가능성, 센서 노드 추측 공격, 오프라인 패스워드 추측 공격, 내부자 공격 등 다양한 보안 위협에 안전함을 확인하였다. 또한, 제안 인증 방식은 계산 비용면에서도 단축된 실행시간을 나타내었고, 전송 비용 측면에서도 Jha 인증 방식보다 향상된 전송 효율을 나타내었다. 그러므로 안전성과 비용 측면을 종합적으로 고려할 때, 제안 인증 방식은 사용자의 프라이버시 문제나 신체적, 경제적 문제가 발생할 수 있는 헬스케어 시스템에 적합하다고 할 수 있다. 향후 연구 과제로는 제안된 인증 방식의 보안성을 유지하면서 보다 효율적인 비용 구조를 달성하기 위한 연구가 필요할 것으로 판단된다.

REFERENCES

[1] 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

[2] 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

[3] 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

[4] 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

[5] F. Wang, G. Xu, and G. Xu., "A provably secure anonymous biometrics-based authentication scheme for wireless sensor networks using chaotic map," IEEE Access, Vol. 7, pp. 101596-101608, 2019. DOI: 10.1109/ACCESS.2019.2930542

[6] 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

[7] 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

[8] S. M. Awais, W. Yucheng, K. Mahmood, M. J. F. Alenazi, A. K. Bashir, A. K. Das, P. Lorenz, "Provably Secure and Lightweight Authentication and Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, Vol. 25, No. 12, pp. 21107-21116, Dec. 2024.

[9] 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, Jan. 2024. DOI: 10.1007/s11042-024-18114-1

[10] W. Huang, "Ecc-based three-factor authentication and key agreement scheme for wireless sensor networks," Sci Rep, Vol. 14, No.1, Jan. 2024. DOI: 10.1038/s41598-024-52134-z 1787

[11] T. Arpitha, D. Chouhan, and J. Shreyas, "Anonymous and robust biometric authentication scheme for secure social IoT healthcare applications," Journal of Engineering and Applied Science, Vol. 46, No. 2, pp. 1-13, Dec. 2024. DOI: 10.1186/s44147-023-00342-1

[12] M. Manickam and G. G. Devarajan, "A three-factor mutual authentication scheme for telecare medical information system based on ECC," Cyber Security and Applictions, Vol. 2, Jan. 2024, Art. No. 100035. DOI: 10.1016/j.csa.2024.100035

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.