Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 9 pp. 697-702, 2023

https://doi.org/10.5762/KAIS.2023.24.9.697
ISSN 1975-4701 / eISSN 2288-4688

다중서버 환경의 E-헬스케어를 위한 안전하고 효율적인 인증 및 키동의 기법

이성운
동명대학교 정보보호학과

Secure and Efficient Authentication and Key Agreement Scheme for E-Healthcare in Multi-server Environments

Sung-Woon Lee
Dept. of Information Security, Tongmyong University

요 약 Barman 등은 다중서버 환경에서 E-헬스케어를 위한 세 가지 인증 요소(스마트카드, 비밀번호, 생체 인식)를 사용하는 인증 및 키 동의 기법을 제안했다. 그러나 Ali 등은 이 기법이 사용자 위장, 서버 위장, 세션키 유출, 비밀 임시 매개변수 유출 공격 등에 취약할 뿐만 아니라 사용자 익명성을 제공하지 않는다는 것을 보여주고 이러한 문제들을 해결하기 위한 기법을 제안하였다. 그러나 Yu와 Park은 Ali 등의 기법이 공격자가 스마트카드의 내부 정보를 추출할 수 있다는 가정하에 사용자 위장 공격, 세션키 노출 공격, 중간자 공격에 성공할 수 있으며 상호인증을 제공하지 못한다는 것을 보여주었다. 본 논문에서는 먼저 Ali 등의 기법이 사용자 연결 가능성과 단일 장애 지점 문제라는 추가적인 보안 문제들을 가지고 있음을 지적하고 다중서버 환경에서 E-헬스케어를 위한 안전하고 효율적인 인증 및 키 동의 기법을 제안한다. 또한 이 기법이 기존의 관련된 기법들보다 안전성 및 연산/통신 비용 면에서 우수함을 보여준다.

Abstract Barman et al. proposed an authentication and key agreement (AKA) scheme using three factors (smartcard, password, and biometric) for e-healthcare in the multi-server environment. On the other hand, Ali et al. showed that the scheme is prone to some attacks, including user impersonation, server impersonation, session-key leakage, and secret temporary parameter leakage, but it does not provide user anonymity. Hence, this paper proposed an improved scheme to solve the problems. Yu and Park reported that Ali et al.'s scheme suffers from many drawbacks, including user impersonation, session key exposure, and man-in-the-middle, and failed to ensure mutual authentication, assuming that an attacker can extract the internal information of a legitimate user's smart card. In addition, Ali et al.'s scheme has additional security problems, including user linkabilities and single-point failure problems. This paper presents a secure and efficient authentication and key agreement scheme for e-healthcare in the multi-server environment. Furthermore, this scheme is superior to related schemes regarding security features and computation/communication costs.

Keywords : Information Security, Authentication, E-Healthcare, Smartcard, Telecare Medicine Information System

본 논문은 2022학년도 동명대학교 교내학술연구비 지원에 의하여 연구되었음. (2022B003)
*Corresponding Author : Sung-Woon Lee(Tongmyong Univ.)
email: staroun@tu.ac.kr
Received July 28, 2023 Revised August 31, 2023
Accepted September 1, 2023 Published September 30, 2023

1. 서론

최근 IT 기술의 발달은 사회 시스템과 사람들의 삶을 획기적으로 변화시키고 있다. 2020년 이후 코로나 바이러스 유행으로 인해 온라인 쇼핑, 온라인 뱅킹, 온라인 교육, E-헬스케어 등 비대면 온라인 서비스에 대한 요구가 훨씬 더 많아졌다. 특히 원격진료 의료정보시스템(TMIS)을 탑재한 E-헬스케어 시스템은 기존 클리닉 의료시스템을 대신해 환자들이 병원이나 보건소를 방문하지 않고도 원격지에서 다양한 의료 서비스를 이용할 수 있도록 해준다[1]. 이러한 대부분의 온라인 의료 서비스는 다수의 사용자에게 동시에 고품질의 다양한 서비스를 제공하기 위해 다중서버 환경을 필요로 한다. 그러나 다중서버 환경에서는 많은 사용자들과 의료 서비스 서버들 간의 메시지들이 공개 채널을 통해 전송되기 때문에 공격자가 다양한 보안 공격을 수행할 수 있다. 특별히 TMIS은 환자의 병명이나 처방전 정보가 노출되어 악용될 수 있으므로 환자의 신원과 의료 정보에 대한 프라이버시가 보호될 수 있어야 한다[3]. 사용자 프라이버시 보호를 위해서는 사용자의 익명성(Anonymity)과 사용자 비연결성(Inlinkability) 성질이 요구된다[2]. 이러한 위협을 제거하기 위해서는 다중서버 환경에서 의료 정보 서비스에 적합한 프라이버시를 보장할 수 있는 인증 및 키 동의 기법이 필요하다[3]. 따라서 본 논문에서는 다중서버 환경에서 원격 환자에게 프라이버시를 보장하며 의료 및 건강 서비스를 제공하기 위해 제안된 인증 및 키 동의 기법들만을 고려한다.

Barman 등은 퍼지 커밋을 사용하여 다중서버 환경에서 e-Healthcare를 위한 세 요소, 즉 스마트카드, 패스워드, 생체정보를 사용하고 환자의 프라이버시를 보장하기 위해 인증 및 키 동의 기법을 제안하였다[3]. 그러나 Ali 등은 Barman 등의 기법이 세션키 유출, 사용자 및 서버 위장 공격, 비밀 임시 매개변수 유출로 이어지는 도난 검증자 공격에 취약하고 사용자 익명성을 제공할 수 없음을 발견하고 개선된 기법을 제안하였다[4]. 그러나 Yu와 Park은 Ali 등의 기법이 공격자가 전력분석을 사용하여 스마트카드 메모리 정보를 추출할 수 있는 가정하에서 사용자 위장 공격, 세션키 노출 공격, 중간자 공격에 취약할 뿐만 아니라, 상호인증을 제공할 수 없음을 보여주었다[5]. 그러나 그들은 Ali 등의 기법에 대한 개선된 기법을 제안하지 못하고 몇 가지 간단한 해결 지침만을 제공하였다.

본 논문에서는 먼저 Ali 등의 기법이 Yu와 Park이 지적한 보안 문제들 이외에도 사용자 비연결성 성질을 제공하지 못할 뿐 아니라 단일 장애 지점 문제(Single point of failure)[9]를 가지고 있음에 대하여 지적하고, 다중서버 환경에서 E-헬스케어를 위한 안전하고 효율적인 세 요소 인증 및 키 동의 기법을 제안하고자 한다. 또한 이 기법이 기존의 같은 환경의 기법들에 비해 보안성 및 연산/통신 비용 면에서 우수함을 보여준다.

본 논문의 구성은 다음과 같다. 2장에서는 Ali 등의 기법에 대한 추가적인 안전성 분석을 수행하고, 3장에서는 다중서버 환경에서 E-헬스케어를 위한 새로운 세 요소 인증 및 키 동의 기법을 제안한다. 그리고 4장에서는 안전성 및 성능 분석을 수행하고 5장에서 결론을 맺는다.

2. Ali 등의 기법에 대한 안전성 분석

여기서는 Ali 등의 기법이 Yu와 Park이 지적한 보안 취약점들 이외에도 두 가지 추가적인 보안 문제들을 가지고 있음을 논의하고자 한다.

2.1 사용자 비연결성

Ali 등은 Barman 등의 기법[3]에서 공격자가 스마트카드 메모리에 저장된 정보를 추출할 수 있는 경우에 사용자 익명성을 제공하지 못함을 보여주었고, 이 문제를 해결하기 위한 새로운 기법을 제안하였다[4]. 그러나 Ali 등의 기법은 사용자 비연결성 성질을 전혀 고려하지 않고 설계되었다. 인증 및 키동의 기법에서 사용자 비연결성 성질은 공격자가 여러 세션들의 인증 메시지들을 도청하여 동일한 사용자의 것인지를 식별할 수 없을 때 제공될 수 있다. 이것은 사용자 프라이버시 유지를 위해 요구되는 성질 중의 하나이다[2].

Ali 등의 기법에서 공격자는 사용자의 로그인 요청 메시지 내의 R_i 값을 도청하여 검사함으로써 동일한 사용자의 인증 메시지인지를 쉽게 식별할 수 있다. 동일한 사용자의 R_i 값은 변하지 않고 항상 같은 값이기 때문이다. 이 공격은 사용자의 스마트카드 내부 정보를 추출 없이 인증 메시지 내의 R_i 값을 도청하는 것만으로도 가능하다.

2.2 단일 장애 지점 문제

Ali 등의 기법에서 등록센터 RC는 사용자와 서비스 서버의 등록을 담당한다[4]. 그러나 RC는 사용자와 서비스 서버 간의 로그인 및 인증 과정에도 항상 실시간으로 참여하도록 설계되어 있다. 즉 사용자와 서비스 서버 사

이의 인증 메시지는 RC를 통해서 전달된다. 이것은 통신 비용을 크게 증가시킬 뿐만 아니라 전체 시스템의 효율성을 크게 감소시킨다. 또한 전체 시스템의 보안과 효율성은 RC의 신뢰성과 성능에 크게 의존할 수밖에 없다. 그리고 만약 RC가 다운된다면 전체 시스템은 마비될 수밖에 없다. 즉 등록센터 RC는 단일 장애 지점 문제[9]를 일으킬 수 있다.

3. 제안된 기법

이 장에서는 2장에서 언급한 보안 문제들을 가지지 않고 다중서버 환경에서 E-헬스케어를 위한 환자의 프라이버시를 보장할 수 있는 세 가지 인증 요소(스마트카드, 비밀번호, 생체 인식)를 사용하는 새로운 인증 및 키 동의 기법을 제안하고자 한다. 이 기법은 네 단계, 즉 서비스 서버 등록 단계, 사용자 등록 단계, 인증 및 키 동의 단계, 패스워드 변경 단계로 구성되어 있다. Table 1은 제안된 기법에서 사용하는 표기법을 보여준다.

Table 1. Notations

Notations	Descriptions
U_i, ID_i, PW_i	A user, his/her id/password
RC, K_{RC}	Registration center, its master key
S_j, SID_j, K_j	A medical service server, its id/secret key
SC_i	Smartcard of U_i
$BIOM_i$	Biometric data of U_i
TP_i	Transformation parameter of U_i
K_{ij}, SK_{ij}	Secret key/session key between U_i and S_j
$E_K[]$, $D_K[]$	Symmetric key encryption/decryption
x?=y	Check whether x equals to y
t	Current timestamp
$\triangle t$	Allowable transmission time delay
$f(\cdot)$	Fuzzy extractor function
$g(\cdot)$	Enc./decoding function for error correction
$h(\cdot)$	Cryptographic one-way hash function
$\oplus$	Bitwise XOR operation
$\|\|$	Concatenation operation

3.1 서비스 서버 등록 단계

환자에게 의료 서비스를 제공하고자 하는 서비스 서버는 안전한 통신 채널을 통해 등록센터에 먼저 등록해야 한다. 등록센터 RC에 서비스 서버 S_j가 등록하는 과정은 다음과 같다.

(1) S_j는 자신의 아이디 SID_j를 선택한 후 RC에 전송한다.
(2) RC는 비밀키 $K_j = h(SID_j||K_{RC})$를 계산하고 S_j에 전송한다.

3.2 사용자 등록 단계

각 사용자는 서비스 서버들을 접근하기 위하여 안전한 통신 채널을 통해 등록센터에 등록하고 스마트카드를 발급받는다. 등록센터 RC에 사용자 U_i의 등록 과정은 다음과 같다.

(1) U_i는 자신의 아이디 ID_i, 임의의 수 r_i를 선택하고 $HID_i = h(ID_i||r_i)$를 계산한 후에 ID_i, HID_i, 그리고 접근할 서비스 서버들의 아이디 목록 $\{SID_j \mid 1 \le j \le m\}$을 RC에게 전송한다.
(2) RC는 먼저 $K_i = h(HID_i||K_{RC})$를 계산하고, 각 SID_j에 대하여 임의의 수 K_{ij}를 선택한 후에 $K_j = h(SID_j||K_{RC})$, $B_{ij} = E_{Kj}[HID_i, SID_j, K_{ij}]$, $G_{ij} = E_{Ki}[HID_i, K_{ij}]$를 계산한다. 그리고 RC는 K_i, $f(\cdot)$, $g(\cdot)$, $h(\cdot)$, $E[]$, $D[]$, $\{SID_j, B_{ij}, G_{ij} \mid 1 \le j \le m\}$를 스마트카드 SC_i에 저장하여 U_i에게 발급해준다.
(3) U_i는 SC_i를 발급받은 후에 패스워드 PW_i를 선택하고 생체정보 $BIOM_i$을 날인한다. SC_i는 생체정보 변환 매개변수 TP_i를 선택하고 $CT_i = f(BIOM_i, TP_i)$, $LTK_i = g_{enc}(r_i) \oplus CT_i$, $PWD_i = h(HID_i||r_i||PW_i)$, $F_i = h(HID_i||PWD_i||CT_i)$, $A_i = K_i \oplus PWD_i$를 계산한다. 그리고 SC_i는 F_i, TP_i, LTK_i, A_i를 저장하고 K_i를 제거한다. 이때 생체정보의 다양성으로 인해 발생할 수 있는 오류를 정정하기 위해 [4]에서 제시한 퍼지 추출 함수 $f(\cdot)$와 오류정정을 위한 변환 함수 $g(\cdot)$을 사용한다.

3.3 인증 및 키 동의 단계

사용자 U_i와 서비스 서버 S_j는 안전한 데이터 통신을 위하여 다음과 같은 과정을 수행해야 한다. 이 단계는 사용자와 서비스 서버 사이에 사용자의 로긴, 상호 인증, 그리고 세션키 생성 및 공유 과정을 포함한다. 세션키는 사용자와 서비스 서버 간의 안전한 데이터 전송을 위한 대칭키 암복호화 등에 사용될 수 있다.

(1) U_i는 스마트카드 SC_i를 리더기에 삽입한 후에 아이디 ID_i, 패스워드 PW_i를 입력한다. 그리고 접근할 서비스 서버 SID_j를 선택하고 생체정보 $BIOM_i$를 날인한다.
(2) SC_i는 $CT_i = f(BIOM_i, TP_i)$, $r_i = g_{dec}(LTK_i \oplus CT_i)$, $HID_i = h(ID_i||r_i)$, $PWD_i = h(HID_i||r_i||PW_i)$를

계산한 후에 F_i ?= $h(HID_i||PWD_i||CT_i)$인지를 확인한다. 만약 같지 않다면 이 세션은 거절된다. 그리고 SC_i는 $K_i = A_i \oplus PWD_i$, $(HID_i, K_{ij}) = D_{K_i}[G_{ij}]$, $V_1 = B_{ij} \oplus SID_j$, $V_2 = h(HID_i||SID_j||K_{ij}||B_{ij}||t_1)$를 계산하고 $\langle V_1, V_2, t_1 \rangle$를 S_j에게 전송한다. 여기서 t_1는 SC_i의 현재 타임스탬프를 의미한다.

(3) S_j는 메시지를 받은 후에 $|t_1 - t_{c1}| \leq \triangle t$인지를 확인한다. 여기서 t_{c1}는 메시지를 받을 때의 타임스탬프이다. 만약 만족하지 않다면 이 세션은 거절된다. S_j는 $B_{ij} = V_1 \oplus SID_j$, $(HID_i, SID_j, K_{ij}) = D_{K_j}[B_{ij}]$를 계산하고 V_2 ?= $h(HID_i||SID_j||K_{ij}||B_{ij}||t_1)$를 확인한다. 만약 만족하지 않다면 이 세션은 거절된다. 그리고 S_j는 임의의 K_{ij}^{new}를 선택한 후 $SK_{ij} = h(SID_j||HID_i||t_1||t_2||K_{ij})$, $B_{ij}^{new} = E_{K_j}[HID_i, SID_j, K_{ij}^{new}]$, $V_3 = E_{K_{ij}}[SID_j, B_{ij}^{new}, K_{ij}^{new}, t_2]$를 계산하고 $\langle V_3 \rangle$를 SC_i에게 전송한다. 여기서 SK_{ij}는 세션키이고 t_2는 S_j의 현재 타임스탬프이다.

(4) SC_i는 메시지를 받은 후에 $(SID_j, B_{ij}^{new}, K_{ij}^{new}, t_2) = D_{K_{ij}}[V_3]$를 계산하고 $|t_2 - t_{c2}| \leq \triangle t$를 확인한다. 여기서 t_{c2}는 메시지를 받을 때의 타임스탬프이다. 만약 만족하지 않다면 이 세션은 거절된다. SC_i는 $SK_{ij} = h(SID_j||HID_i||t_1||t_2||K_{ij})$, $G_{ij}^{new} = E_{K_i}[K_{ij}^{new}]$를 계산하고, $\{B_{ij}, G_{ij}\}$를 $\{B_{ij}^{new}, G_{ij}^{new}\}$로 변경한다.

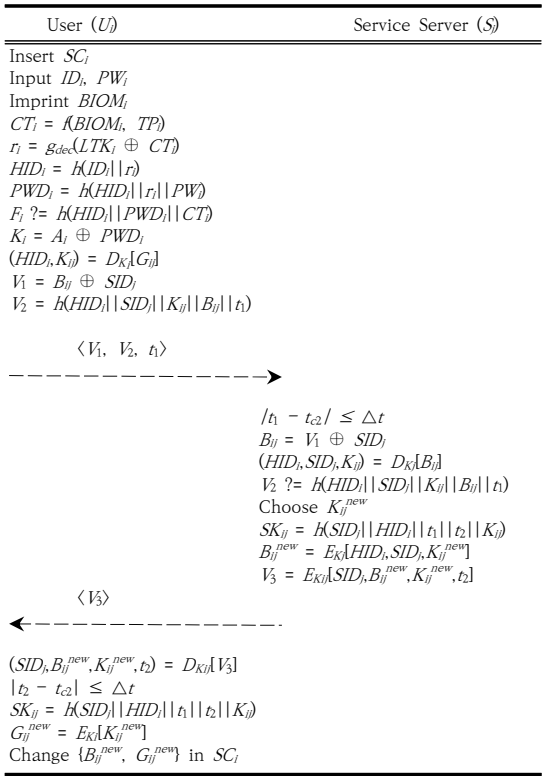


Fig. 1. Authentication and Key Agreement

3.4 패스워드 변경 단계

사용자 U_i가 패스워드 PW_i를 새로운 패스워드 PW_i^{new}로 변경할 때 다음과 같이 수행된다.

(1) U_i는 SC_i를 삽입한 후에 ID_i와 PW_i를 입력하고 생체정보 $BIOM_i$를 날인한다.

(2) SC_i는 $CT_i = f(BIOM_i, TP_i)$, $r_i = g_{dec}(LTK_i \oplus CT_i)$, $PWD_i = h(HID_i||r_i||PW_i)$를 계산하고 F_i ?= $h(HID_i||PWD_i||CT_i)$를 확인한다. 만약 만족하지 않다면 이 세션은 거절된다. 그리고 SC_i는 U_i에게 새로운 패스워드 PW_i^{new}를 입력하도록 요청한다.

(3) U_i는 새로운 PW_i^{new}를 입력한다.

(4) SC_i는 $PWD_i^{new} = h(HID_i||r_i||PW_i^{new})$, $F_i^{new} = h(HID_i||PWD_i^{new}||CT_i)$, $A_i^{new} = A_i \oplus PWD_i \oplus PWD_i^{new}$. SC_i는 $\{F_i, A_i\}$를 $\{F_i^{new}, A_i^{new}\}$로 변경한다.

4. 안전성 및 성능 분석

4.1 안전성 분석

이 절에서는 제안된 인증 및 키 동의 기법이 널리 알려진 주요 공격들에 대하여 안전함을 보여준다[3,4]. 이때 안전한 해쉬함수와 대칭키 암호 알고리즘이 사용된다고 가정한다.

4.1.1 사용자 위장 공격

제안된 기법의 인증 및 키 동의 단계에서 공격자는 서비스 서버 S_j에 대하여 사용자 U_i로 위장하려고 시도할 수 있다. 이를 위해 공격자는 서비스 서버의 검증을 통과할 수 있는 $V_1 = B_{ij} \oplus SID_j$, $V_2 = h(HID_i||SID_j||K_{ij}||B_{ij}||t_1)$를 계산할 수 있어야 한다. 그러나 공격자는 U_i와 S_j 사이에 공유되어 있는 비밀키인 K_{ij}를 알지 못하기 때문에 타당한 V_1와 V_2를 계산하기 어렵다. 그러므로 제안된 기법

은 사용자 위장 공격에 안전하다.

4.1.2 서비스 서버 위장 공격

공격자는 사용자 U_i에 대하여 서비스 서버 S_j로 위장하려고 시도할 수 있다. 이를 위해서 공격자는 사용자의 로긴 요청인 $\langle V_1, V_2, t_1\rangle$를 받은 후에 사용자의 검증을 통과할 수 있는 응답 메시지인 $V_3 = E_{K_{ij}}[SID_j, B_{ij}^{new}, K_{ij}^{new}, t_2]$를 계산할 수 있어야 한다. 그러나 공격자는 U_i와 S_j 사이에 비밀키인 K_{ij}를 알지 못하기 때문에 타당한 V_3를 계산하기 어렵다. 그러므로 제안된 기법은 서비스 서버 위장 공격에 안전하다.

4.1.3 재전송 공격

공격자는 이전 세션의 인증 메시지 $\langle V_1, V_2, t_1\rangle$, $\langle V_3\rangle$를 도청한 후에 새로운 세션에서 재사용함으로써 사용자나 서비스서버로 위장하는 등과 같은 공격을 시도할 수 있다. 제안된 기법에서는 이러한 재전송 공격을 막기 위하여 사용자 U_i와 서비스서버 S_j는 각 세션의 인증 메시지 V_1, V_2, V_3에 새로운 타임스탬프 t_1, t_2를 포함하여 전송하고 수신자는 미리 설정된 허용시간 $\triangle t$를 사용하여 타임스탬프의 유효성을 검사함으로써 과거 메시지를 재사용하는 재전송 공격을 탐지할 수 있다.

4.1.4 오프라인 패스워드 추측 공격

공격자는 $\langle V_1, V_2, t_1\rangle$와 $\langle V_3\rangle$ 메시지들을 도청한 후에 오프라인으로 패스워드 추측 공격을 시도하여 사용자의 패스워드 PW_i를 알아내려고 시도할 수 있다. 이를 위해서 공격자는 취득한 메시지들을 활용하여 추측한 패스워드 PW_i^*가 정확한지 확인할 수 있어야 한다. 그러나 공격자는 U_i와 S_j 사이에 비밀키인 K_{ij}를 알지 못하기 때문에 추측한 패스워드 PW_i^*의 정확성을 확인하기 어렵다. 그러므로 제안된 기법은 사용자 위장 공격에 안전하다.

4.1.5 사용자 익명성

공격자는 도청한 메시지들 $\langle V_1, V_2, t_1\rangle$와 $\langle V_3\rangle$로부터 사용자의 ID_i나 HID_i를 알아내려고 시도할 수 있다. 그러나 공격자가 이 정보들로부터 사용자의 아이디를 알아내기 위해서는 서비스서버 S_j의 비밀키 K를 알아야 한다. 따라서 제안된 기법은 사용자의 익명성을 제공할 수 있다.

4.1.6 사용자 연결가능성 문제

환자의 정보에 대한 프라이버시 보호를 위해 익명성 이외에도 사용자 비연결성(Inlinkability) 성질을 고려해야 한다. 사용자 비연결성은 공격자가 다른 세션들에서 얻은 인증 메시지들 $\langle V_1, V_2, t_1\rangle$, $\langle V_3\rangle$이 같은 사용자 U_i의 것인지를 구별할 수 없을 때 보장된다. 공격자는 제안된 기법에서 암호학적으로 안전한 해쉬함수와 대칭키 암호 알고리즘 때문에 이를 확인하기 어렵다. 따라서 제안된 기법은 사용자 비연결성을 제공한다.

4.1.7 단일 장애 지점 문제

제안된 기법에서 등록센터 RC는 사용자와 서비스 서버의 등록만을 담당하고, 사용자와 서비스 서버 사이의 인증 및 키 동의 단계에는 실시간으로 전혀 개입할 필요가 없다. 만약 RC에 장애가 발생했다고 하더라도 기존 사용자 U_i가 서비스 서버 S_j로 부터 서비스를 제공받는 데는 전혀 문제가 없다. 따라서 제안된 기법은 단일 장애 지점 문제(Single point of failure)를 가지고 있지 않다.

4.2 성능 분석

일반적으로 암호 기법의 성능은 기존의 관련된 기법들과 보안 특성과 계산 및 통신 비용을 비교함으로써 분석된다[3,4,6-8].

Table 2는 제안된 기법과 관련된 기법들 사이에 다양한 보안 특징들에 대한 비교를 보여준다. 제안된 기법은 다른 기법들과는 달리 모든 보안 특징들을 충족시키고 있음을 알 수 있다.

Table 2. Comparison of Security Features

Feature \ Scheme	Ours	[3]	[4]	[6]	[7]	[8]
F1	o	x	o	o	o	o
F2	o	o	o	o	o	o
F3	o	o	o	o	o	o
F4	o	o	o	o	o	o
F5	o	o	o	o	o	o
F6	o	o	x	o	o	o
F7	o	x	o	o	o	o
F8	o	x	x	o	o	o
F9	o	x	x	o	o	o
F10	o	o	o	x	o	o
F11	o	x	x	o	x	x
F12	o	o	x	o	o	o

F1: User anonymity, F2: Three-factor security, F3: Resistance to replay attacks, F4: Resistance to insider attacks, F5: Resistance to off-line password guessing attacks, F6: Resistance to stolen smart card attacks, F7: Resistance to user impersonation attacks, F8: Resistance to server impersonation attack, F9: Mutual authentication, F10: Resistance to Denial of Service attacks, F11: Inlinkability, F12: No Single point of failure

Table 3은 제안된 기법의 인증 및 키 동의 단계에서 사용된 주요 연산들의 계산 및 통신 비용을 관련된 기법들과 비교하여 보여준다. 제안된 기법이 다른 기법들보다 우수함을 알 수 있다.

Table 3. Comparisoin of Comp. and Comm. Cost

Scheme	User	Server	RC	Comm. round
Ours	5*H*+1*F*+3*S*	2*H*+3*S*		2
[3]	9*H*+1*F*	7*H*		2
[4]	6*H*+1*F*	3*H*+1*S*	5*H*+2*S*	4
[6]	10*H*	8*H*		3
[7]	9*H*+2*E*	6*H*+2*E*		3
[8]	10*H*	8*H*+2S		3

H: Hash function, *E*: ECC point multiplication
S: Symmetric encryption/decryption
F: Fuzzy extractor function

5. 결론

본 논문에서는 먼저 원격 의료 정보시스템에서 사용가능한 다중서버 환경에서 프라이버시를 제공하기 위해 설계된 Barman 등의 기법이 Yu와 Park이 지적한 여러 보안 문제들에 취약한 이외에도 다른 세션들에서 사용자 비연결성 성질을 제공하지 못하고 단일 장애 지점 문제를 가지고 있음을 보여주었다. 또한 이러한 보안 문제들을 해결한 새로운 인증 및 키 동의 기법을 제안하였다. 그리고 제안된 기법이 잘 알려진 다양한 공격들에 대하여 안전할 뿐 아니라 관련된 다른 기법들에 비교하여 보안 특성과 주요 연산 계산 및 통신 비용 면에서 우수함을 보여주었다. 제안된 기법은 수많은 환자들에게 다양한 의료 서비스들을 제공하는 대형 병원 같은 의료정보시스템에 채택되어 사용된다면 환자의 프라이버시가 크게 높일 수 있을 것으로 기대된다.

References

[1] K. Srivastava, A. K. Awasthi, S. D. Kaul, and R. C. Mittal, "A hash based mutual RFID tag authentication protocol in telecare medicine information system", *Journal of Medical System*, Vol.39, No.1, pp.153, 2015.

[2] Tianjie Cao, Jingxuan Zhai, "Improved Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems", Journal of Medical Systems, Vol.37, 2013.

[3] S. Barman, H. P. H. 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.12557-12574, 2019.

[4] Z. Ali, S. Hussain, R. H. U. Rehman, A. Munshi, M. Liaqat, N. Kumar, and S. A. Chaudhry, "ITSSAKA-S: An improved three-factor symmetrickey based secure AKA scheme for multi-server environments", *IEEE Access*, Vol.8, pp.107993-108003, 2020.

[5] S. Yu, Y. PARK, "Comments on 'ITSSAKA-S: An Improved Three-Factor Symmetric-Key Based Secure AKA Scheme for Multi-Server Environments'", *IEEE Access*, Vol. 8, pp. 193375-193379, 2020.

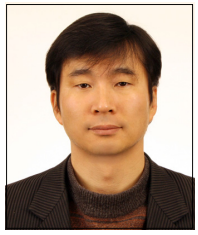
[6] S. A. Chaudhry, H. Naqvi, M. K. Khan, "An enhanced lightweight anonymous biometric based authentication scheme for TMIS", *Multimedia Tools and Applications*, Vol.77, pp.5503-5524, 2018.

[7] A. G. Reddy, E. J. Yoon, A. K. Das, V. Odelu, and K. Y. Yoo, "Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment", *IEEE Access*, Vol.5, pp.3622-3639, 2017.

[8] A. Irshad, S. A. Chaudhry, S. Kumari, M. Usman, K. Mahmood, and M. S. Faisal, "An improved lightweight multiserver authentication scheme", International Journal of Communication Systems, Vol.30, No.17, 2017.

[9] B. B. Gupta1, V. Prajapati, N. Nedjah, P. Vijayakumar, A. El-Latif, X. Chang, "Machine learning and smart card based two-factor authentication scheme for preserving anonymity in telecare medical information system (TMIS)", Neural Computing and Applications, Vol.35, pp.5055-5080, 2023.

이 성 운(Sung-Woon Lee) [정회원]



- 1993년 8월 : 전남대학교 전산통계학과 (이학석사)
- 2005년 2월 : 경북대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수

〈관심분야〉
정보통신, 정보보호