Journal of the Korea Academia-Industrial cooperation Society
Vol. 20, No. 6 pp. 1-8, 2019

https://doi.org/10.5762/KAIS.2019.20.6.1
ISSN 1975-4701 / eISSN 2288-4688

개인키 위탁관리 서버를 이용한 전자의무기록 지문인증 모델

이용준[1], 전태열[2*]
[1]국방보안연구소, [2]알파비트

An Fingerprint Authentication Model of ERM System using Private Key Escrow Management Server

Yong-Joon Lee[1], Taeyeol Jeon[2*]
[1]Defense Security Institute
[2]AlphaBit

요 약 의료정보는 환자에게 중요한 개인정보로써 반드시 보호되어야 하는 중요 정보이다. EMR((Electronic Medical Records) 시스템은 개인정보와 의료정보가 유출될 경우, 환자의 사생활 침해 등 매우 심각한 피해를 초래할 수 있어 EMR 시스템의 의료정보는 사용자 접근에 관한 제어 및 통제 강화 등 높은 보안성이 요구되는 시스템이다. 특히 의료인이 전자의무기록에 접근할 때, 보안이 강화된 신원확인에 대한 인증방식이 반드시 필요하다. 그러나 기존의 공인인증서 기반의 인증모델은 개인키 관리, 권한위임 등의 문제로 인해 전자의무기록의 보안 특성을 반영하지 못하였다. 본 연구에서는 기존의 전자의무기록(EMR) 시스템 접근 시 문제점을 해결할 수 있는 보안이 강화된 지문인식 기반 인증 모델을 제안한다. 제안한 인증 모델은 PEMS(Private-key Escrow Management Server)를 이용한 EMR 지문인증 모델로서, 개인키 위탁 프로토콜과 개인키 인출 프로토콜을 적용하여, 개인키 관리와 권한위임 문제를 해결할 수 있도록 하였다. 제안한 인증 모델은 성능 실험을 통해 기존의 공인인증서 기반 인증에 비해 수행시간 단축된 것을 확인할 수 있었고, 기존 전자서명 비밀번호 방식을 대체 가능하며, 사용자의 편의성이 증가된 장점이 있다.

Abstract Medical information is an important personal information for patients, and it must be protected. In particular, when medical personnel approach electronic medical records, authentication for enhanced security is essential. However, the existing public certificate-based certification model did not reflect the security characteristics of the electronic medical record(EMR) due to problems such as personal key management and authority delegation. In this study, we propose a fingerprint recognition-based authentication model with enhanced security to solve problems in the approach of the existing electronic medical record system. The proposed authentication model is an EMR system based on fingerprint recognition using PEMS (Private-key Escrow Management Server), which is applied with the private key commission protocol and the private key withdrawal protocol, enabling the problem of personal key management and authority delegation to be resolved at source. The performance experiment of the proposed certification model confirmed that the performance time was improved compared to the existing public certificate-based authentication, and the user's convenience was increased by recognizing fingerprints by replacing the electronic signature password.

Keywords : Electronic Medical Records, Fingerprint Recognition, Certification, Private Key, Escrow Management

*Corresponding Author : Taeyeol Jeon(AlphaBit)
Tel: +82-10-8735-5081 email: tyjeon@alphabit.co.kr
Received May 2, 2019 Revised June 5, 2019
Accepted June 7, 2019 Published June 30, 2019

1. 서론

금융거래시스템, 의료정보시스템, 전자입찰시스템 등 다양한 온라인 공공 서비스 분야에 공인인증서 기반의 사용자 인증 방식으로 사용되고 있지만, 공인인증서가 법적 효력을 제공하는 장점에 비해 사용자 개인이 안전한 저장매체에 자신의 개인키를 관리해야 하는 불편함이 있다[1, 2]. 또한 사용자에 의한 자의적인 키 위임의 경우, 법적 분쟁의 소지가 있으며, 전자서명 비밀번호의 보안강도가 약화되는 문제점도 있다[3].

전자의무기록(Electronic Medical Records; EMR) 시스템의 경우, 독립적인 사설망(private network)에 구축하여 진료행위 시, 의료인의 인증 서비스를 제공하고 있으며, 의료인의 인증을 통한 로그인 방법으로는 아이디와 비밀번호를 확인하는 방법과 공인인증서를 기반으로 사용자 인증을 하고 있다. 하지만 EMR 시스템은 보안 취약성으로 인해 의료정보의 유출이 발생될 가능성이 높다. 보안이 취약한 EMR 시스템은 개인정보와 의료정보가 유출될 경우, 환자의 사생활 침해 등 매우 심각한 피해를 초래할 수 있어 EMR 시스템의 의료정보는 사용자 접근에 관한 제어 및 통제 강화 등 높은 보안성이 요구되는 시스템이다[4, 5].

최근 많은 연구가 이루어지고 있는 지문인식 기반의 인증은 주요한 시스템의 접근 시 본인만이 시스템에 접근할 수 있는 높은 보안강도를 가지고 있으며, 신체적 특징을 이용하기 때문에 키 관리가 편리하다는 장점이 있다. 이에 반하여 지문 인식은 완벽한 인식률을 제공하기 어렵고, 아직은 법적 효력을 제공하지 못하는 한계점도 가지고 있다[6].

최근에는 환자의 진료정보를 작성한 의료 기록에 대하여 의료인의 서명이 필요한 경우에는 전자서명에 의해 전자의무기록의 신뢰성을 확보하고 있다[7]. 그러나 공인인증서 기반 인증방식은 전자서명법에 의한 법적효력과 의료기록의 신뢰성을 확보할 수 있지만, 개인키 관리의 불편함과 개인키 권함위임에 대해 모두 감시할 수 없는 한계점이 있다.

이에 따라, 지문 인식 기술을 활용하여 개인키를 인출하는 방식의 사용자에게 편의성을 제공하고 보안강도를 높이기 위한 공인인증서와 지문인식을 융합하는 연구가 최근 수행되어 왔다[8].

따라서 본 연구에서는 EMR 시스템의 보다 효과적인 사용자 접근통제 및 보안강화를 위해 개인키 위탁관리 서버를 이용한 EMR 지문인증 모델을 설계하여, 개인키 관리에 있어서의 불편함 해소와 자의적 또는 고의적인 권한위임에 의해 의료정보가 유출되거나 의료사고가 발생 시, 책임소재를 명확히 하도록 개선하고자 한다.

제안하는 모델은 개인키를 동일한 시스템이 아닌 신뢰할 수 있는 제3의 다른 시스템에 저장한 후, 지문 템플릿 등록 및 인식 시에만 개인키를 인출하는 지문인식 기반 키 위탁관리 서버를 이용한 인증 모델이며, 공개키 기반 구조의 표준을 준용하면서도 기존의 공인인증서 사용자의 키 관리에 대한 불편함을 해소할 수 있고, 자의적, 고의적인 개인키 위임을 방지할 수 있는 장점이 있다.

2. 관련 연구

2.1 EMR 시스템의 공인인증서 기반 인증

ERM 시스템의 공인인증서 인증모델은 의료인이 자신의 개인키로 생성한 전자서명을 검증하여 의료인의 신원을 확인한다. 의료인은 EMR 시스템에 접속하기 위해 전자서명을 수행하며, 시스템은 전자서명된 인증서의 유효성과 인증서 상태, 그리고 전자서명 검증 등을 통해 인증 여부를 결정한다[9]. Fig. 1은 EMR 시스템의 공인인증서 발급 프로세스를 나타낸 것이다.

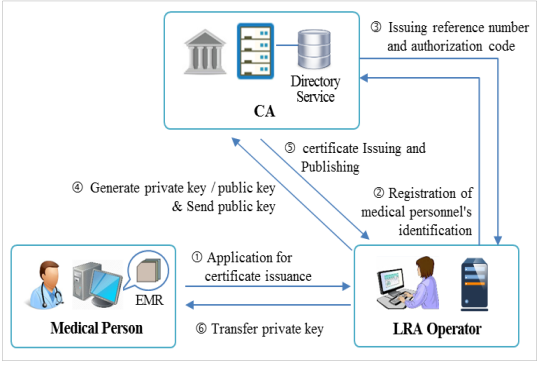


Fig. 1. Process for issuing public certificate of EMR system

EMR 시스템은 전자서명법과 의료법을 준수하여 공인인증서를 발급하고 운영한다. EMR 시스템의 의료인에 대한 공인인증서 기반 인증 프로세스는 Fig. 2와 같다.

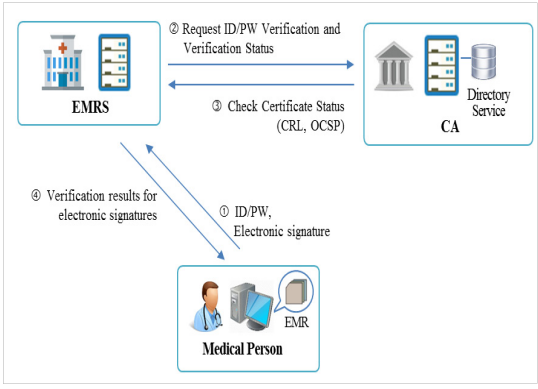


Fig. 2. Process for authentication based on public certificate of EMR system

EMR 시스템의 공인인증서 인증은 기본적인 보안 기능을 제공하지만, 다음의 몇 가지 문제점을 가지고 있다.

개인키의 보안수준이 전자서명 비밀번호에 대하여 의료인이 전자서명 비밀번호를 기억하기 용이한 단순한 정보나 자신의 신상정보 등을 조합하여 사용하는 경우에는 보안이 취약할 수밖에 없다. 또한 EMR 시스템은 통상적으로 사설망에 구축되어 있어 외부와의 통신이 단절된 네크워크 구조로 되어 있다. 안전한 EMR 인증을 수행하기 위해서는 인증서 상태를 실시간으로 확인할 수 있는 OCSP 방식을 사용해야 하지만, 독립망 형태의 EMR 시스템의 네크워크 특성상의 한계 때문에 1일 단위로 제공되는 CRL(Certificate Revocation Lists)을 통해 인증서 상태확인이 가능하다. 만약 OCSP (Online Certificate Status Protocol) 방식을 채택한 경우에는 공인인증기관간의 통신장애가 발생 시, EMR 시스템 접근을 할 수 없으므로 이 방식은 긴급성을 요구하는 EMR 시스템에는 적합하지 못하다[8]. 따라서, ERM 시스템과 같이 외부와 통신이 필요하지 않는 내부망의 특성을 고려한 보안이 강화된 새로운 인증방식이 필요하다.

의료인은 자신의 개인키를 안전하게 관리를 해야 하지만, 의료인의 진료행위는 다양한 이동성이 필요하므로 개인키를 여러 개의 의료단말기에 복사하여 사용하게 되면 개인키 유출 등의 보안상 문제가 발생된다. 이러한 개인키 복사의 문제를 해결하기 위해 의료기관에서 개인키 관리 시스템을 도입하여 활용하고 있으나, 이 경우 개인키를 중앙집중식으로 관리하기 때문에 보안위협은 더 증가하고 있는 실정이다. 또한 개인키를 안전하게 관리하기 위해 의료인의 개인키를 스마트카드나 보안토큰 등 별도의 저장매체에 저장하는 경우에는 의료인이 항상 해당 저장매체를 관리해야 하는 불편함이 있다[11].

기존 EMR 인증 시스템은 인증서 발급에 있어서 EMR 시스템의 폐쇄적 특성으로 인해 LRA(Local Registration Authority) 운영자에게 인증서 발급을 위임하고 있다. 하지만 의료인이 업무의 편의성을 위해 다른 의료인에게 자신의 개인키를 위임하는 경우, EMR 시스템은 이러한 위임행위를 감사할 수 없어 진료행위의 부인방지가 취약해진다[12]. 따라서 이러한 의료인의 타인에게의 개인키 위임이 불가한 새로운 인증방식이 필요하다.

2.2 전자서명 기반 ERM 시스템 인증 시 접근제어의 문제점

2.2.1 개인키 관리의 불편함

의료인의 업무는 빈번한 이동성을 요구하기 때문에 자신의 개인키를 별도의 의료 단말기에 복사하여 사용할 경우, 개인키 관리에 대한 어려움이 있고 항상 보안 위협에 노출될 수밖에 없다[14]. 특히 개인키를 소지하지 않은 경우에는 재발급 절차를 수행해야 하므로 의료인이 직접 개인키 관리를 해야 하는 불편함이 있다.

2.2.2 개인키의 위임 문제

의료인은 인증서 발급에 있어서 EMR 시스템의 폐쇄적 특성으로 인해 LRA 운영자에게 발급을 위임하고 있다. 더욱이 많은 의료인들은 다른 동료 의료인 또는 간호사에게 자신의 개인키를 위임하는 경우, 의료 분쟁의 소지가 발생하게 된다[13, 14]. 따라서, 의료인 간 개인키 위임이 불가능하도록 보안이 강화된 인증 방식이 필요하다.

2.2.3 EMR 시스템의 통신 위협

EMR 시스템은 통상적으로 사설망에 구축되기 때문에 외부와의 통신이 사실상 불가능한 구조로 되어 있다. 따라서, 인증서 발급, 획득, 상태 확인 등과 같이 공인인증기관(CA)과 통신하는 구간에서 통신 장애가 발생하는 경우에는 시스템으로의 접근 자체가 불가능하며, 이는 의료시스템에 요구되는 무장애 특성에 적합하지 않다[13].

3. 지문인식 기반 EMR 시스템 인증 모델

제안하는 개인키 위탁관리 서버(Private-key Escrow Management Server; PEMS)를 이용한 지문인식 기반

EMR 시스템 인증 모델은 개인키 위탁과정과 인출과정으로 구성된다. 제안 인증 모델은 공인인증기관으로부터 발급받은 개인키를 지문인식 기반으로 제3의 시스템에 위탁하고 위탁자가 필요 시, 개인키를 인출하여 사용할 수 있도록 하여 의료인이 자신의 개인키를 직접 관리해야 하는 불편함을 줄일 수 있으며, 사용자에 의한 자의적, 고의적 개인키 위임을 사전에 방지할 수 있다.

3.1 PEMS를 이용한 지문인식 기반 EMR 시스템 인증 모델

제안하는 개인키 위탁관리 서버를 이용한 지문인식기반 EMR 시스템 인증 모델에서의 의료인이 EMR 서버에 지문템플릿(Fingerprint template)을 등록하는 프로세스는 Fig. 3과 같다.

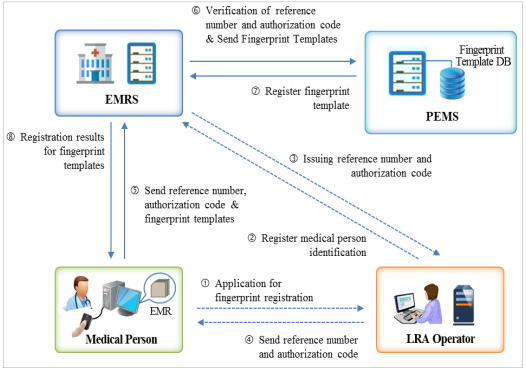


Fig. 3. Fingerprint registration process for fingerprint recognition-based EMR system

Fig. 4는 의료인의 지문인증 프로세스를 나타낸 것이다.

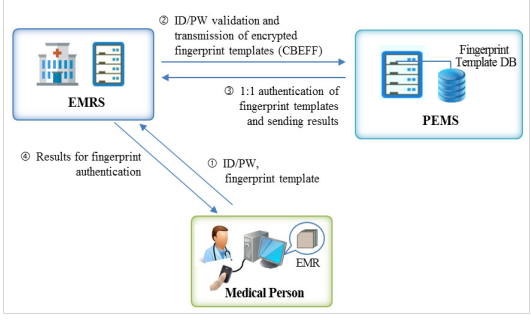


Fig. 4. Fingerprint Certification Process of the fingerprint recognition-based EMR system

제안하는 ERM 시스템에서의 지문인식기반 인증 모델은 EMR 시스템의 사용자 권한을 획득하기 위해서 의료인은 자신의 아이디와 비밀번호로 1차적인 인증 수행과 암호화된 지문 템플릿 표준 CBEFF(Common Biometric Exchange File Format)을 전송하고, PEMS 서버에서 2차적인 지문인증인 2-Factor 인증을 수행하여 보안수준을 높일 수 있다. 또한 환자에 대한 진료 및 처방 등 주요 업무에 대해 의료인으로 하여금 보다 책임 있고 신속하며 정확한 진료 지원이 가능하며, 비인가자가 EMR 시스템에 불법적 접근 시, 사전 차단이 가능하다.

3.2 개인키 위탁 프로토콜

제안하는 개인키 위탁관리 서버(PEMS)를 이용한 지문인식 기반 EMR 시스템 인증 모델은 다음의 개인키 위탁 프로토콜을 활용하여 개인키 위탁을 수행하게 된다.

- $PEMS$: 키 관리 Server
- $User$: 키 위탁자(사용자)
- $Cert_{PEMS}$: 키 관리 Server의 인증서
- FIE_{User} : 등록된 사용자의 지문 이미지
- FIM_{User} : 매칭된 사용자의 지문 이미지
- FTE_{User} : 등록된 사용자의 지문 템플릿
- FTM_{User} : 매칭된 사용자의 지문 템플릿
- ID_{User} : 사용자 ID
- pri : 사용자의 개인키
- PBE_{pri} : 암호화된 사용자의 개인키
- PWD_{pri} : 사용자의 전자서명 비밀번호
- $Envelop$ () : 비대칭키의 암호화 함수
- $Develop$() : 비대칭키의 복호화 함수
- $Encrypt$() : 대칭키의 암호화 함수
- $Decrypt$() : 대칭키의 복호화 함수
- $TKE = (ID_{User} \| FTE_{User} \| PBE_{PRI} \| PWD_{PRI})$: 키 위탁 토큰(TK)
- $ETKE = Envelop_{PEMS}(TKE)$: 키 위탁 토큰(TK)의 암호봉투
- $TKM = (ID_{User} \| FTM_{User})$: 키 인출 토큰(TK)
- $ETKM = Encrypt_K(TKM)$: 암호화된 키 인출 토큰(TK)
- $EETKM = Envelop_{PEMS}(K \| ETKM)$: 키 인출 토큰(TK)의 암호봉투

Fig. 5는 지문인식 기반의 개인키 위탁 프로토콜을 나타낸 것이다. 사용자는 제안하는 키 위탁 프로토콜을 수행하면 자신의 지문인식을 이용하여 원하는 장소나 이동 시에도 자신의 개인키의 키를 복원하여 사용할 수 있는 장점이 있다.

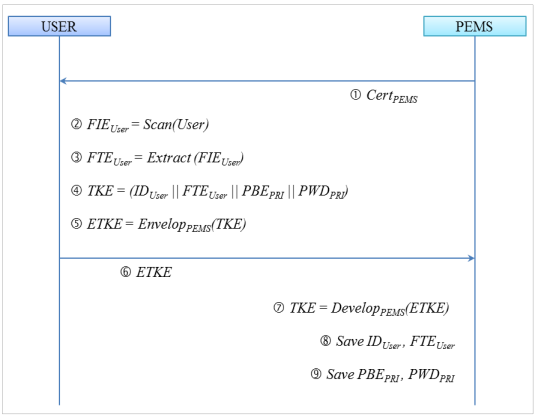


Fig. 5. Private Key Escrow Protocol

① 사용자는 키 위탁관리 서버의 인증서($Cert_{PEMS}$)를 획득하고, 획득한 키 관리 서버의 인증서에 대해 유효성 및 상태확인을 검증한다. 키 위탁관리 서버에 있는 인증서에서 추출되어진 공개키는 키 위탁 토큰을 비대칭키로 암호화하는데 사용한다.

② 사용자는 자신의 지문 템플릿을 등록하기 위해 지문 이미지(FIE_{User})를 스캔하며, 시스템은 스캔된 지문 이미지의 품질을 확인한 후 등록에 적합하지 않는 경우에는 사용자에게 재스캔을 요청한다.

③ 스캔한 지문 이미지(FIE_{User})에서 특징점을 추출한 후, 등록 템플릿(FTE_{User})을 생성한다. 등록 템플릿 생성 후, 지문 이미지는 시스템 메모리에서 완전히 폐기하여 사용자의 생체정보를 보호한다.

④ 키 위탁 토큰(TKE)을 키 위탁관리 서버에 등록하기 위해 생성한다. 키 위탁 토큰(TKE)은 사용자 아이디(ID_{User}), 등록 템플릿(FTE_{User}), 암호화된 개인키(PBE_{pri}), 전자서명 비밀번호(PWD_{pri})로 구성되어 있다.

· $TKE = ID_{User} \| FTE_{User} \| PBE_{PRI} \| PWD_{PRI}$

⑤ 키 위탁관리 서버의 공개키를 이용하여 키 위탁 토큰(TKE)에 대해 비대칭키 암호화를 작업을 수행한다. 키 위탁 토큰 암호봉투는 키 위탁관리 서버(PEMS)에 있는 개인키에 의해서만 복호화가 가능하기 때문에 토큰이 외부로 유출되지 않는다.

· $ETKE = Envelop_{PEMS}(TKE)$

⑥ 사용자로부터 생성된 위탁 토큰 암호봉투(ETKE)를 키 위탁관리 서버에 전송한다.

⑦ 키 위탁관리 서버의 개인키로 이전에 전송받은 키 위탁 토큰 암호봉투(ETKE)를 복호화하며, 복호화 작업이 정상적으로 수행되면 키 위탁 토큰이 안전하게 복구된다.

· $TKE = Develop_{PEMS}(ETKE)$

⑧ 키 위탁관리 서버는 키 위탁 토큰(TKE)에서 사용자 아이디(ID_{User}), 등록 템플릿(FTE_{User})을 데이터베이스에 등록한다.

⑨ 키 위탁관리 서버는 등록된 사용자 계정과 구별된 테이블에 암호화된 개인키(PBE_{PRI}), 전자서명 비밀번호(PWD_{PRI})를 저장한다.

3.2 개인키 인출 프로토콜

Fig. 6은 지문인식 기반의 개인키 인출 프로토콜을 나타낸 것이다. 제안하는 키 인출 프로토콜을 사용하면 사용자의 지문(생체)인식을 이용하여 원하는 진료장소 또는 이동시에도 의료인의 개인키를 인출하여 ERM 시스템 접근을 위한 전자서명을 편리하게 사용할 수 있다.

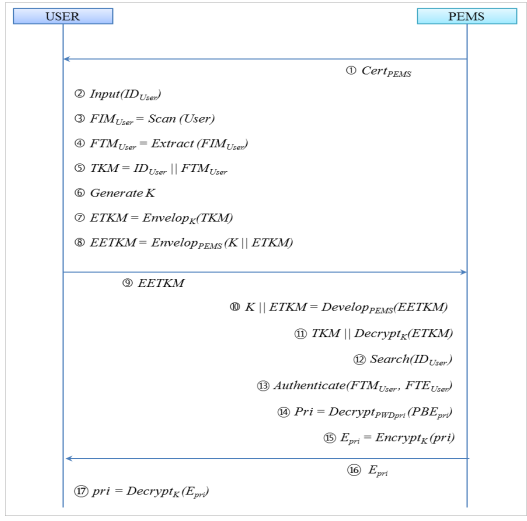


Fig. 6. Private key fetch protocol

① 사용자는 키 위탁관리 서버에 있는 인증서($Cert_{PEMS}$)를 획득한 후, 획득한 키 위탁관리 서버의 인증서의 유효성 및 상태확인을 검증한다. 키 위탁관리 서버의 인증서로 부터 추출된 공개키는 키 인출 토큰의 비대칭키 암호화에 이용한다.

② 사용자는 사용자 아이디(ID_{User})를 입력한다. 사용자 아이디는 키 위탁관리 서버의 데이터베이스에 등록 여부를 확인하는 정보로써 사용된다.

③ 사용자의 지문을 인식하기 위해 지문 샘플(FIM_{User})을 스캔하며, 스캔된 지문 이미지의 품질을 확인한 후, 적합하지 않으면 재스캔을 요청한다.

④ 획득된 지문 이미지(FIM_{User})의 특징점을 추출한 후, 매칭 템플릿(FTM_{User})을 생성하며, 매칭 템플릿을 생성한 후에는 지문 이미지를 시스템 메모리에서 완전 폐기하여 사용자의 생체정보를 보호한다.

⑤ 키 위탁관리 서버에 전송할 키 인출 토큰(TKM)을 생성하며, 키 인출 토큰은 사용자 아이디(ID_{User})와 매칭 템플릿(FTM_{User})으로 구성된다.

· $TKM = ID_{User} \| FTM_{User}$

⑥ 사용자는 키 위탁관리 서버와 통신구간의 보안을 위해 세션키(K)를 생성한다.

⑦ 사용자는 키 인출 토큰을 세션키로 하여 대칭키 암호화 작업을 수행한다.

· $ETKM = Encrypt_K(TKM)$

⑧ 키 위탁관리 서버의 공개키로 세션키(K)와 암호화된 키 인출 토큰(ETKM)에 대하여 비대칭키 암호화를 수행한다. 키 인출 토큰 암호봉투(EETKM)는 키 관리 서버의 개인키로만 복호화되기 때문에 토큰이 외부로 유출되지 않는다.

· $EETKM = Envelop_{PEMS}(K \| ETKM)$

⑨ 키 위탁관리 서버에 사용자가 생성한 키 인출 토큰의 암호봉투(EETKM)를 전송한다.

⑩ 전송받은 키 인출 토큰의 암호봉투(EETKM)를 키 위탁관리 서버에 있는 개인키로 복호화 작업을 수행한다. 정상적으로 복호화가 수행되면, 세션키(K)와 암호화된 키 위탁 토큰(ETKM)을 복호화한다.

· $K \| ETKM = Develop_{KMS}(EETKM)$

⑪ 키 관리 서버는 복호화한 세션키를 이용하여 암호화된 키 위탁 토큰(ETKM)에 대해 복화화 작업을 수행한다.

· $TKM = Decrypt_K(ETKM)$

⑫ 키 위탁관리 서버는 키 인출 토큰의 USER ID로 DB를 검색하여 매칭되는 사용자 아이디에 해당하는 정보를 추출한다.

⑬ 키 위탁관리 서버는 매칭 템플릿과 등록 템플릿을 1:1 비교를 통해 사용자의 본인 여부를 판별한다.

⑭ 키 위탁관리 서버는 1:1 지문비교 결과, 적합하면 해당 인출자의 별도의 DB 테이블에서 암호화된 개인키(PBE_{pri})와 전자서명 비밀번호(PWD_{pri})를 인출한 후, 암호화된 자신의 개인키를 전자서명 비밀번호로 복호화 작업을 수행한다.

· $pri = Decrypt_{PWD_{pri}}(PBE_{pri})$

⑮ 키 위탁관리 서버는 사용자와 교환된 세션키로 개인키를 대칭키 암호화한다.

· $E_{pri} = Encrypt_K(Pri)$

⑯ 키 위탁관리 서버는 사용자에게 세션키로 암호화한 개인키를 전송한다.

⑰ 사용자는 프로토콜 초기 단계에서 생성된 세션키로 전송받은 암호화된 개인키에 대해 복호화 작업을 수행한다. 사용자는 복구된 개인키(pri)로 전자서명 수행이 가능하다.

· $pri = Decrypt_K(E_{pri})$

4. 실험 및 평가

제안한 인증 모델의 성능 실험을 위해서 국내 의료기관을 대상으로 지문인식 적용 사례를 통해 실험을 수행하였다.

실험에서는 의료인이 접속하는 EMR 시스템에 지문 스캐너를 이용하여 3주간 테스트를 수행하였다. 의료인의 PC는 Windows 7, CPU 4.5 GHz, RAM 16G, HDD 1T이며, 지문 스캐너는 520pi, 208 pixel, 256 grayscale 스캔 성능의 국내 제품으로 테스트하였으며, 인증서상태 확인은 CRL 매커니즘을 이용하여 로컬 PC에 저장한 상태에서 테스트하였다.

Table 1. Result of EMR digital signature

Step	Category	Contents	Algorithm	Data Size	Execution time
1	Generate electronic signature	Enter electronic signature password (8 digits or more) and generate electronic signature	RSA 2048, SHA-2	2,308 Bytes	4.80 s
2	Electronic Signature Verification	Verification of electronic signatures	RSA 2048, SHA-2	-	0.29 s
3	Checking the status of the certificate	Check the certificate status	CRL(Local Search)	5,206 Bytes	0.51 s
Total results				7,514 Bytes	5.60 s

Table 1은 기존의 공인인증서를 적용한 EMR 인증방식으로 100회의 전자서명에 대한 수행 결과이다. 평균 수행시간이 5.6초가 소요되는 것을 확인할 수 있다.

Table 2. Result of EMR fingerprint recognition

Step	Category	Contents	Algorithm	Data Size	Execution time
1	Time to generate fingerprint template	Extract Fingerprint Scanning and Features	Extract Fingerprint Template	512 Bytes	2.56 s
2	Time to create CBEFF (encryption)	Biometric Common Format and Encryption	AES, SHA-2	8,264 Bytes	0.32 s
3	Time to decrypt CBEFF	Comparison Between Fingerprint Feature Points	1:1 Matching (limit 60 points)	8,264 Bytes	0.22 s
4	Time to match fingerprints	Comparison Between Fingerprint Feature	1:1 Matching (limit 60 points)	512 Bytes	0.51 s
Total results				8,264 Bytes	3.61 s

Table 2는 제안하는 지문인증 방식으로 EMR 시스템에서 100회의 전자서명에 대한 수행결과이다. 평균 수행시간이 3.61초로 기존의 공인인증서를 적용한 방식시간에 비해 수행시간이 단축되었다.

본 연구에 있어서 생체인식 정보에 대한 개인정보 보호를 위해 국제표준을 반영하였으며, 본 실험에는 CBEFF에서 제시하고 있는 생체정보 암호화를 위해서 AES 알고리즘을 사용하였으며, CBEFF 형식에 대한 무결성을 검증을 위해 SHA-2를 사용하여 실험을 하였다. 사용자의 지문원본 이미지는 완전삭제하여 시스템에 저장하지 않는 것을 원칙으로 하였다.

실험결과에서 나타나듯이 기존의 공인인증서 기반의 인증방식과 비교하여 제안 인증방식이 수행시간이 개선된 것으로 확인되었으며, 기존의 전자서명 비밀번호 방식을 의료인 지문으로 대체함으로써 인증 속도 단축뿐만 아니라 사용자의 편의성도 증가된 것을 알 수 있다.

5. 결론

전자의무기록은 환자의 진료와 관련된 정보을 담고 있기 때문에 전자의무기록은 환자 개인의 개인정보 중에서도 민감하고 중요한 정보이다. 전자의무기록 시스템에 저장된 환자의 질병과 의료인의 진료에 대한 기록은 환자와 의료인 모두에 있어서 중요한 개인정보이므로 반드시 안전하게 보호되어야 한다. 문서형태의 의무기록은 관리와 보관상에 한계가 있기 때문에, 최근의 의무기록은 마이크로필름 또는 광디스크 등에 저장 및 관리되고 있으며, 처방을 전달하는 시스템에서는 환자 인적사항과, 처방한 내역, 그리고 검사 결과 등이 모두 텍스트 형태로 입력되어 진료에 활용되고 있다.

이러한 개인의 의료정보를 관리하는 EMR 시스템에서의 사용자 인증은 EMR시스템의 접근에 대한 허가 여부를 판별함과 동시에 해당 의료인에 대한 시스템 접근 및 사용 권한을 부여하는 중요한 보안요소이다. 기존 공인인증서 기반의 인증방식은 환자에 대한 진료정보를 이용하거나 다른 의료기관에 전송할 때, 진료기록이 임의로 수정되거나 변조되는 것을 방지하기 위해 채택하였다. 그러나 의료인이 개인키를 스마트카드나 보안토큰 등의 별도의 저장매체에 보관해야 하는 불편함이 있고, 의료인의 공인인증서 발급과 인증서상태 확인 등을 위해 외부와 실시간으로 통신해야 하는 사설망 구조인 EMR 시스템에서는 보안상 적절하지 않다. 또한 개인키의 생성과 관리에 있어서 타인으로의 권한위임이 가능한데도 EMR 시스템에는 이를 감사할 수 있는 별도의 보안기능이 없어 신뢰성이 낮은 한계가 있다.

이러한 문제를 해결하기 위해 본 논문에서는 보다 신뢰성 높은 EMR 시스템을 구축 및 운영하기 위하여 개인키 위탁관리 서버를 이용한 지문인증 모델을 제안하였다. 제안하는 모델은 의료인의 EMR 시스템 접속 시, 지문인식을 적용하여 강화된 신원확인과 부인방지를 제공한다. 제안하는 ERM 시스템에서의 지문인식 기반 사용자 인증 모델은 의료인에게 개인키 관리에 있어서의 문제점들을 개선하고, 별도로 외부와의 통신이 필요하지 않기 때문에 사설망 구조인 EMR 시스템에 매우 적합한 인증방식을 제공하며, 특히 공인인증서 기반 인증에 있어서 가장 큰 문제점인 타인으로의 개인키의 위임을 원천적으로 차단할 수 있어 EMR 시스템의 신뢰성을 향상시킬 수 있는 장점이 있다.

References

[1] C. S. Kruse, B. Smith, H. Vanderlinden, A. Nealand, “Security Techniques for the Electronic Health Records”, *Journal of Medical Systems*, Vol.41, No.8, pp.127-139, July 2017.

DOI: https://doi.org/10.1007/s10916-017-0778-4

[2] J. S. Lee, H. J. Kim, M. S. Jun, "A Study on a Secure Internet Service Provider Model Using Smart Secure-Pad," Journal of the Korea Academia-Industrial, Vol.14, No.3, pp.1428-1438, 2015.
DOI: http://dx.doi.org/10.5762/KAIS.2013.14.3.1428

[3] J. W. Kim, J. H. Park, M. S. Jun, "A Design of Smart Banking System using Digital Signature based on Biometric Authentication", *Journal of the Korea Academia-Industrial*, Vol.16, No.9, pp.6282-6289, 2015.
DOI: http://dx.doi.org/10.5762/KAIS.2015.16.9.6282

[4] G. D. Mogli, "Fingerprint-based crypto-biometric system for network security", *Journal on Information Security*, Vol.2, No.4, pp.156-165, 2011.
DOI: http://dx.doi.org/10.4038/sljbmi.v2i4.2245

[5] S. Y. Min, B. W. Jin, "Design of Integrated Authentication Scheme for Safe Personal Information Management in a U-Health Environment," Journal of the Korea Academia-Industrial, Vol.15, No.6, pp.3865-3871, 2014.
DOI: http://dx.doi.org/10.5762/KAIS.2014.15.6.3865

[6] S. Barman, D. Samanta, S. Chattopadhyay, "Role of Biometrics in healthcare privacy and security management system", *Journal of Bio-Medical Informatics*, Vol.2015, No.3, pp.1-12, April 2015.
DOI: https://doi.org/10.1186/s13635-015-0020-1

[7] H. Chao, S. Twu, C. Hsu, "A Patient-Identity Security Mechanism For Electronic Medical Records (EMRs) During Transit and At Rest", *Journal of Medical Informatics and the Internet in Medicine*, Vol.30, No.3, pp.227-240, July 2009.
DOI: https://doi.org/10.1080/14639230500209443

[8] W. Yang, S. Wang, J. Hu, G. Zheng, C. Valli, "Security and accuracy of fingerprint-based biometrics: A review", *International Journal of Symmetry*, Vol.11, No.2, pp.141-150, 2019.
DOI: https://doi.org/10.3390/sym11020141

[9] N. Lo, C. Wu, Yo. Chuang, "An authentication and authorization mechanism for long-term electronic health records management", *Journal of Procedia Computer Science*, Vol.111, pp.145-453, 2017.
DOI: https://doi.org/10.1016/j.procs.2017.06.021

[10] Zhou, X. Lin, X. Dong, Z. Cao, "PSMPA: Patient Self-controllable and Multi-level Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System", *IEEE Transactions on Parallel and Distributed Systems*, Vol.26, No.6, pp.1693-1703, 2015.
DOI: https://doi.org/10.1109/TPDS.2014.2314119

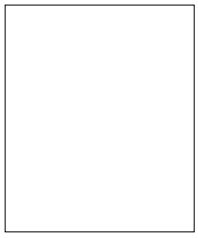
[11] M. Vigil, D. Cabarcas, J. Buchmann, J. Huang, "Assessing trust in the long-term protection of documents", *2013 IEEE Symposium on Computers and Communication(ISCC)*,Split, Croatia, 7-10 July 2013.
DOI: https://doi.org/10.1109/ISCC.2013.6754943

[12] W. Lei, Y. Li, Y. Sang, H. Shen, "A Secure Anonymous Authentication Scheme for Electronic Medical Records Systems ", *2016 IEEE 13th International Conference on e-Business Engineering (ICEBE)*, pp. 48-55, Macau, China, Nov. 2016.
DOI: https://doi.org/10.1109/ICEBE.2016.019

[13] V. Liu, M. Musen,T. Chou, "Data Breaches of Protected Health Information in the United States", *Journal of the American Medical Association*, Vol.313, No.14, pp.1471-1473, 2015.
DOI: https://doi.org/10.1001/jama.2015.2252

[14] H. Ma, R. Zhang, G. Yang, Z. Song, K. He, Y. Xiao, "Efficient Fine-Grained Data Sharing Mechanism for Electronic Medical Record Systems with Mobile Devices", *IEEE Transactions on Dependable and Secure Computing*, pp.1-11, June 2018.
DOI: https://doi.org/10.1109/TDSC.2018.2844814

이 용 준(Yong-Joon Lee) [종신회원]



- 2005년 2월 : 숭실대학교 컴퓨터학과 박사
- 2010년 2월 ~ 2006년 3월 : 한국인터넷진흥원 수석연구원
- 2016년 4월 ~ 현재 : 국방보안연구소 선임연구원

〈관심분야〉
산업보안, 사이버보안, 기밀유출차단

전 태 열(Tae-Yeol Jeon) [정회원]

- 2006년 2월 : 수원대학교 컴퓨터공학과 학사
- 2014년 11월 : 알파비트 대표이사
- 2018년 2월 : 서울대학교 차세대 융합기술연구원 최고전략과정 (WCCP) 11기 졸업

〈관심분야〉
정보보호 정보통신