http://dx.doi.org/10.3745/KIPSTC.2011.18C.6.379

지문인식 기반의 전자의무기록 시스템 인증 모델

이 용 준†

요 약

의료정보는 환자에게 중요한 개인정보로써 반드시 보호돼야 한다. 특히 전자의무기록에 접근할때, 의료인의 강화된 신원확인에 대한 인증방식이 필요하다. 기존의 공인인증서 기반 인증모델은 개인키 관리, 권한위임 등 문제점으로 전자의무기록의 특성을 반영하지 못했다. 본 논문에서는 전자의무기록 시스템에 의료인이 접근하는 경우 지문인식 기반 인증 모델을 적용하여 강화된 인증방식을 제안한다. 전자의무기록의 지문인증 모델은 의료업무의 특성을 반영하여 개인키 관리, 권한위임 문제를 원천적으로 해결하였다.

키워드 : 전자의무기록, 공인인증서, 지문인식

An Authentication Model based Fingerprint Recognition for Electronic Medical Records System

Yong-joon, Lee†

ABSTRACT

Ensuring the security of medical records is becoming an increasingly important problem as modern technology is integrated into existing medical services. As a consequence of the adoption of EMR(Electronic Medical Records) in the health care sector, it is becoming more and more common for a health professional to edit and view a patient's record. In order to protect the patient's privacy, a secure authentication model to access the electronic medical records system must be used. A traditional identity based digital certificate for the authenticity of EMR has private key management and key escrow of a user's private key. In order to protect the EMR, The traditional authentication system is based on the digital certificate. The identity based digital certificate has many disadvantages, for example, the private key can be forgotten or stolen, and can be easily escrow of the private key. Nowadays, authentication model using fingerprint recognition technology for EMR has become more prevalent because of the advantages over digital certificate -based authentication model. Because identity-based fingerprint recognition can eliminate disadvantages of identity-based digital certificate, the proposed authentication model provide high security for access control in EMR.

Keywords : EMR(Electronic Medical Record), Digital Certificate, Fingerprint Recognition

1. 서 론

전자의무기록 시스템은 독립적인 사설망에서 구축하여 진료행위를 위해 의료인의 인증을 제공하고 있다. 의료인의 인증을 통한 로그인 방법으로 일차적으로 아이디와 비밀번호를 확인하고, 의료인의 접속기록에 대한 로그를 저장하여 감사를 위한 근거로 사용할 수 있다. 의료정보의 유출은 개인정보와 의료정보로써 사생활 침해의 측면에서 심각성을 가진다. 그러므로 전자의무기록 시스템은 의료정보에 대하여 접근제어에 관한 통제 강화 등 보안의 강화가 필요하다.

미국의 경우 HIPAA(전자 의료 보험 청구법 : Health Insurance Portability Accountability Act)는 의료정보 비밀유지(사생활 정보 포함), 정보보안 표준 등의 규정을 마련하고 있다. 국내도 전자서명법과 의료법에 근거하여 개인정보의 보호항목을 추가하고 전자의무기록에 전자서명의 적용을 의무화하였다. 일반적으로 전자의무기록의 접속하기 위해서 의료인은 스마트카드를 카드리더기에 삽입하고 공인인증서를 이용하여 인증하는 방법 등을 사용하고 있다.

환자의 진료정보를 작성한 의료행위에 대하여 의료인의 서명이 필요한 경우 전자서명으로 대체하여 전자의무기록의 신뢰성을 확보하고 있다. 공인인증서 기반의 인증방식은 전자서명법의 법적효력과 의료행위의 신뢰성을 확보할 수 있지만, 개인키 관리의 취약점과 고의적인 권함위임에 대해 감시할 수 없는 한계가 있다.

† 정 회 원 : 한국인터넷진흥원 인터넷침해대응센터 책임연구원
논문접수 : 2011년 6월 14일
수 정 일 : 1차 2011년 9월 5일
심사완료 : 2011년 9월 26일

본 논문에서는 전자의무기록 시스템의 효과적인 접근통제 및 보안강화를 위해 지문인식 기반 인증 모델을 설계하여 개인키 관리의 문제와 고의적인 권한위임을 차단하여 의료정보 유출 또는 의료사고가 발생하는 경우 책임소재에 대한 문제를 개선하고자 한다.

2. 기존 연구

2.1 전자의무기록 보안 요구사항

전자의무기록(EMR : Electronic Medical Records)은 종이 매체에 의해 기록돼 온 의료기록을 업무처리 방식이나 정보의 범위, 정보내용에 있어 변형 없이 동일하게 전산화를 통해 개선한 형태를 말한다. 따라서 환자의 진료행위를 중심으로 발생한 업무상의 자료나 진료 및 수술·검사 기록을 전산에 기반을 두어 입력·보관하는 시스템을 통칭한다.

따라서 전자의무기록은 전자적으로 수집, 관리, 사용, 전송되는 환자의 진료정보와 환자의 인적사항 등 개인정보와 직접적으로 연관된 정보를 처리하기 때문에 높은 수준의 보안이 필요하다. 현재 의료기관에서 운영하는 전자의무기록 시스템에서는 의료인의 신원확인을 위해 기본적으로 아이디와 비밀번호를 사용하고 있으며 주기적인 비밀번호 변경을 통해 일차적인 안전성을 확보하고 있다. 전자의무기록에 인증(Authentication), 무결성(Integrity), 비밀성(Confidentiality), 부인봉쇄(Non-Repudiation)의 4가지 보안 요구사항을 제공하기 위해 의료법 제18조의 2(처방전의 작성 및 교부), 제21조의 2(전자의무기록)에 공인 전자서명 적용을 의무화하고 있다. 전자의무기록에 공인 전자서명을 적용하면 전자의무기록 작성 의료인의 신원확인, 진료내용의 위변조 방지, 기록한 진료정보의 부인방지를 제공한다[9].

2.2 공인인증서 기반 인증 모델

공인인증서 기반의 인증 모델은 의료인의 개인키로 생성한 전자서명을 검증함으로써 의료인의 신원을 확인한다. 의료인은 전자의무기록 시스템에 접속을 위해 전자서명을 수행하며 시스템은 해당 인증서의 유효성, 인증서의 상태, 전자서명 검증을 통해 인증여부를 판별한다[2].

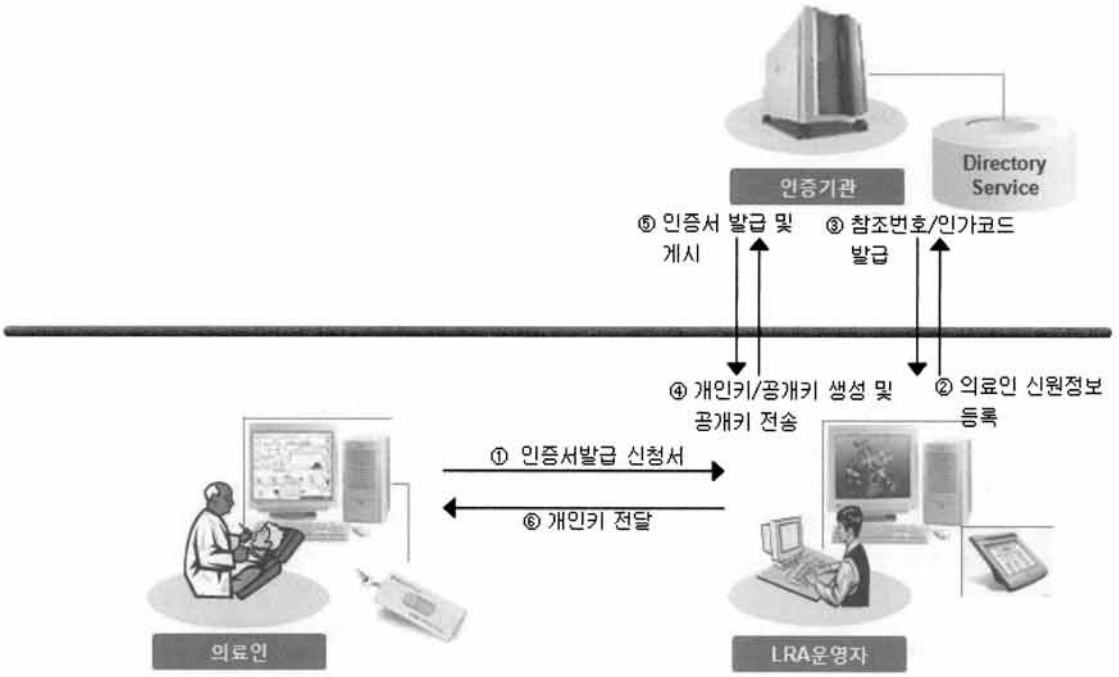
- EMR 시스템의 공인인증서 발급단계

전자의무기록은 전자서명법과 의료법을 준수하여 공인인증서를 발급 및 운영하며 발급단계는 (그림 1)과 같다.

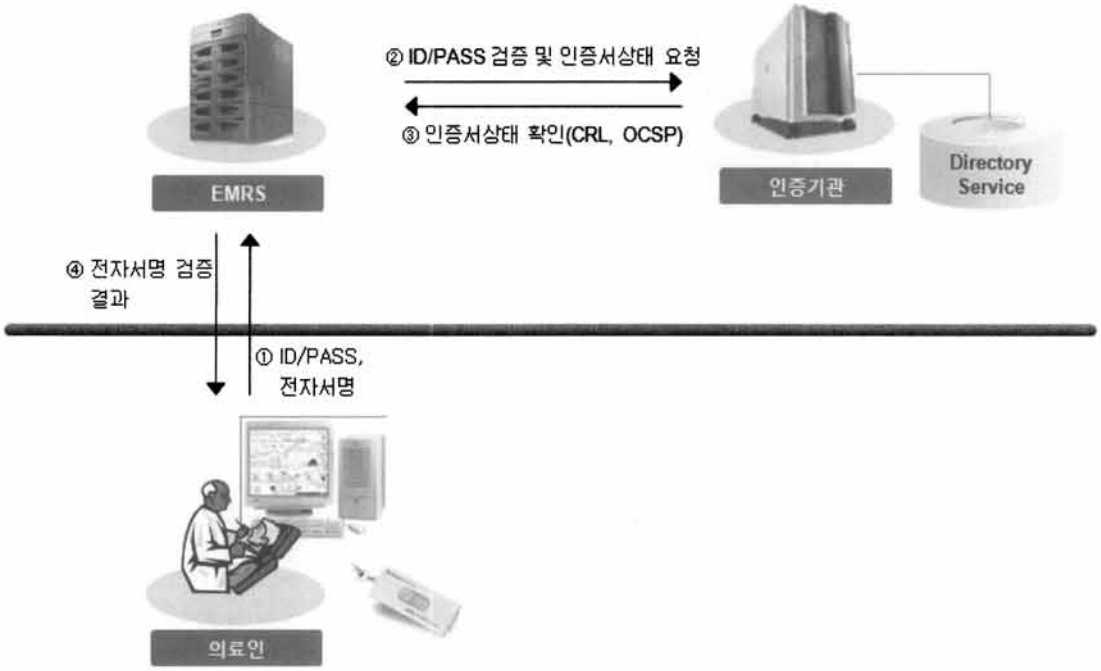
① 의료인은 의료기관내의 LRA(Local Registration Authority) 운영자에 대면확인을 통해 인증서 신청서를 제출한다.
② LRA 운영자는 공인인증기관에 등록 소프트웨어를 통해 의료인의 신원정보를 입력한다.
③ 인증기관은 인증서발급에 필요한 참조번호/인가코드를 생성하여 LRA운영자에게 송신한다.
④ LRA 운영자는 참조번호/인가코드를 이용하여 의료인의 개인키과 공개키를 생성하고 공개키를 공인인증기관에 전송하여 인증서 발급을 요청한다.
⑤ 공인인증기관은 LRA 운영자가 요청한 의료인의 인증서를 발급하고 디렉토리에 게시한다.
⑥ LRA 운영자는 의료인의 인증서를 공인인증기관으로부터 수신한다. LRA 운영자는 의료인에게 개인키와 인증서를 스마트카드/보안토큰에 저장하여 전달하고 개인키 분실에 대비하여 EMR 시스템내의 키관리시스템에 백업한다.

- EMR 시스템의 공인인증서 기반 인증단계

전자의무기록은 의료인에 대한 공인인증서 기반 인증단계는 (그림 2)와 같다.



(그림 1) EMR 시스템의 공인인증서발급 단계



(그림 2) EMR 시스템의 공인인증서 기반 인증단계

① 의료인은 개인키가 저장된 스마트카드/보안토큰을 의료단말에 삽입하거나 백업된 키관리시스템에서 개인키를 인출한다. 의료인은 EMR 시스템에 접속할 때 아이디/비밀번호, 전자서명, 인증서를 EMR 서버에 전송한다.

② EMR 서버는 일차적으로 수신한 아이디/비밀번호로 의료인의 신원을 확인한다. 신원확인이 완료되면 EMR 서버는 이차적으로 인증서의 유효성을 검증, 인증서의 상태 확인, 전자서명 검증을 순차적으로 수행한다. EMR 서버는 외부통신으로 공인인증기관에 인증서상태 요청을 한다.

③ 공인인증기관은 인증서의 상태 확인을 위해 인증서폐지목록(CRL : Certificate Revocation Lists) 메커니즘을 통해 일반적으로 1일 이내의 인증서 폐지 여부를 제공하며 온라인인증서상태확인(OCSP : Online Certificate Status Protocol)의 경우 실시간으로 인증서상태를 확인할 수 있는 정보를 제공한다.

④ EMR 서버는 검증된 전자서명에 대한 로그를 저장하여 감사기록에 대비한후 전자서명 검증결과를 제공한다. 의료인은 EMR 시스템의 접근이 허가되고 환자의 신원정보 및 진료기록이 가능하다.

2.3 공인인증서 기반 인증모델의 문제점

EMR 시스템의 공인인증서 기반 인증은 기본적인 보안 요구사항을 제공하지만, 다음의 문제점을 가지고 있다.

- 전자서명 비밀번호에 의한 보안수준 저하

개인키의 보안수준이 전자서명 비밀번호에 종속적으로 의료인이 전자서명 비밀번호를 기억하기 쉬운 단순정보 또는 신상정보를 조합하여 사용하는 경우 보안이 취약하게 된다.

- 실시간 인증서상태 확인의 부재[3]

EMR 시스템은 일반적으로 사설망 형태로 외부통신이 단절된 구조로 되어 있다. 안전한 EMR 인증을 위해서는 인증서 상태를 실시간으로 확인하는 OCSP방식을 채택해야 하지만 독립망 형태의 EMR 시스템의 한계에 의해 1일단위로 제공되는 CRL을 통해 인증서 상태확인이 가능하다. 만약 OCSP 방식을 채택한 경우 공인인증기관과 통신장애가 발생하는 경우 EMR 시스템의 접근이 안되어 긴급성을 요구하는 EMR 시스템에 부적합하다. 따라서 외부와 통신이 필요하지 않는 내부망에서의 인증방식이 필요하다.

- 개인키 관리의 취약점[6]

의료인은 개인키를 안전하게 관리해야 하지만 진료행위가 다양한 이동성을 요구하기 때문에 개인키를 다수의 의료단말기에 복사하여 사용함으로써 개인키 유출의 문제가 있다. 개인키 복사의 문제를 해결하기 위해 의료기관의 도입한 개인키 관리 시스템은 의료인의 이동성을 제공하지만 개인키를 중앙집중식으로 관리함으로써 보안위협은 더 증가하고 있다. 개인키의 안전한 관리를 위해 의료인 개인키를 스마트카드/보안토큰 등의 하드웨어에 저장하는 경우, 항상 휴대해야 하는 불편함이 있다.

- 개인키 위임의 취약점[10]

의료인은 인증서 발급단계에서 EMR 시스템의 폐쇄성으로 인해 LRA 운영자에게 발급을 위임하고 있다. 의료인이 업무적 편의성을 위해 다른 의료인에게 개인키를 위임하는 경우 전자의무기록 시스템은 위임행위를 감사할 수 없기 때문에 진료정보에 대한 부인방지가 취약하게 된다. 따라서 의료인이 개인키 위임이 불가한 인증방식이 필요하다.

3. 제안하는 지문인식 기반 인증 모델

본 논문에서 제안하는 전자의무기록 시스템에 대한 지문인식 기반 인증은 의료인의 지문 특징점으로 인증하는 모델을 설계하였다. 일반적으로 바이오인식은 신체적 특징인 지문, 얼굴, 홍채, 정맥 등을 식별하는 방법과 인체의 행위나 특성을 이용한 음성, 서명 등의 방법이 있다[1].

진료업무를 고려하여 인증방식이 편리하고 개인 식별이 우수한 지문인식을 채택하여 의료인의 인증 모델에 적용하였다. 지문인식은 등록과 인식의 2가지 단계로 구성된다. 지문등록 단계는 의료인의 지문샘플을 획득하여 특징점을 추출한 후 지문템플릿을 생성하고 등록하여 지문인식 단계에서 비교대상으로 사용된다[4-5]. 지문인식 단계는 의료인의 지문샘플을 획득하여 특징점을 추출한 후 지문등록 단계에서 등록된 지문템플릿과 비교하여 동일인 여부를 인식한다. 지문인식 방법은 사용목적에 따라서 식별과 인식으로 사용된다. 식별은 데이터베이스에 등록된 복수 지문템플릿과 비교하는 것이며, 인식은 등록된 단일 지문템플릿과 비교하여 정합 여부를 판별하는 방식이다[7-8].

3.1 바이오인식 시스템의 개요

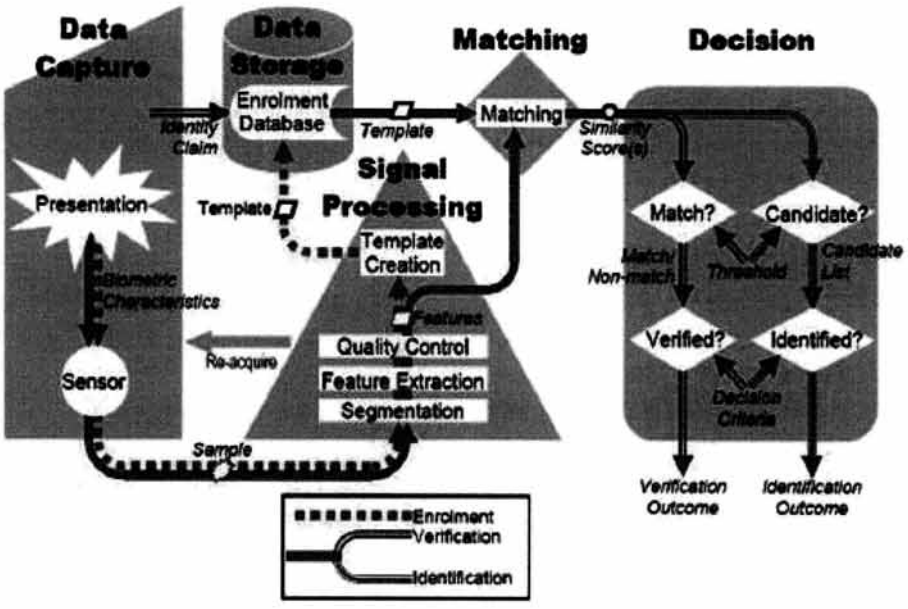
바이오인식 시스템은 사용자의 바이오정보에 기반하여 신분확인을 원하는 사용자가 본인여부를 확인하는 시스템을 말한다. 일반적으로 바이오정보로는 지문, 얼굴, 홍채, 손등정맥, 지정맥 등의 정적 바이오정보와 서명, 음성, 걸음새와 같은 대상자의 동적 바이오정보를 이용하는 것으로 나눌 수 있다. 이러한 바이오인식 시스템의 구성도는 국제표준기구(ISO)에서 (그림 3)과 같이 제정하였다.

바이오인식 시스템은 3가지의 구성으로 나누어져 있다. 등록(Enrollment)은 사용자의 바이오정보로부터 개인식별(Identification)과정이나 개인인증(Verification)과정에서 필요로 하는 바이오인식 템플릿을 생성하고 저장하는 과정을 의미한다. 개인식별과정은 주어진 바이오인식 템플릿에 대해서 이것이 누구의 것인지 신원을 밝히는데 목적이 있다. 이때 바이오인식 시스템은 저장장치내의 모든 바이오인식 템플릿과의 비교를 통하여 가장 유사도가 높은 대상자의 식별정보를 제공하게 된다. 이러한 이유로 이를 1:N 비교한다. 개인인증은 사용자가 본인의 바이오인식 템플릿과 함께 개인식별용 ID를 제시하게 되면, 주어진 바이오인식 템플릿에 대해서 이것이 주장하고 있는 본인이 맞는지의 여부를 판별하는데 목적이 있다. 이때 바이오인식 시스템은 저장장치내의 해당 ID의 바이오인식 템플릿과의 비교를 통하여 대상자의 인증여부를 결정하게 된다. 이러한 이유로 이를 1:1 비교라고 한다.

3.2 바이오정보 보호 방안

공인인증서와 같은 일반적인 사용자 인증방식은 인증정보가 유출되면 재발급을 통해 문제해결이 가능하지만, 바이오정보는 생체에 기반한 정보이기 때문에 한번 유출되면 문제해결의 방법이 어렵다. <표 1>과 같이 대한 문제를 해결하기 위해 바이오정보 보호를 위한 다양한 국제표준이 제정되었다.

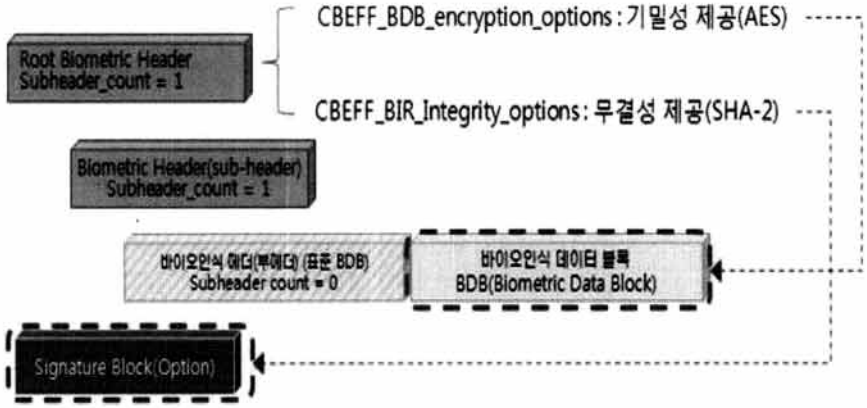
- ISO/IEC JTC1 SC37(Biometrics) W3에서 바이오정보 공통 교환형식(19785-1)가 제정되어 바이오정보 유형 및 기밀성 등의 제공이 가능하다.
- ISO/IEC JTC1 SC27(IT Security Techniques) WG5에서 바이오인식 보호 표준으로 개방형 네트워크에서의 바이오인증을 위한 기술규격(24761), 바이오정보 보호(24745)가 제정되었다.
- ITU-T SG17 Q.9(Security Study-Group Telebiometrics Question)에서는 네트워크 환경의 바이오인식 시스템의



(그림 3) 바이오인식 시스템의 구성도

〈표 1〉 바이오정보 보호 국제표준

표준명	주요내용
CBEFF(Common Biometric Exchange File Format) (ISO/IEC 19785-1)	바이오인식 공통 규격으로써, 바이오정보의 형태 뿐 아니라 기밀성의 보안 기능을 제공
Authentication Context for biometrics (ISO/IEC 24761)	ACBio는 개방적인 네트워크엣 바이오인증을 이용하기 위한 기술규격으로 데이터의 기밀성, 무결성을 제공
Biometrics Information Protection (ISO/IEC 24761)	개인식별 정보와 바이오정보의 시스템의 구성에 따르는 기밀성, 무결성, 가용성의 보안요구사항에 대한 표준안 제공
Telebiometrics Protection Procedures (ITU-T X.1086)	통신상에서 정보획득, 변조, 불법접근 등과 같은 다양한 위협으로부터 바이오정보를 보호하기 위해 기술적, 관리적 측면에서 보안대책 가이드라인 제시
바이오인증 프레임워크 (ITU-T X.bhsm 진행中)	바이오 보안토큰을 기반으로 인증을 하기 위한 프레임워크 개발
바이오인식 기반 원격의료 통합 프레임워크 ((ITU-T X.tif 진행中)	원격의료에서 바이오정보와 의료정보에 대한 통합 보안 프레임워크 개발



(그림 4) 바이오정보 보호(ISO/IEC 19785-1 적용)

위협에 대한 보호절차(X.1086), 바이오정보 보호 가이드라인(X.1086)이 제정되었으며, 바이오 보안토큰을 활용한 바이오인증 프레임워크(X.bhsm), 바이오인식 기반 원격의료 통합 프레임워크(X.tif)은 제정중에 있다.

본 논문에서는 (그림 4)와 같이, 전자의무기록시스템의 특성을 고려하여 전송되는 바이오정보는 이미지가 아닌 템플릿 기반으로 전송되기 때문에 CBEFF에서 지정한 기밀성을 위한 암호화로 AES 알고리즘과 무결성을 제공하기 위해 해쉬함수 SHA-2를 기반으로 보안성을 제공한다.

3.3 EMR 시스템의 지문인식 기반 인증 모델 설계

- EMR 시스템의 지문등록 단계

(그림 5)는 의료인이 EMR 서버에 지문템플릿을 등록하는 프로세스를 나타내었다.

① 의료인은 의료기관내의 LRA(Local Registration Authority) 운영자에 대면확인을 통해 지문등록 신청서를 제출한다.

② LRA 운영자는 EMR 시스템에 의료인의 지문등록 신청정보를 입력한다.

③ EMR 서버는 등록요청 받은 의료인의 참조번호/인가코드를 생성하여 LRA 운영자에게 전송한다.

④ LRA 운영자는 의료인에게 지문등록에 필요한 참조번호/인가코드를 전달한다.

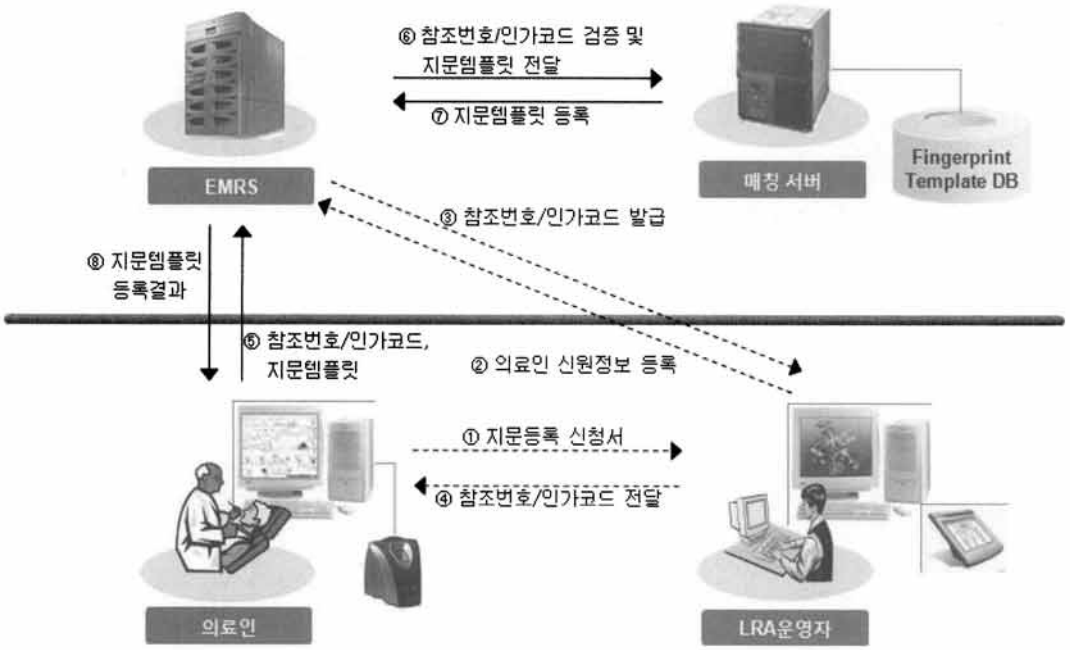
④ 의료인은 참조번호/인가코드를 입력하고 의료단말기의 지문센서에 지문을 스캔하여 지문샘플을 입력한다. 지문샘플은 품질을 검사하여 임계치 이상의 지문샘플만 전송되며 품질이 낮은 경우 지문을 재스캔해야 한다.

⑤ EMR 서버는 수신한 참조번호/인가코드를 확인하고 의료인의 계정정보와 지문샘플을 매칭 서버에 전송한다.

⑥ 매칭 서버는 수신한 의료인의 지문샘플에서 특징점을 추출하여 지문템플릿과 계정정보를 지문 데이터베이스에 저장한다.

⑦ 매칭 서버는 EMR 서버에 의료인의 계정정보와 지문템플릿의 저장된 결과를 전송한다.

⑧ EMR 서버는 의료인에게 지문등록 결과를 전송한다.

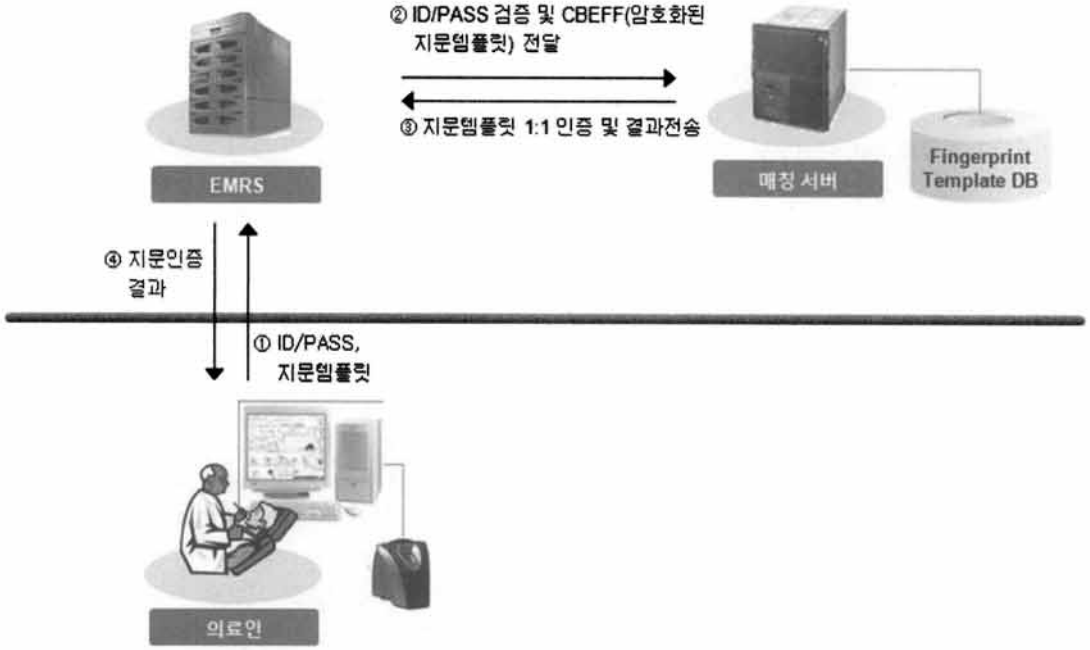


(그림 5) EMR 시스템의 지문등록 단계

- EMR 시스템의 지문인증 단계

지문인식 기반의 인증 모델은 전자의무기록 시스템 권한을 획득하기 위해서 의료인은 아이디와 비밀번호로 일차적인 인증을 수행하고, 매칭 서버에서 이차적인 지문인증을 통해 2-Factor 인증을 하여 보안수준을 높인다. 제안한 지문인증은 환자에 대한 진료, 처방의 중요업무에 의료인의 책임있고 신속, 정확한 진료를 지원할 수 있으며 비인가자에 대한 EMR 시스템의 불법적인 접근을 차단할 수 있다. (그림 6)은 의료인의 지문인증 단계를 나타내었다.

① 의료인은 지문센서에 스캔하여 지문샘플을 입력한다. 지문샘플은 품질을 검사하여 임계치 이상의 지문샘플만 전송되며 품질이 낮은 경우 지문을 재스캔해야 한다. 이때 바이오정보의 보호를 위해 지문이미지는 전송하지 않으면, 템플릿만을 전송한다. 이때 송부되는 지문템플릿은 CBEFF 포맷으로 변환되며, 기밀성을 위해 지문템플릿은 AES 암호화를 수행하고, CBEFF 전체에 대한 무결성은 SHA-2를 수행한다. 의료인은 아이디, 비밀번호, CBEFF (암호화된 지문템플릿)를 EMR 서버에 전송하여 인증요



(그림 6) EMR 시스템의 지문인증 단계

청을 한다. 이때 의료인의 아이디, 비밀번호는 SSL을 통해 보안이 제공된다.

② EMR 서버는 의료인의 아이디, 비밀번호를 확인한 후 매칭 서버에 CBEFF(암호화된 지문템플릿)을 전송하여 지문인증을 요청한다.

③ 매칭 서버는 의료인의 CBEFF(암호화된 지문템플릿)에서 SHA-2를 수행하여 전송된 CBEFF의 무결성을 검증한후, 서버에 저장된 AES 키를 지문템플릿을 복호화 한다. 지문샘플에서 특징점을 추출하고 해당 아이디에 해당하는 지문특징점과 1:1 매칭을 수행한다. 임계치 범위내에 속한 경우 해당 의료인은 동일인으로써 식별되며 임계치 범위를 넘는 경우 인증되지 않는다. 매칭 서버는 EMR 서버에 매칭결과를 전송한다.

④ EMR 서버는 의료인에게 지문인증 결과를 전송한다.

3.4 지문인식 기반 인증의 특징

제안하는 EMR 시스템의 지문인식 기반 인증은 기존의 공인인증 기반 인증과 비교하여 다음과 같은 특징을 가지고 있다.

- 의료인 인증의 편의성 제공

공인인증서 기반 인증은 의료인이 스마트카드/보안토큰에 개인키를 안전하게 관리해야 하도록 권고하지만 진료업무 특성인 이동성과 긴급성이 고려되지 않아, 개인키를 복사하여 사용함으로써 유출에 대한 위협이 있으며 빈번한 전자서명 비밀번호의 입력으로 인한 불편함이 있다. 또한 개인키를 분실하거나 전자서명 비밀번호를 기억하지 못하는 경우 공인인증서를 재발급해야 하는데 이러한 인증의 불편함은 EMR 시스템에 항상 접속 가능해야 하는 진료업무에 적합하지 않는다. 제안하는 지문인식 기반 인증은 전자서명 비밀번호 입력을 대신하여 의료인이 지문을 스캔함으로써 전자서명 비밀번호를 기억하지 않아도 되며 개인키를 스마트카드/보안토큰에 휴대해야 하는 책임이 없기 때문에 진료업무의 편의성을 제공한다.

- EMR 시스템의 사설망 구성에 적합

공인인증서 기반 인증은 의료인의 인증서 발급과 인증서 상태 확인을 위해 EMR 서버와 공인인증기관과 통신구간을 개방해야 하는 문제점이 있었다. 이는 EMR 서버에 대한 위협과 함께 통신부하를 증가시킴으로 의료시스템에 부적합한 인증방식이다. 제안하는 지문인식 기반의 인증은 사설망에 적합하도록 의료기관내에 매칭 서버를 구성함으로써 외부에 통신구간을 개방하는 문제점이 없기 때문에 EMR 시스템의 사설망의 특성에 가장 적합한 방식이다.

- 고의적 권한위임의 차단

공인인증서 기반 인증의 가장 중요한 문제점은 의료인이 개인키 생성에서부터 관리에 이르기까지 위임이 가능하다는 점이다. 이러한 문제점은 의료정보의 책임성을 제공하기 위해 채택한 공인인증 방식이 기술적인 문제로 인하여 고의적 위임이 가능하게 함으로써 신뢰성에 문제가 제기될 수 있다. 제안하는 지문인식 기반 인증은 의료인의 지문으로 인증하기 때문에 원천적으로 위임이 불가능하여 공인인증서 기반 인증의 가장 큰 위협인 권한위임을 차단하는 특징을 가지고 있다.

4. 실 험

본 제안의 실험을 위해서 100이상의 국내 의료기관을 대상으로 지문인식을 적용한 사례로 실험을 수행하였다. 실험에서는 의료인이 접속하는 EMR 시스템에 지문마우스를 이

(그림 7) 지문인증 기반의 EMR 로그인

〈표 2〉 EMR 전자서명 수행결과

단계	데이터 그룹	데이터 내용	알고리즘	데이터 크기	수행시간
①	전자서명 생성	전자서명 비밀번호 (8자리이상) 입력 및 전자서명 생성	RSA 2048, SHA-2	2,308 Bytes	4.80 s
②	전자서명 검증	전자서명 검증	RSA 2048, SHA-2		0.29 s
③	인증서 상태 확인	인증서상태 확인	CRL (Local 검색)	5,206 Bytes	0.51 s
총수행 결과				7,514 Bytes	5.60 s

〈표 3〉 EMR 지문인식 수행결과

단계	데이터 그룹	데이터 내용	알고리즘	데이터 크기	수행시간
①	지문템플릿 생성시간	지문스캔 및 특징점 추출	지문템플릿 추출	502 Bytes	2.94 s
②	CBEFF(암호화) 생성시간	바이오인식 공통형식 및 암호화	AES, SHA-2	8064 Bytes	0.37 s
③	CBEFF(암호화) 복호시간	지문특징점간 비교	1:1 매칭(한계 60점)	8064 Bytes	0.28 s
④	지문매칭시간	지문특징점간 비교	1:1 매칭(한계 60점)	502 Bytes	0.57 s
총수행 결과				8064 Bytes	4.16 s

용하여 3주간 테스트를 수행하다. 의료인의 데스트탑은 윈도우 XP, CPU 2.5 GHz, RAM 4G, HDD 500G 이며, 지문스캐너는 508 dpi, 200 pixel, 256 grayscale 스킨이 가능한 국내 제품으로 테스트 하였다. (그림 7)은 EMR 시스템의 지문인증을 나타낸다.

<표 2>는 기존의 공인인증서를 적용한 방식에 대해 100회의 수행결과를 반영하였으며, 인증서상태 확인은 CRL 매커니즘으로 로컬에 저장한 상태에서 테스트를 실시하였다. 수행시간은 전자서명 비밀번호 입력시간이 8자리 이상의 권고에 따라서 수행시간이 큰 것으로 나타났다.

<표 3>은 신규로 지문인증을 적용한 방식에 대해 100회의 수행결과를 반영하였으며, 지문인증실패는 제외하였다. 공인인증서 기반의 인증과 비교하여 수행시간이 개선된 것으로 파악되었으며, 전자서명 비밀번호를 대체하여 지문을 인식함으로써 사용자의 편의성이 증가되었다.

<표 3>과 같이 EMR에서 지문인증을 도입하는 경우, 공인인증서 기반의 인증에 비해 개인키 관리 불필요, 개인키 위임 방지, 내부망 적합성에서는 우수하지만 인식률과 법적 보장에서는 아직 부적합하다.

본 논문의 바이오인식 정보에 대한 프라이버시 보호 방법은 기존에 제안된 다양한 국제표준을 검토하였으며, 실질적으로 본 실험에 적용하기 위해서 CBEFF에서 제안하고 있는 바이오정보 암호화를 위해 AES 알고리즘과 CBEFF 형식에 대한 무결성을 제공하기 위해 SHA-2를 채택하여 수행하였다. 특히 지문원본 이미지는 저장하지 않는 것을 원칙으로 하였다.

지문인식률과 법적보장이 부적합 이유는 다음과 같다.

- 지문인식의 성능

지문인식은 완전한 인식률을 제공할 수 없다. 공인인증서와 같이 완전한 인식률을 제공할 수 없으며 특히 지문이 손상되거나 시간이 지남에 따라서 변형된 경우 등록된 지문템플릿을 사용할 수 없다.

- 법적효력의 부재

공인인증서 기반의 인증은 전자서명법과 의료법에 의해 법적효력을 가지고 있지만 지문인증은 법적효력을 부여받지 못하고 있다. 최근 금융권을 중심으로 공인인증서 이외의 OTP(One Time Password), 지문인식 등의 인증수단에 대해 효력확대를 고려하고 있어 법적효력의 문제를 해결될 것으로 전망된다.

따라서 제안하는 지문인식 기반의 EMR 인증 방식은 현 시점에서는 공인인증서와 결합하여 Two-Factor 인증으로 사용될 때 법적보장과 보안기능에 완전한 기능을 제공할 것으로 예상됩니다.

〈표 4〉 전자여권 보안기능 비교

보안기능 \ 인증방식	공인인증서	지문인식
개인키 관리 불필요	N	Y
개인키 위임 방지	N	Y
인증시 내부망 적합	N	Y
인식률	Y	N
법적보장	Y	N

5. 결 론

의료정보는 환자의 진료와 관련된 모든 정보를 의미하며 이는 개인의 프라이버시 중에서도 민감한 중요정보이다. 의료기관의 의료 및 질병에 대한 전산기록은 환자 개인에게 중요한 개인정보로써 안전하게 보호되어야 한다. 문서형태의 의무기록은 관리 및 보관상에 한계가 있기 때문에 마이크로필름 또는 광디스크 등에 저장하여 관리한다. 처방전달 시스템 환경에서는 환자의 인적사항, 처방내역, 검사결과 등이 텍스트 형태로 입력되어 진료에 활용하고 있다. 전자의무기록은 의료인이 진료기록을 정보처리 시스템에만 입력하여 법적효력을 가지는 가장 진보된 의료정보시스템이다.

개인의 의료정보를 관리하는 EMR 시스템의 인가는 전자의무기록시스템에 접속여부를 결정함과 동시에 해당 의료인에 대한 권한을 설정하는 가장 중요한 보안요소다. 기존의 공인인증서 기반 신원확인은 의료인의 진료정보를 전자문서 형태로써 의료기관내에 전송하거나 활용할 때, 진료기록의 임의로 수정되거나 변조되는 것을 방지하고 강화된 신원확인을 통해 진료기록의 신뢰성 증명하고 있다. 그러나 의료인이 개인키를 스마트카드/보안토큰에 보관해야 하는 문제와 의료인의 공인인증서 발급 및 인증서상태 확인을 위해 외부와 실시간 통신하여 EMR 시스템의 사설망 구조에 적합하지 않다. 또한 개인키의 생성에서 관리에 이르기까지 권한위임이 가능하지만 EMR 시스템에는 감사할 수 있는 기능이 없어 신뢰성에 문제를 가진다.

본 논문에서는 신뢰할 수 있는 전자의무기록 시스템을 확보하기 위하여 지문인식 기반 인증 모델을 제안하였다. 제안하는 모델은 의료인이 EMR 시스템 접속에 대하여 이차적으로 지문인식을 적용하여 강화된 신원확인과 부인방지를 제공한다. 제안하는 지문인식 기반의 인증은 의료인에게 개인키 관리의 문제를 개선하고 외부의 통신이 필요하지 않아 EMR 시스템의 사설망 구조에 적합한 인증방식을 제공한다. 특히 공인인증서 기반 인증의 가장 큰 문제점인 개인키 위임을 원천적으로 차단하여 EMR 시스템의 신뢰성을 향상시킬 수 있다.

향후 연구로는 의료인의 개인키와 지문정보를 결합하여 인증의 편리성과 보안기능을 동시에 충족할 수 있는 융합된 인증방식에 대한 연구가 필요하다.

참 고 문 헌

[1] Despina Polemi, "TTPs and biometrics for securing the payment of telemedical services." *Future Generation Computer Systems, Vol.15, Issue 2, pp.265-276,* 1999.

[2] Michael Fritscher, "Towards A Unique World-wide Digital Certificate," *Proceedings of the Fifth Americas Conference on Information Systems,* 1999.

[3] D.H. Yum and P.J. Lee, "Identity-Based Cryptography in Public Key Management," *In Proceedings of EuroPKI,* pp.71-84, 2004

[4] A. Kholmatov and B.A. Yanikoglu, "Biometric Authentication using Online Signatures," *In Proceedings of ISCIS,* pp.373-380, 2004.

[5] S. Krawczyk and A.K. Jain, "Securing Electronic Medical Records Using Biometric Authentication," *In Proceedings of AVBPA,* pp.1110-1119, 2005.

[6] A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method," *Pattern Recognition Letters, Vol.26, Issue 15, pp.2400-2408,* 2005.

[7] Chao LI, Yi-xian YANG and Xin-xin NIU, "Biometric-based personal identity-authentication system and security analysis," *The Journal of China Universities of Posts and Telecommunications, Vol.13, Issue 4, pp.43-47,* 2006.

[8] A. Bhargav-Spantzel, A.C. Squicciarini and E. Bertino, "Privacy Preserving Multi-Factor Authentication with Biometrics," *In Proceedings of Digital Identity Management, pp.63-72,* 2006.

[9] R. Agrawal and C. Johnson, "Securing electronic health records without impeding the flow of information," *International Journal of Medical Informatics, Vol.76, Issues 5-6, pp.471-479,* 2007.

[10] A. Salaiwarakul and M. Ryan, "Analysis of a Biometric Authentication Protocol for Signature Creation Application," *In Proceedings of IWSEC, pp.231-245,* 2008.

이 용 준

e-mail : yjlee@kisa.or.kr

1999년 강남대학교 전자계산학과(학사)

2001년 숭실대학교 컴퓨터학과(공학석사)

2005년 숭실대학교 컴퓨터학과(공학박사)

2005년~2006년 현대정보기술
바이오솔루션팀 과장

2007년~2009년 LG CNS 기술연구부문 부책임연구원

2010년~현 재 한국인터넷진흥원 인터넷침해대응센터
책임연구원

관심분야 : 인터넷침해대응, 전자신분증, 바이오인식, 공인인증