디지털산업정보학회 논문지 제5권 제3호-2009년 9월

지문인식 기반을 이용한 전자의무기록 시스템 접근제어에 관한 연구

백 종 현* · 이 용 준** · 염 흥 렬*** · 오 해 석****

A study of access control using fingerprint recognition for Electronic Medical Record System

Baek, Jong Hyun · Lee, Yong Joon · Youm, Heung Youl · Oh, Hae Seok

〈Abstract〉

The pre-existing medical treatment was done in person between doctors and patients. EMR (Electronic Medical Record) System computerizing medical history of patients has been proceed and has raised concerns in terms of violation of human right for private information. Which integrates "Identification information" containing patients' personal details as well as "Medical records" such as the medical history of patients and computerizes all the records processed in hospital. Therefore, all medical information should be protected from misuse and abuse since it is very important for every patient. Particularly the right to privacy of medical record for each patient should be surely secured. Medical record means what doctors put down during the medical examination of patients. In this paper, we applies fingerprint identification to EMR system login to raise the quality of personal identification when user access to EMR System. The system implemented in this paper consists of embedded module to carry out fingerprint identification, web server and web site. Existing carries out it in client. And the confidence of hospital service is improved because login is forbidden without fingerprint identification success.

Key Words : Electronic Medical Record System, Fingerprint Recognition

Ⅰ. 서론

현재 전자의무기록시스템은 사설망 내에서의 보안을 전제로 시행되고 있다. 사용자의 인증을 통한 로그인 방법으로 전통적인 아이디와 패스워드를 확인하고, 사용자의 이용에 대한 로그를 저장해 둠으로써 사용자의 사용 유무를 검사할 수 있도록 하고 있다. 이외의 방법으로는 아이디카드를 사용하여 사용자가 카드리더기에 자신의 개인 카드를 삽입하여 자신이 현 위치의 컴퓨터에서 작

* 한국정보보호진흥원 전자인증팀장
** LG CNS, 책임연구원(교신저자)
*** 순천향대학교 정보보호학과 교수
**** 경원대학교 컴퓨터공학과 교수

업을 할 것임을 인식시켜 인증하는 방법 등을 사용하고 있다. 사용자 인증은 환자의 진료카드를 작성한 이후, 의사의 서명이 필요한 부분에서도 요구되는데, 이때 로그인한 로그로써 사용자가 이 문서를 작성했는가를 판단하는데 사용한다. 만약 이 사용자가 잠시 자리를 비운 사이에 다른 사람이 일을 처리하더라도 알 수 없으며 사용자가 타인에게 아이디와 패스워드를 양도하는 문제도 발생할 수 있다[1-2].

병원정보의 유출은 개인 정보 유출과 사생활 침해의 측면에서 심각성을 가진다. 그러므로 전자의무기록 시스템은 보유 정보에 대하여 접근제어에 관한 통제 강화 등 보안의 강화가 필요하다. 미국의 경우 HIPAA (전자 의료보험청구법: Health Insurance Portability Accountability Act)는 의료 정보 비밀유지(사생활 정보 포함), 정보보안 표준 등의 규정을 마련하고 있다. 우리 정부도 이와 같은 시대 흐름에 맞추어 의료법에 개인정보의 보호항목을 추가하였으며, 공인인증기관 전자서명의 적용을 허가하였다. 본 논문에서는 병원정보시스템 중 전자의무기록 시스템의 효과적인 접근통제 및 보안강화를 위해 지금까지 개인인증을 위해 사용되고 있는 패스워드 또는 전자인증을 대신해 지문인증을 이용하여 전자의무기록 시스템의 접근제어를 통해 패스워드의 해킹 또는 대여로 발생할 수 있는 개인정보유출 또는 의료사고 발생 시 책임소재 구분 등의 문제들을 차단할 수 있는 방안에 제시하고자 한다[3-5].

II. 관련연구

2.1 공인인증서 기반의 인증

공인인증서 기반의 인증은 개인키의 소유자가 생성한 전자서명을 검증함으로써 신원을 확인한다. 개인키 소유자는 공인인증을 요청하는 시스템을 접근할 때 전자서명을 수행하며 시스템은 해당 인증서의 유효성, 인증서의 상태를 확인하고 전자서명을 검증한 후 인증여부를 판별한다.

공인인증서 기반의 인증은 다음과 같은 문제점을 가지고 있다.

첫 번째, 개인키의 보안 강도가 전자서명 비밀번호에 의존적이라는 문제가 있다. 개인키 소유자는 전자서명 비밀번호를 기억하기 쉬운 단순정보 또는 신상정보를 사용하는 경우가 많기 때문에 보안이 취약한 문제가 있다.

두 번째, 공인인증서 기반의 인증을 요구하는 시스템에 접근하기 위해서 사용자는 해당 개인키를 스마트카드 또는 토큰 등의 안전한 하드웨어에 보관하여 휴대해야 하는 불편함의 문제가 있다.

세 번째, 개인키 소유자는 키 위임을 할 수 있기 때문에 분쟁의 소지가 발생한다. 개인키의 분실 또는 고의적인 키 위임 행위에 대하여 확인할 수 있는 방법이 없다[6].

2.2 지문인식 기반의 인증

바이오 인식은 신체적 특징인 지문, 얼굴, 홍체, 정맥 등을 식별하는 방법과 사람의 행위나 형태적 특성을 이용한 음성, 서명 등의 방법이 있다. 이러한 생체 특징들을 이용한 인증방식 중 개인 내 변화가 적고 개개인별로 유일하기 때문에 지문 인식방식이 상대적으로 증가하고 있다.

지문 인식은 등록과 검증의 2가지 단계로 구성된다. 등록 단계에서 지문 샘플이 획득되며 유일한 특징점을 추출하여 지문 템플릿을 생성하여 저장한 후 인식 단계에서 사용된다. 인식 단계에서 지문 샘플을 획득하여 특징점을 추출한 후 등록 단계에서 저장된 지문 템플릿과 비교하여 동일인 여부를 인식한다[5].

지문 인식은 식별과 인식의 2가지 주요 목적을 가지고 있다. 식별은 시스템의 데이터베이스에 등록된 복수 템플릿과 비교하는 것이며 인식은 등록된 단일 템플릿과 비교하여 정합 여부를 판별하는 것이다[6].

지문 인식은 다음과 같은 문제점을 가지고 있다.

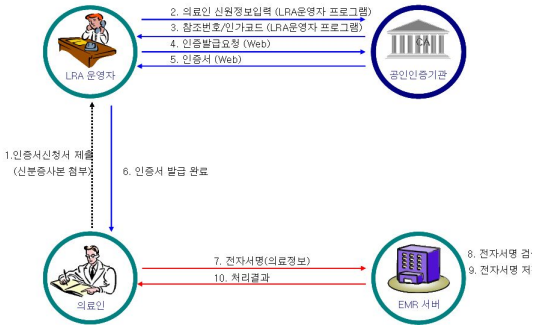
첫 번째, 지문 인식은 법적효력을 가지지 못하는 한계를 가지고 있다.

두 번째, 지문인식은 완전한 인식률을 제공할 수 없다. 지문인식 알고리즘 개선에 대한 연구가 지속적으로 연구가 되었으나 완전한 인식률을 제공할 수 없으며 특히 지문이 손상되거나 변형되는 경우는 등록된 지문 템플릿을 사용할 수 없다[7].

Ⅲ. 기존 시스템의 분석

전자서명 기반의 EMR 시스템 접근제어는 <그림 1>에 나타내었다.

(1) 의료인은 LRA운영자에 대면확인을 인증서신청서를 제출한다.
(2) LRA운영자는 공인인증기관에 신청 의료인에 대한 신원정보를 입력하고 결과값으로 참조번호/인가코드를 전달받는다.
(3) LRA운영자는 신청 의료인을 위임하여 개인키과 공개키를 생성한 후 공개키를 공인인증기관에 제출하여 인증서 발급을 요청한다.
(4) 공인인증기관은 LRA운영자가 요청한 신청 의료인의 인증서를 발급한 후 디렉토리에 게시한다.
(5) LRA운영자는 신청 의료인의 인증서를 공인인증기관으로부터 전송받는다.
(6) LRA운영자는 신청 의료인에게 개인키와 인증서를 전달하고 EMR 시스템에 접속할 경우 전자서명으로 인증하도록 한다.
(7) 의료인은 EMR시스템에 접근할 때 해당 아이디와 함께 전자서명 데이터와 인증서를 EMR 서버에 전송한다.
(8) EMR 서버는 전송된 인증서의 유효성과 인증서 상태를 확인한다. 이때 인증서폐지목록(CRL : Certificate Revocation Lists) 메커니즘을 이용하는 경우는 일반적으로 24시간 이내의 인증서 폐지 여부가 확인가능하며 온라인인증서상태확인(OCSP : Online Certificate Status Protocol)의 경우 실시간으로 인증서상태 확인이 가능하다.
(9) EMR서버는 검증된 전자서명 데이터에 대하 로그로 기록하여 추후 분쟁이 발생에 대비한다.
(10) 의료인은 전자서명 수행결과를 전송받는다.



<그림 2> 관리시스템의 구조도

전자서명 기반의 EMR 접근제어는 다음과 같은 문제점이 존재한다.

(1) EMR 시스템의 통신 위협

EMR 시스템은 일반적으로 사설망 형태로써 외부통신이 불가능한 구조로 되어 있다. 따라서 인증서 발급, 인증서 획득, 인증서 상태 확인과 같이 공인인증기관과 통신하는 구간에 있어서 직접적인 통신의 개방으로 인한 위협이 증가한다. 더하여 해당 통신에 장애가 발생 경우 시스템의 접근 자체가 불가능하기 때문에 의료시스템의 무장애 특성에 적합하지 않다[8].

(2) 개인키 관리의 불편함

의료인의 업무 자체가 이동성을 요구하기 때문에 개인키를 의료단말기에 복사하여 사용함으로써 개인키 관

리에 대한 위협과 함께 불편함에 대한 개선이 요구된다. 특히 개인키를 소지하지 않은 경우 재발급 절차를 수행해야 함으로 의료인에 대한 불편함을 개선되어야 한다[9].

(3) 개인키 위임의 문제

의료인은 인증서 발급 단계에서 EMR 시스템의 폐쇄성 때문에 LRA운영자에게 발급 자체를 위임하고 있다. 더하여 의료인은 다른 의료인 또는 간호사에게 개인키를 위임함으로써 의료분쟁의 여지가 존재한다. 따라서 의료인이 개인키를 위임이 불가능한 보안인증 방식이 요구된다[10].

Ⅳ. 지문인증 기반 의료시스템

본 논문에서 제안하는 지문인증 기반의 접근제어는 의료인의 지문정보의 특징점으로 인증하는 방식을 설계한다.

<그림 2>는 의료인이 EMR 서버에 지문 정보를 등록하는 프로세스를 나타내었다.

(1) 의료인은 지문센서에 본인의 지문을 스캔하여 지문이미지를 제공한다. 지문센서의 종류 및 알고리즘 방식에 따라서 다양한 이미지가 획득된다. 지문이미지를 서버에 전송하기 전 지문이미지의 품질을 확인한다. 등록된 지문이미지에 따라 인식률의 차이가 현저하기 때문에 이미지의 품질이 낮은 경우 수차례 획득이 가능하다.

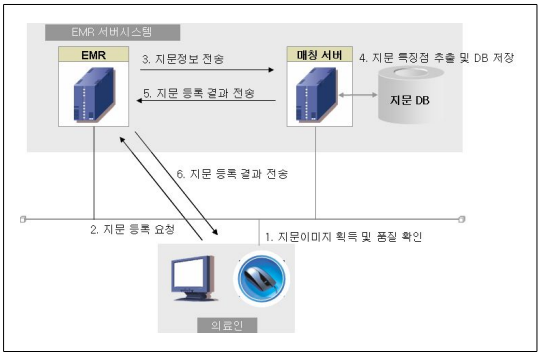
(2) EMR 시스템에 지문등록을 요청한다. 이때 의료인의 아이디, 패스워드와 함께 지문이미지를 서버에 전송한다. 지문이미지는 생체정보로써 프라이버시가 특히 요구되는 중요정보이기 때문에 보안채널이 요구된다.

(3) EMR 서버는 요청받은 의료인의 신상정보와 지문이미지를 매칭 서버에 전송한다. EMR서버와 매칭서버의 통신구간에서 서버간 통신보안이 요구된다.

(4) 매칭서버는 전송된 의료인의 지문이미지의 특징점을 추출한 후 신상정보와 함께 지문 DB에 저장한다. 지문이미지 또는 지문특징점을 저장시에는 DB 보안을 적용하여 의료인의 프라이버시를 보장해야 한다.
저장된 지문특징점 정보는 지문인증시에 1:1 매칭 또는 1:N 매칭 등에 사용된다.

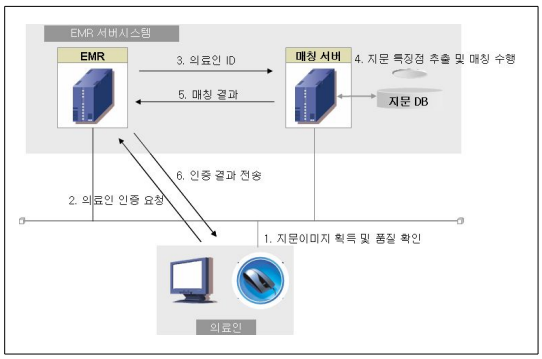
(5) 매칭서버는 EMR서버에 의료인의 신상정보와 지문정보가 저장된 결과를 전송한다.

(6) EMR서버는 의료인에게 지문정보 등록 결과를 전송한다.



<그림 2> 의료인 지문 등록 프로세스

본 제안하는 지문 인증 기반의 접근제어는 처방 업무 권한을 보유한 사용자가 비밀번호 인증을 수행하고 접근관리 서버에서 권한 부여를 하기 전에 강한 인증 요구를 위하여 다시 한 번 인증을 수행한다. 이러한 기능은 환자의 처방과 같은 중요한 업무에 지문인증 통합을 통하여 의료진의 책임 있고 신속, 정확한 처방을 지원할 수 있으며 비인가자에 대한 시스템의 불법적인 접근을 차단할 수 있다. <그림 3>은 의료인의 지문 인증 프로세스를 나타내었다. 지문인증 구간인 의료인, EMR서버, 매칭서버는 보안채널이 유지되고 있다.



<그림 3> 의료인 지문 인증 프로세스

V. 지문인증 기반 의료시스템

제안하는 EMR에서의 지문인식 기반의 인증은 기존의 전자서명 방식과 비교하여 다음과 같은 효율성을 가진다.

(1) 의료인의 편의성 제공

전자서명 방식은 의료인이 개인키를 안전하게 관리하도록 권고하고 있으나 실제 의료인의 업무상 이동성이 보장되어야 하며 빈번한 전자서명 비밀번호의 입력과 개인키 관리의 위협으로 인한 불편함이 존재하고 있다. 개인키를 분실하거나 전자서명 비밀번호를 기억하지 못하는 경우 인증서 재발급이 요구되는데 이는 의료시스템의 항상 접근 가능해야 하는 시스템에 적합하지 않는다. 제안하는 지문인식 방식은 전자서명 비밀번호 입력 대신 지문을 스캔함으로써 기억해야 하는 불편함과 개인키 관리의 책임이 없기 때문에 의료인의 편의성을 제공한다.

(2) EMR의 사설망 특성에 적합성 보장

기존의 전자서명 방식의 인증은 의료인의 인증서의 유효성과 상태를 확인하기 위해 EMR서버와 공인인증기관과 통신구간을 개방해야 하는 문제점이 있었다. 이는 EMR 서버에 대한 위협과 함께 통신부하를 증가시킴으로 의료시스템에 부적합한 인증방식이다. 제안하는 지문인식 기반의 인증은 사설망에 적합하도록 서버측에 매칭 서버를 구성함으로써 외부에 통신구간을 개방하는 문제점이 없기 때문에 EMR의 사설망이라는 특성에 가장 적합한 방식이다.

(3) 권한 위임 봉쇄

전자서명 방식 인증의 가장 큰 문제점은 의료인이 개인키 생성에서부터 관리에 이르기까지 위임이 가능하다는 점이다. 이러한 문제점은 의료분쟁을 방지하고 의료정보의 신뢰성을 제공하기 위해 채택한 공인인증방식이 합법적인 위임방식을 제공함으로써 신뢰성에 문제가 제기될 수 있다. 제안하는 지문인식 방식은 의료인의 지문을 특성으로 하기 때문에 원천적으로 위임이 불가능 하며 최근 위조지문에 대한 연구가 진척이 됨에 따라 가장 신뢰성있는 보안인증방식으로 평가받고 있다. 따라서 제안하는 지문인식 방식이 전자서명의 가장 큰 위협인 권한 위임을 봉쇄하는 특징을 가지고 있다.

VI. 결론

의료정보는 환자의 진료와 관련한 모든 정보를 의미하며 이는 개인의 프라이버시 중에서도 민감한 중요 정보이다. 최근 개인의 의료정보를 안전하게 보호하기 위한 법, 제도, 기술, 표준이 급속히 발전하고 있다. 의료기관의 의료 및 질병에 대한 전산기록은 환자 개인에게 있어서 민감한 사안이기 때문에 어느 분야의 정보 보다 안전하게 보호되어야 한다.

의료정보에 대한 시스템의 발전이 거듭하고 있으며 특히, 전자의무기록은 병원에서 사용되는 종이문서 대신 데이터를 전산매체에 저장하는 방식이다. 현재의 문서 의무기록은 일정기간 이후에는 관리 및 보관상에 한계가 오기 때문에 마이크로필름 또는 광디스크 등에 저장하여 관리한다. 처방전달시스템 환경에서는 환자의 인적사항,

처방내역, 검사결과 등이 텍스트형태로 입력되어 진료 중에 활용하고 있다. 이에 더하여 의사가 기재하는 진료 기록만을 전산에 입력하여 보다 진보된 전자의무 기록이 구축한 시스템이다. 중요 개인정보를 활용하고 있는 EMR시스템에서의 신원확인은 전자의무기록시스템에 접속여부를 결정함과 동시에 해당 의료인에 대한 권한을 설정하는 가장 중요한 보안요소이다.

기존의 전자서명방식의 신원확인은 의사의 처방전을 전자문서 형태로 병원의 해당부서로 전달하거나 진료기록의 경우 내용이 임의로 수정되거나 변조되는 것을 방지하고 신원확인을 이용해 내용을 증명하고 처방전을 기록한 의사의 신원을 확인하여 의료사고 시 발생할 수 있는 불필요한 분쟁을 막을 수 있다. 그러나 개인키를 의료인이 관리해야 하는 불편함과 EMR 시스템의 사설망 구조의 특징에 적합하지 않는다. 또한 개인키의 생성에서 관리에 이르기까지 타인에게 위임이 가능함으로써 EMR 시스템에 부적합한 한계를 가지고 있다

본 논문에서는 신뢰할 수 있는 전자의무기록시스템을 보장하기 위하여 의료정보시스템에 지문인식기술을 적용하는 모델을 제안하였다. 제안하는 모델은 의사, 간호사, 의료인의 접속에 대하여 지문인식을 적용함으로써 신원확인과 부인방지를 제공한다. 제안하는 지문인식 기반의 EMR의 인증은 사용자에게 개인키 관리의 불편함을 개선할 수 있으며 외부의 통신이 요구되지 않아 사설망 구조에 가장 적합한 보안인증을 제공한다. 특히 전자서명 인증 방식의 가장 큰 문제점인 개인키 위임을 원천적으로 봉쇄함으로써 EMR 시스템의 신뢰성을 향상시킬 수 있다.

따라서 현재의 전자서명 방식의 인증과 비교하여 전자의무기록 시스템에 지문인식기술을 적용함으로써 의료 분쟁 시 의사의 처방에 대하여 내력을 관리함으로써 신뢰할 수 있는 의료정보시스템을 제공할 수 있으며 불법적인 사용자의 접근을 차단함으로써 개인의료정보의 유출을 방지할 수 있다.

향후 연구과제로는 의료인의 지문정보에 대한 프라이버시 보호를 위한 방법론과 전자서명과 지문인식 기술이 융합할 수 있는 연구가 요구된다.

참고문헌

[1] 박두희, 송재영, 이남용, 전자의무기록 보안표준화에 관한 고찰, 숭실대학교, 2005.

[2] 니트젠, 지문인식기술 설명자료, 2005.

[3] 김학일, 생체인식기술의 7가지 질문, 인하대학교 정보통신공학부, 2005.

[4] 서정욱, 2005. 서울대학교 병원 의료정보화 사례보고, 2005.

[5] 김윤연, EMR사례분석, 2004년 대한의료정보학회 추계학술대회, 부산대학교, 2004.

[6] 김동수, 전자의무기록의 개념 및 도입현황, 2004년 한국병원경영학회, 연세대학교, 2004.

[7] MANSFILED, A.J., KELLY, G.P., CHANDLER, D.J. and KANE, J. Biometric Product Testing Final Report. 2002.

[8] Chu Yee Liau, Stephane Bressan, Kian-Lee Tan, “Efficient Certificate Revocation : A P2P Approach” in ASIAN 2002 Workshop on Southeast Asian Computing Research, 2002.

[9] Andrew Nash, William Duane, Celia Joseph, Derek Brink, “PKI : Implementing and Managing E-Security”, 2001, pp. 41-48.

[10] OECD, 2001. OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data.

논문접수일 : 2009년 5월 20일
수 정 일 : 2009년 8월 20일
게재확정일 : 2009년 9월 10일

■ 저자소개 ■

백 종 현
Baek, Jong Hyun

2001년 4월~현재 한국인터넷진흥원 전자인증팀장
ITU-T SG17 Q.6 의장
1998년 2월 순천향대학교 전자공학과(석사)
1996년 2월 순천향대학교 전자공학과(학사)

관심분야 : 정보보호, PKI, 유비쿼터스 보안
E-mail : jhbaek@kisa.or.kr

이 용 준
Lee, Yong Joon

2006년 9월~현재 LG CNS 기술연구부문 부책임연구원
2005년 2월 숭실대학교 컴퓨터학과(박사)
2001년 2월 숭실대학교 컴퓨터학과(석사)
1999년 2월 강남대학교 전자계산학과(학사)

관심분야 : 개인정보보호, 바이오인식, PKI
E-mail : bigman@lgcns.com

염 흥 열
Youm, Heung Youl

1990년 9월~현재 순천향대학교 정보보호학과 교수
ITU-T SG17 부의장/SG17 WP2 의장
1990년 2월 한양대학교 전자공학과(박사)
1983년 2월 한양대학교 전자공학과(석사)
1981년 2월 한양대학교 전자공학과(학사)

관심분야 : 인터넷보안, USN보안, IPTV보안
E-mail : hyyoum@sch.ac.kr

오 해 석
Oh, Hae Seok

2003년~현재 경원대학교 소프트웨어대학 교수
1982년~2003년 숭실대학교 정보과학대학 교수
1989년 2월 서울대학교 계산통계학과(박사)
1981년 2월 서울대학교 계산통계학과(석사)
1975년 2월 서울대학교 응용수학과(학사)

관심분야 : 정보보호, 멀티미디어, 데이터베이스
E-mail : oh@kyungwon.ac.kr