U-Healthcare 환경에서 환자정보보호를 위한 전자차트 부분 암호화 기법 설계

신 선 희* · 김 현 철** · 박 찬 길*** · 전 문 석*

A Design of Electronic Health Records Partial Encryption Method for Protecting Patient's Information on the U-Healthcare Environment

Shin, Seon Hee · Kim, Hyun Chul · Park, Chan Kil · Jeon, Moon Seog

〈Abstract〉

By using the U-Healthcare environment, it is possible to receive the health care services anywhere anytime. However, since the user's personal information can be easily exposed in the U-Healthcare environment, it is necessary to strengthen the security system. This thesis proposes the technique which can be used to protect the personal medical records at hospital safely, in order to avoid the exposure of the user's personal information which can occur due to the frequent usage of the electronic chart according to the computerization process of medical records. In the proposed system, the following two strategies are used: i) In order to reduce the amount of the system load, it is necessary to apply the partial encryption process for electronic charts. ii) Regarding the user's authentication process for each patient, the authentication number for each electronic chart, which is in the encrypted form, is transmitted through the patient's mobile device by the National Health Insurance Corporation, when the patient register his or her application at hospital.

Regarding the modern health care services, it is important to protect the user's personal information. The proposed technique will be an important method of protecting the user's information.

Key Words : U-Healthcare, Parital Encryption, Patient's Information

Ⅰ. 서론

언제 어디서나 질병의 예방, 진단, 치료, 사후 관리 등 보건의료 서비스를 제공하는 U-Healthcare는 유비쿼터스 헬스케어(Ubiquitous Healthcare)의 약자로서 1988년 마크 와이저(Mark Weiser)의 논문 "The Computer for the 21st century"[1]를 통해 IT 기술 분야에 처음 소개되었으며, 현재에는 차세대 컴퓨팅 환경을 의미하는 용어로 널리 통용되고 있다. 유비쿼터스 컴퓨팅은 "Aal

* 숭실대학교 컴퓨터공학과 교수(제1저자)
** 한국기술정보연구원 정보화전략팀
*** 한국사이버대학교 정보보안학과 교수(교신저자)

Space", "Aal Thca", "Aal Network", "Aal Device", "Aal Service"를 지원하는 네트워크 기반의 컴퓨팅 환경으로, 초창기 물리적 공간에 대한 한계가 있었으나 최근에는 모바일 컴퓨팅 개념이 추가되어 시공간을 초월한 자유로운 컴퓨팅 환경으로 발전하였다[2].

사용자는 유비쿼터스 컴퓨팅을 이용한 U-Healthcare 시스템을 통해 언제 어디서나 건강상태를 진단받고 그에 맞는 치료를 받을 수 있다. 또한 U-Healthcare 시스템은 인간의 평균수명 연장과 건강한 삶을 영위할 수 있도록 하는 보건의료와 IT 기술이 융합된 시스템이라 할 수 있다[3].

U-Healthcare 시스템은 사용자들로 하여금 시간적, 물리적 제약 없이 더 나은 의료 서비스를 제공한다는 점에서 편리성, 효율성, 영속성을 제공하고 보장한다. 그러나 정보 산업의 발전과 비례하여 이를 악용하는 보안 침해 사고 역시 증가하고 있다. 또한 U-Healthcare 시스템이 개인의 병력 및 건강상태와 같은 민감한 정보를 서비스 개체로 사용하기 때문에 해당 정보를 보호할 수 있는 방안이 필요하다. 특히 이렇게 민감한 정보의 악용에 대해서는 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"을 통해 강력한 규제를 가하고 있으나, 정보의 악용을 완전히 차단하기에는 한계가 있다[4]. 해당 정보가 유출되어 오남용될 경우 개인에게 육체적, 정신적으로 심각한 피해를 줄 뿐만 아니라 금전적인 피해가 발생하는 등 2차적인 문제를 발생시킬 수 있다. 그러므로 U-Healthcare 시스템의 안전성을 보장하고, 이를 지속적으로 발전시키기 위해서는 해당 정보를 보호할 수 있는 보안 기술이 필요하다.

본 논문은 U-Healthcare 환경에서 전자차트에 대한 무결성, 기밀성, 신뢰성, 가용성 및 부인방지의 보장을 목적으로 한다. 특히 본 연구에서는 전자차트 전체를 암호화하는 것이 아닌 중요한 정보만 부분 암호화함으로써 속도처리를 향상시켰으며 전자차트의 보안성 및 효율성을 강화하였다. 이를 위해 다음 세 가지의 주요 연구를 수행하였다.

첫째, 의료 통합 시스템을 제안하여 병원과 환자 모두에게 편리하고 안전한 시스템을 제공한다. 의료보험공단에서 환자 개개인과 병원의 정보를 저장하고 있으며, 병원은 의료보험공단에 접속하여 정보를 이용한다.

둘째, 전자차트 내 환자의 중요한 정보만 부분 암호화하여 전자차트의 로딩시간을 줄이고자 하였고, 주민등록번호 노출에 대한 안전성을 제공하여 환자의 개인정보를 보호한다.

마지막으로 의사가 환자를 진료할 때 환자는 의료보험공단으로부터 수신한 인증번호를 의사에게 전달함으로써 전자차트의 신뢰성과 보안성을 강화한다.

본 논문은 전자차트에 적용되는 암호화 기법 및 이에 대한 안전성을 기술하고, 새로운 형태의 통합 시스템을 제안한다.

본 논문은 다음과 같이 구성된다. 2장에서는 선행 연구로써 U-Healthcare, 의무기록 전산화에 대하여 살펴본다. 3장에서는 제안하는 내용으로써, 전자차트 부분 암호화 기법을 제안하고, 이를 구체화하기 위하여 부분 암호화 및 복호화 알고리즘, 전자서명에 대하여 기술한다. 4장에서는 실험 및 비교 분석으로써, 제안한 기법을 바탕으로 시스템의 프로토타입을 구현하고 기존 시스템과의 보안성 비교를 통해 안전성을 확인한다. 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

2.1 U-Healthcare

2000년대 초반부터 웰빙과 함께 U-Healthcare 산업이 각광을 받고 있다. 세계의 고령화가 진행되면서 일상적으로 건강관리를 받아야 하는 계층의 증가와 함께 세계적으로 건강에 관한 관심이 높아지고 있기 때문에 U-Healthcare 산업이 지속적으로 성장하고 있다. 세계의 고령화 진행속도를 살펴보면, 일본은 36년, 미국은 86년,

프랑스는 156년으로 나타났다. 이에 비해 한국은 고령화의 진행속도가 26년으로, 초고령 사회 도달 속도가 세계에서 가장 빠르다[5]. 또한 이에 따라 노인에 대한 보건의료 서비스의 수요가 급증하고 있다. <표1>은 통계청에서 발표한 주요국가의 인구고령화속도에 관한 자료이다. 2019년에는 노인의료비가 65세 이상의 노인이 전체 의료비를 상회할 것으로 예상되고 있다[6].

< 표 1 > 주요국가의 인구고령화 속도

구 분	도 달 연 도			소 요 년 수	
	(고령화사회/7%)	(고령사회/14%)	(초고령사회/20%)	7% → 14%	14% → 20%
한 국	2000년	2019년	2026년	19년	7년
일 본	1970년	1994년	2006년	24년	12년
미 국	1942년	2013년	2028년	71년	15년
프랑스	1864년	1979년	2020년	115년	41년

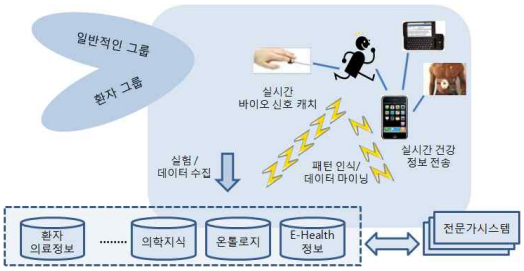
(자료: 통계청, 장래인구추정(2006)

질병구조의 다양화로 인한 만성 퇴행성 질환의 증가로 새로운 의료 기술이 요구되고, 신종 전염성 질병의 확산으로 인하여 국가적인 신속한 대응 체제가 필요시 되고 있다. 또한 국민들의 생활수준이 향상되어 질 높고 고급화된 다양한 보건 의료 서비스를 요구하며, 건강에 대한 관심의 증가로 각종 건강관리 서비스의 수요가 증가하고 있다.

이러한 현상으로 인해 작고 휴대 가능한 다양한 종류의 생체신호 센서가 출현하였고, IT 기술과 Healthcare 시장의 접목으로 U-Healthcare 산업이 지속적으로 발전하고 있기 때문에 언제 어디에서든 자신의 건강상태를 모니터링하고 개인화된 건강관리 서비스를 받을 수 있는 U-Healthcare 시대가 도래하고 있다.

<그림 1>은 사용자에게 부착된 생체신호 측정 센서가 무선 통신 네트워크에 연결되어 자신의 생체신호에 대하여 실시간으로 건강관리 서비스를 받는 전형적인 U-Healthcare 서비스 프레임워크를 나타낸다[5].

U-Healthcare 환경에서는 시간과 공간의 제약 없이 의료 서비스를 받을 수 있고 다른 산업과 마찬가지로 U-Healthcare의 발전은 정부와 개인, 학교, 병원과의 유기적인 관계 속에서 이루어지며 일반적으로 정보통신분야와 보건의료분야의 단순 연결이 아닌 관련된 모든 분야의 기술이 융합되어 서비스를 지원하는 "종합 의료 서비스 시스템"이다[7].



<그림 1> U-Healthcare 환경

2.2 의무기록 전산화

EMR은 기존의 종이 차트 시스템에서 탈피하여 환자의 진료기록을 관리 및 검색하는 시스템이다. 즉, 병원에서 사용되는 종이문서를 없애고 모든 데이터를 전산매체에 저장하는 방식이다. 종이 차트의 경우 관리 및 보관의 한계가 존재한다[8]. 이에 따라 종이 차트의 내용을 하드디스크 및 광디스크 매체 등에 수록하고 관리한다. 정부는 2002년 3월 의료법 개정안에서 "진료기록 등을 전자서명법에 의한 전자서명이 기재된 전자문서로 작성·보관할 수 있다"고 규정함으로써 전자의무기록 도입을 위한 법적 근거를 마련했다. 전자의무기록의 법적근거는 개정된 의료법 제23조 규정에 의한다[9].

① 의료인이나 의료기관 개설자는 제22조의 규정에도 불구하고 진료기록부 등을 「전자서명법」에 따른 전자서명이 기재된 전자문서(이하 "전자의무기록"이라 한다)로 작성·보관할 수 있다.
② 의료인이나 의료기관 개설자는 보건복지가족부령으

로 정하는 바에 따라 전자의무기록을 안전하게 관리·보존하는 데에 필요한 시설과 장비를 갖추어야 한다. <개정 2008. 2. 29>

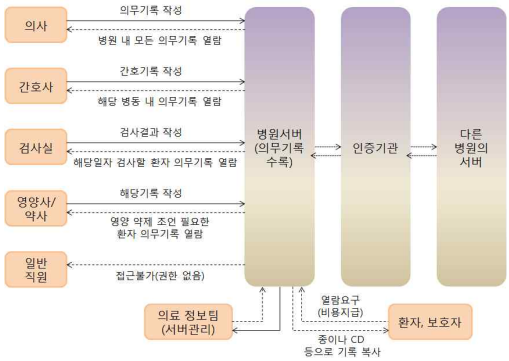
③ 누구든지 정당한 사유 없이 전자의무기록에 저장된 개인정보를 탐지하거나 누출·변조 또는 훼손하여서는 아니 된다.

환자의 의료 행위 시 작성되는 모든 형태의 자료는 전자차트 형태로 저장될 뿐만 아니라 처방전이나 보험, 영상기록 정보 등의 내용도 전자적으로 저장한다.

의료 기술과 IT 기술의 접목으로 인해 모바일이나 PDA, 노트북 등의 기기를 이용하여 환자를 진료하고, 환자는 통합된 전자의무기록 시스템과 처방 전달시스템에 의해 신속하고 정확한 의료 서비스를 이용할 수 있다.

EMR의 주요 내용은 환자의 기초정보부터 병력사항, 약물반응, 건강상태, 진찰 및 입원/퇴원 기록, 방사선 및 화상진찰 결과, 기타 보조연구결과 등이고 처방전달시스템인 OCS와 영상전송시스템인 PACS를 모두 포함하는 개념이다[9].

<그림 2>는 전자의무기록 개념도를 나타낸 것이다.



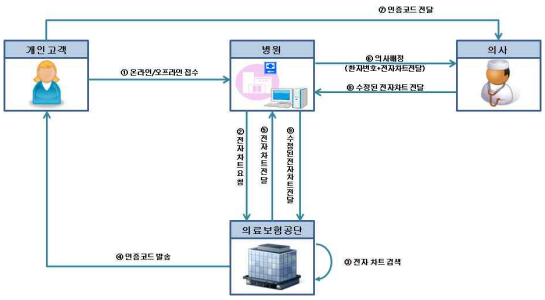
<그림 2> 전자의무기록 개념도

전자의무기록과 전자서명을 의료법이 허용함으로써 병원들은 의료정보화 사업을 꾸준히 진행하고 있다. 전자의무기록은 환자의 모든 정보를 종이차트 대신 전산화하는 제도로 국내에 도입한 이후부터 꾸준히 확산되고 있다.

Ⅲ. 제안하는 시스템

3.1 제안 시스템의 개요

본 논문에서 제안하는 시스템은 <그림 3>의 개념도와 같이 환자와 병원의 서버, 의료보험공단의 U-Healthcare 서버, 환자에게 배정되는 의사로 구성된다. 개인고객 즉, 환자는 의료보험공단과 병원에 가입이 되어 있어야 하고 병원과 의료보험공단 사이에 가입이 필요하다. 의사는 해당 병원 소속이어야 하고, 병원과 의사 사이는 서로 신뢰할 수 있다.



<그림 3> 제안 시스템의 전제 개념도

전자차트 부분 암호화 시스템은 다음과 같다.

과정① : 개인고객 즉, 환자는 병원에 온라인 또는 오프라인으로 접수한다.

과정② : 해당 병원은 의료보험공단에 접수 완료된 환자의 전자차트를 요청한다.

과정③ : 의료보험공단은 병원으로부터 접수된 환자의 전자차트를 검색한다.

과정④ : 의료보험공단의 전자차트 검색이 완료되면

해당 환자에게 인증번호를 발송한다.

과정⑤ : 의료보험공단은 전자차트를 요청했던 병원에 해당 환자의 전자차트를 전달한다.

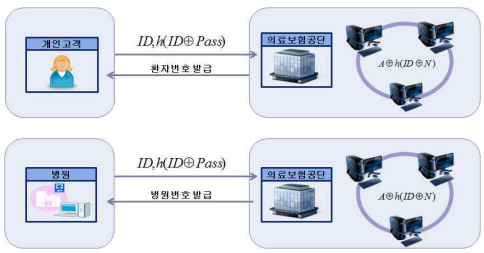
과정⑥ : 병원은 환자에게 의사를 배정하고 의사에게 환자번호와 전자차트를 전달한다.

과정⑦ : 의사는 진료가 끝나면 전자차트를 병원에게 전달한다.

과정⑧ : 병원은 의사로부터 수신한 환자의 전자차트를 의료보험공단에 전달한다.

3.2 전자차트 부분 암호화 기법

전자차트 시스템을 이용하기 위해서는 다음과 같은 요구조건을 고려하여야 한다. <그림 4>는 전자차트 시스템을 이용하기 위한 가입 절차를 나타낸다.



<그림 4> 가입 및 번호 발급 절차

개인고객 즉, 환자는 의료보험공단에 가입하게 되면 의료보험공단은 환자에게 고유한 환자번호를 발급해준다. 병원 역시 시스템을 이용하기 위해서 의료보험공단에 가입을 해야 하고 의료보험공단에서는 병원에게 고유한 병원번호를 발급한다.

환자가 의료보험공단에 ID와 패스워드를 입력하면 의료보험공단에는 환자의 ID와 패스워드를 해쉬한 값인 A와 의료보험공단 자체에서 생성한 랜덤 값, 환자의 ID를 해쉬한 값을 저장하고 의료보험공단은 환자에게 환자번호를 발급한다. 병원도 의료보험공단에 병원의 ID와 패스워드를 입력하면 의료보험공단에는 병원의 ID와 패스워드를 해쉬한 값인 A와 의료보험공단 자체에서 생성한 랜덤 값, 병원의 ID를 해쉬한 값을 저장하고 병원에게 고유한 병원번호를 발급한다. 등록된 환자의 확인 및 병원의 확인은 의료보험공단 자체에서 생성된 랜덤 값을 통해 확인할 수 있다.

환자가 병원에 내원하였을 때, 환자번호를 이용하여 접수하면 병원은 의료보험공단에 해당 환자의 전자차트를 요청한다. 전자차트 시스템은 개인의 사생활 보호와 환자의 정보보호를 위하여 환자의 신상 정보와 병명 등 중요한 정보만 부분 암호화한다. 또한 환자의 이름과 환자번호, 생년월일, 처방약 등의 정보를 제외한 신상 정보 및 처방전 등의 중요한 정보는 대칭키 암호화 알고리즘을 사용하여 암호화한다. <그림 5>처럼 전자차트는 중요한 정보만 부분 암호화한다.

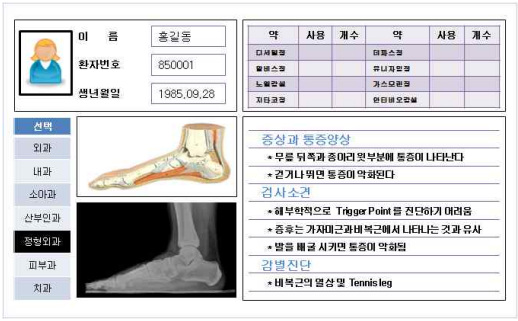
<그림 5> 전자차트 부분 암호화

부분 암호화 된 전자차트를 복호화하기 위해서는 의료보험공단에서 환자에게 보내주는 인증번호가 필요하다.

병원이 의료보험공단에 해당 환자에 대한 전자차트를 요청하고 의료보험공단이 병원에게 해당 환자의 전자차트를 전달해주는 과정에서 의료보험공단은 환자에게 부분 암호화되어 있는 전자차트의 인증번호를 해당 환자의 모바일 기기로 발송한다.

<그림 6>은 의료보험공단에서 환자의 무선 단말기로 인증번호를 전송하는 것을 나타낸다.

<그림 6> 환자에게 전달된 인증번호



<그림 7> 전자차트의 복호화

의료보험공단으로부터 전자차트에 대한 인증번호를 수신한 환자는 의사의 진료 시, 의사에게 인증번호를 전달한다.

환자에게 인증번호를 전달받은 의사는 부분 암호화되어 있는 전자차트에 인증번호를 입력한다. 전자차트는 환자가 전달한 인증번호가 정확하다면 복호화가 가능하다. <그림 7>은 환자의 인증번호로 복호화 된 전자차트를 나타낸 것이다.

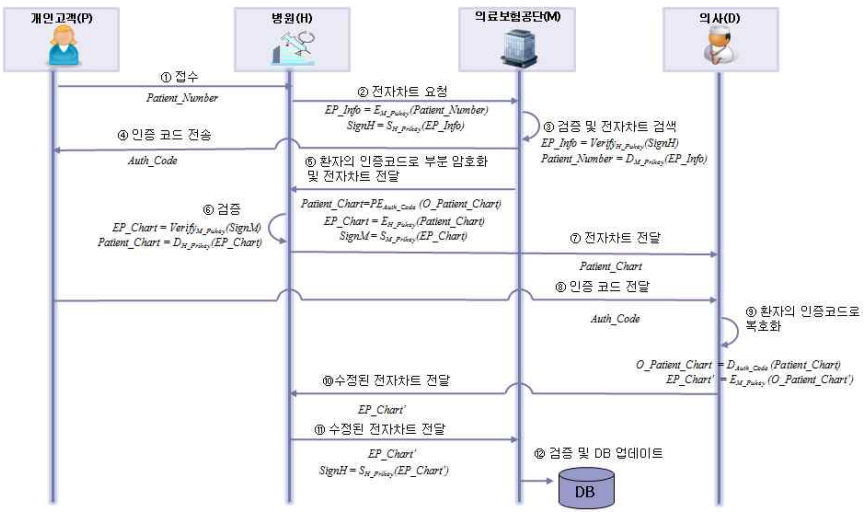
진료에 필요한 정보가 복호화되기 때문에, 환자는 의사로부터 진료를 받을 수 있다.

3.3 전자차트 부분 암호화 프로토콜

이 절에서는 제안하는 전자차트 부분 암호화 기법의 프로토콜 <그림 8>에 대해서 설명한다.

과정① : 환자는 자신의 환자번호(Patient_Number)로 병원에 접수를 한다.

과정② : 병원에서 의료보험공단의 공개키(M_Pukey)를 이용하여 환자의 번호를 암호화하고병원 자신의 개인키(H_Prikey)로 전자서명(SignH)을 수행한다.



<그림 8> 부분 암호화 프로토콜

$EP\_Info = E_{M\_Pukey}(Patient\_Number)$
$SignH = S_{H\_Prikey}(EP\_Info)$

과정③ : 병원으로부터 환자의 전자차트를 요청 받은 의료보험공단이 병원의 공개키로 전자서명을 검증하여, 해당 환자의 전자차트를 검색하고, 의료보험공단 자신의 개인키(M_Prikey)로 환자의 번호를 복호화한다.

$EP\_Info = VerifyH\_Pukey(SignH)$
$Patient\_Number = DM\_Prikey(EP\_Info)$

과정④ : 의료보험공단은 환자에게 인증번호(Auth_Code)를 전송한다.

과정⑤ : 의료보험공단은 환자의 전자차트(O_Patient_Chart)를 환자에게 전송하는 인증코드로 부분 암호화한다. 부분 암호화한 환자의 전자차트를 병원의 공개키로 전자차트를 암호화하고 의료보험공단 자신의 개인키로 전자서명을 한다.

$Patient\_Chart = PEAuth\_Code(O\_Patient\_Chart)$
$EP\_Chart = EH\_Pukey(Patient\_Chart)$
$Sign\ M = SM\_Prikey(EP\_Chart)$

과정⑥ : 의료보험공단으로부터 전자차트를 수신한 병원은 의료보험공단의 공개키(M_Pukey)로 전자서명을 검증하고, 병원의 공개키로 환자의 전자차트를 복호화 한다.

$EP\_Chart = VerifyM\_Pukey(SignM)$
$Patient\_Number = DH\_Prikey(EP\_Chart)$

과정⑦ : 병원은 의사에게 해당 환자의 부분 암호화 되어 있는 전자차트(Patient_Chart)를 전달한다.

과정⑧ : 환자는 의료보험공단으로부터 수신한 인증번호를 의사에게 전달한다.

과정⑨ : 의사는 병원에 수정된 환자의 전자차트(EP_Chart')를 전달한다.

과정⑩ : 병원은 수정된 환자의 전자차트를 병원 자신의 개인키로 서명을 수행한 후, 의료보험공단으로 전송한다.

EP_Chart'
$SignH = SH\_Prikey(EP\_Chart')$

과정⑪ : 의료보험공단은 병원으로부터 환자의 전자차트를 수신한 후 병원의 공개키를 이용하여 전자서명을 검증한다. 그 다음 의료보험공단의 개인키로 환자의 전자차트를 복호화하여 의료보험공단 데이터베이스에 저장한다.

$EP\_Chart' = Verify_{H\_Pukey}(SignH)$
$O\_Patient\_Chart' = D_{M\_Prikey}(EP\_Chart')$
$"Update\_DB"(O\_Patient\_Chart')$

Ⅳ. 실험 및 비교분석

본 논문에서 제안하는 시스템의 우수성을 평가하기 위하여 실험과 기존의 전자의무기록 시스템과의 비교 및 분석을 수행하였다.

4.1 실험 및 성능평가 환경

제안하는 기법의 성능평가를 위한 시스템은 Intel(R) Core(TM)2 Duo CPU @3.00GHz의 PC의 MS-Windows 7 Professional 운영체제 하에서 Visual C# 2008을 이용하여 구현하였다.

사용자 정보를 보호하기 위한 전자차트 전송에 사용할 키는 RSA 공개키 암호화 알고리즘으로 구현하였고, 기밀성을 보장하기 위해 AES 대칭키 암호화 알고리즘을 적용하였다.

제안하는 기법의 실험은 전자차트 내에서 중요한 부

분만 부분 암호화 및 복호화하는 기법으로 진행하였다.

환자가 병원에 내원하였을 때 병원은 의료보험공단에 환자번호를 전달하고 의료보험공단은 환자번호를 검색하여 해당 환자의 전자차트를 찾는다. 전자차트의 부분 암호화되어 있는 부분은 중요한 정보로 환자에게 전송되는 인증번호를 통하여 복호화되고 진료가 끝난 후 다시 암호화 한다.

인증번호는 의료공단서버에서 랜덤하게 생성되고 의료보험공단에서 발행하는 인증번호와 환자에게 전송한 인증번호가 같지 않다면 암호화 및 복호화가 되지 않는다. 의사가 올바른 인증번호가 입력한다면 암호화 및 복호화가 진행되고 환자의 진료 후에는 수정된 전자차트를 저장하고 의료보험공단으로 전송한다.

4.2 실험 결과

제안하는 기법의 암호화 및 복호화 과정은 환자번호를 선택하면 해당 환자의 기록이 나타난다. <그림 9>는 C#을 이용한 시뮬레이션 환경을 구축한 것으로 의료보험공단이 환자의 정보를 검색하기 전 화면이다.

<그림 9> 전자차트 메인 화면

사용자 부분은 환자의 사진과 환자번호, 환자의 이름 및 생년월일이 표시되고, 진단 부분은 X-ray사진이나 CT, MRI 사진을 포함한다. 그 외 의사의 처방전과 처방약을 표시한다.

다음은 암호화 상태의 전자차트를 복호화하는 의사코드(Pseudo code)이다.

```
Bitmap Decryption(A, B)
{
  if ( Width > 4096 || Height > 4096 )
  HowLength = 4;

  while(true)
  {
   if( i + HowLength <= Length )
  {
   i += HowLength;
   int[ ]x = int[(Width / HowBit) * (Height / HowBit)];
  }
   sub_x = null;

while(flag)
  sub_x = ToString(i, HowLength);
```

```
  for(x=HowLength - 1 to 0)
  {
   toString(Length - x - i - 1,1);
  }
   i += 1;
 if(count >= Length)
 {
  flag = false;
 }

  Color temp;

return gBitmap;
}
```

전자차트 암호화는 전자차트 내의 영상 정보에 암호화키를 더한 후 100(16)으로 모듈러 연산을 통해 나온 결과 값이 암호화된 색상 정보 값이다. 100(16)이라는 숫자는 RGB로 표현할 수 있는 모든 경우의 수를 의미한다. 먼저 전자차트에 대한 번호를 해쉬함수로 반복수행하여 암호화키를 생성하고, 생성된 암호화키와 전자차트의 각 픽셀에 색상 정보값과 연산하여 원본색상이 아닌 변형된 색상으로 전자차트를 암호화한다.

전자차트 복호화는 공개키로 암호화된 키를 사용자의 개인키로 복호화하여 암호화키를 획득한 후 암호화된 전자차트의 이미지에 복호화연산을 적용하여 복호화한다.

<그림 10>은 의사가 전자차트를 실행 했을 때의 화면이다.

<그림 10> 암호화 되어있는 전자차트

병원으로부터 환자번호와 환자의 전자차트를 수신한 의사는 해당 환자의 전자차트 내에서 환자번호를 선택하면 환자의 사진 및 환자 이름과 생년월일의 정보가 나타나고 처방전과 CT, MRI등의 사진은 암호화된 상태로 나타난다.

전자차트는 의료보험공단이 환자의 모바일로 보낸 인증번호를 의사가 입력하면 복호화한다.

<그림 11>은 전자차트의 복호화 수행결과 화면이다.

<그림 11> 복호화한 전자차트

환자는 X-ray 사진 및 환자 상태를 나타내는 전자차트의 처방 내용이 복호화되어 의사에게 진료를 받는다. 처방전 및 처방약의 내용은 수정이 가능하며 수정된 전자차트는 저장하고 부분 암호화를 진행한 후 의료보험공단으로 전송한다.

4.3 비교분석

현재 우리나라 EMR, OCS 및 PACS 도입에 있어 주요 쟁점으로는 전자차트 및 영상전송시스템에 관한 표준과 호환성, 신뢰성, 안전성 등이 있다. 전자차트는 환자에 관한 정보를 저장하고 있기 때문에 악용 가능성이 높다. 현재 사용하고 있는 전자차트는 암호화를 사용하지 않으며 환자의 주민등록번호만 알고 있으면 누구나 쉽게 볼 수 있다. 제안 시스템은 기존 시스템에서 취약했던 정보보안 부분을 강화하여 사용자에게 안전한 시스템을 제공한다. 또한 EMR 시스템과 PACS, OCS시스템을 통합하여 사용자에게 편리한 시스템을 제공한다. 다음 <표 2>은 기존 시스템과 제안하는 부분 암호화 한 전자차트 시스템의 특징을 비교한 표이다.

<표 2> 제안하는 시스템과 기존 시스템의 특징 비교

	B사	Y사	제안하는 시스템
특징	· OCS 연동 · 영상EMR · 입력 편의도구	· 일정관리 · 질병정보 · 검사관리	· 통합관리 · 부분 암호화 · 전자서명 · 사용자인증 · EMR, OCS, PACS 연동
장점	· 가이드라인 제공	· 가이드라인 제공	· 안전한 전송 · 사용자 정보보호 · 위·변조 어려움 · 전자서명 이용 · 사용자 인증
단점	· 사용자 정보 유출가능 · 위·변조 가능	· 사용자 정보 유출가능 · 위·변조 가능	· 편의성이 떨어짐

기존 전자차트 시스템의 특징을 보면 영상 EMR 시스템을 사용하여 편리한 UI를 제공하고 질병정보 등의 가이드라인을 사용자의 모바일이나 집전화로 제공한다. 또한 입력 편의 기능을 제공하여 사용자가 원하는 입력 기능으로 전자차트를 작성할 수 있도록 제공하고, 일정관리와 검사에 관한 내용을 주기적으로 제공한다.

제안하는 시스템에서는 EMR 시스템과 OCS, PACS를

연동하여 하나의 시스템으로 모든 기능을 사용할 수 있다. 뿐만 아니라, 전자차트를 부분 암호화하고 전자서명을 수행한 후에 공개키로 암호화하여 전송하기 때문에 환자의 정보가 노출될 위험이 적다. 또한 전자차트 전체를 암호화 한 것이 아니라 부분 암호화하였기 때문에 암호화 및 복호화 속도가 빠르다.

Ⅳ. 결론

본 논문은 EMR, OCS, PACS 등의 시스템 통합과 사용자 정보를 보호하면서 효율적인 전자차트 시스템을 사용하기 위한 기법을 제안하였으며 제안하는 프로토콜에 입각하여 시스템 프로토타입을 구현하였고, 성능평가를 위해 기존 시스템과의 비교 분석을 수행하였다.

본 논문에서는 환자의 주민등록번호를 노출하지 않기 위해 의료보험공단이 개별적으로 발급해주는 환자번호를 사용하였고, 병원이 의료보험공단에게 환자의 전자차트를 요구할 때 해당 환자의 환자번호를 공개키로 암호화한 후 서명과 함께 전송하여 보안성을 강화하였다. 성능부분에 있어서도 기존의 EMR, OCS, PACS 등과의 비교분석 결과 사용자의 프라이버시 침해와 전자차트 유출 부분에 대하여 안전하였다.

제안하는 기법은 중요한 정보의 부분에 부분 암호화를 하였고 사용자 인증과 전자서명을 사용하는 등의 보안기능을 추가하여 사용자 정보를 안전하게 보호하였다. 또한 부분 암호화를 복호화하기 위한 인증번호를 환자의 모바일로 전송함으로써 정확한 사용자 인증을 수행하였다. 모든 진료가 끝난 후엔 의사가 의료보험공단에게 수정된 환자의 전자차트를 암호화하여 전송함으로써 안전한 통신이 가능하게 하였다.

개인정보가 중요한 현재, 의료계에도 개인정보를 보호하는 연구가 필요하며 U-Healthcare 환경에서는 사용자 정보보호를 위한 보안기술의 개발 및 사용자들의 노력이 필요할 것이다.

참고문헌

[1] Mark Weiser, “The Computer for the 21st century”, Morgan Kaufmann Publishers Inc, pp. 933-940, 1995.

[2] 김경진, 홍승필, “e-Healthcare 환경 내 개인정보 보호 모델”, 한국인터넷정보학회, 인터넷정보학회논문지 제 10권, 제2호, pp. 29-40, 2009.

[3] 김미화, “디지털시대의 전자정부 구축에 따른 정보보호에 관한연구”, 정보보호21C 12월호, pp. 104-111, 2008.

[4] 대법원, “정보통신망 이용촉진 및 정보보호 등에 관한 법률”, 대법원, 2001.

[5] 손미란, “일본의 고령자복지와 고용촉진에 관한연구”, 배재대학교 석사학위논문, 2005.

[6] 김지희, “유비쿼터스 사회에서의 노인 생활혁신 방안”, 이슈리포트 05-04호, 2005.

[7] 한국전산원, “유비쿼터스 시대의 생활, 교육, 문화 서비스 발전방안연구”, 한국전산원, 2004.

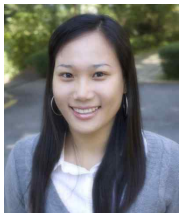
[8] 윤석권, “환자관리를 위한 EMR 관리 System”, 한국정보기술학회, 한국정보기술학회논문지, 제 4.

[9] 보건복지부, “의료법”, 보건복지부, 2008.

[10] 김신효, 송지은, 정명애, 정교일, “의료정보화 및 보안 기술 표준화 동향”, ETRI, 전자통신동향분석 제 21권, 제 6호, 2006.

[11] 채영문, “e-Heath 산업육성을 위한 정책제언-강원도 원격의료사업을 중심으로”, 연세대학교 보건대학원, 2005.

■ 저자소개 ■



신 선 희
Shin, Seon Hee

2009년 9월~현재 숭실대학교 컴퓨터학과 석사과정
2008년 2월 상지대학교 컴퓨터공학과

관심분야 : 네트워크 보안, U-Healthcare
E-mail : seonhee0928@hanmail.net

김 현 철
Kim, Hyun Chul

2009년 5월~현재 한국기술정보연구원 정보화전략팀 선임연구원
2009년 2월 숭실대학교 컴퓨터과학과 (공학박사)
2005년 2월 경원대학교 전산계산학과(석사)
2003년 2월 인제대학교 정보컴퓨터학부

관심분야 : 공전소, DRM, 보안 정책 및 전략
E-mail : dmzpolice@kisti.re.kr

박 찬 길
Park, Chan Kil

2010년 2월~현재 한국사이버대학교 교수
2006년 2월 숭실대학교 컴퓨터과학과 (공학박사)
1995년 2월 서울산업대학교 전산계산학과(석사)

관심분야 : DRM, 네트워크보안, 이동통신보안
E-mail : ckpark@mail.kcu.ac

전 문 석
Jun, Moon Seog

1991년 3월~현재 숭실대학교 컴퓨터학과 교수
1989년 2월 University of Maryland (전산학박사)
1986년 2월 University of Maryland (전산학석사)
1981년 2월 숭실대학교 전산학과

관심분야 : 네트워크 보안, U-Healthcare
E-mail : seonhee0928@hanmail.net

논문접수일 : 2010년 7월 6일
수 정 일 : 2010년 9월 1일
게재확정일 : 2010년 9월 7일