다중 인증 기술을 이용한 의료정보 보호시스템

김진묵* · 홍성식**

요 약

최근 들어 스마트폰과 유비쿼터스 컴퓨팅 기술의 발전으로 인해 U-헬스케어 서비스에 대한 이용 요구가 급격히 증가하고 있다. 더욱이 스마트폰을 이용한 의료정보시스템에 대한 접근과 사용 요구도 급격히 증가하고 있다. 의사들이나 환자들이 스마트폰을 이용해서 의료정보시스템에 아무 곳에서나 쉽고 빠르게 접근해서 의료 서비스를 제공 받을 수 있는 장점을 갖는 것과 달리 의료정보들에 대한 사생활 보호문제, 위치정보 노출문제, 개인정보 침해 등과 같은 보안 문제가 발생할 가능성이 높아졌다. 그러므로 본 연구에서는 의료 근로자들이 스마트폰을 사용해서 의료정보시스템에 접속하여 환자들에 대한 의료정보들을 기록, 저장, 수정, 관리할 때 발생할 수 있는 보안 문제들로부터 안전한 의료정보 보호시스템을 제안하고자 한다. 제안시스템에서는 의료 근로자들이 의료정보시스템에 접근 시 GOTP를 추가로 SMS로 전달받아 추가 인증 단계를 거침으로써 신분 위조 공격을 차단할 수 있도록 하였다. 그리고 제안시스템에서 사용자와 의료정보시스템 사이에 송·수신하는 모든 정보들을 스마트폰에서도 처리가 가능한 가볍고 빠른 암호 알고리즘을 적용함으로써 비밀성, 무결성, 위치정보 노출, 개인정보 침해 등에 대해서 방지할 수 있다.

A Protection System of Medical Information using Multiple Authentication

Jin-Mook Kim* · Seong-Sik Hong**

ABSTRACT

Recently, A utilization request of the U-Healthcare services are increasing rapidly. This is because the increase in smartphone users and ubiquitous computing technology was developed. Furthermore, the demand for access to and use of medical information systems is growing rapidly with a smartphone. This system have the advantage such as they can access from anywhere and anytime in the healthcare information system using their smartphone quickly and easily. But this system have various problems that are a privacy issue, the location disclosure issue, and the potential infringement of personal information. this problems are arise very explosive. Therefore, we propose a secure information security system that can solve the security problems in healthcare information systems for healthcare workers using smartphone. Our proposed system, doctors record, store, modify and manage patient medical information and this system would be safer than the existing healthcare information systems. The proposed system allows the doctor to perform further authentication by transmitting using SMS to GOTP message when they accessing medical information systems. So our proposed system can support to more secure system that can protect user individual information stealing and modify attack by two-factor authentication scheme. And this system can support confidentiality, integrity, location information blocking, personal information steal prevent using cryptography algorithm that is easy and fast.

Key words : U-Healthcare service; Medical system; Security services; Authentication; GOTP

접수일(2014년 11월 17일), 수정일(1차: 2014년 12월 29일)
게재확정일(2014년 12월 31일)

* 선문대학교 / IT교육학부
** 혜전대학교 / 인터넷보안과, 교신저자

1. 서 론

의료정보시스템이란 의료 행위들을 지원하기 위해서 EHR(Electronic Health Records)을 중심으로 한 전산시스템을 말한다. 최근에는 유비쿼터스 컴퓨팅 기술들과 스마트폰이 기존의 의료정보시스템에 추가됨으로써 의료관계자들은 언제, 어디서나 환자의 정보에 접근하여 의학적으로 필요한 예방, 진단, 치료 및 사후관리를 위한 행위를 할 수 있는 U-헬스케어서비스를 제공할 수 있다[1].

하지만 U-헬스케어시스템을 위해서 반드시 선행하여 해결해야만 하는 것이 있다. 바로 보안 서비스에 관한 문제이다[2, 6] 일반적으로 유·무선 네트워크 환경에서 제공하는 서비스들에 관해서 선행해야 할 대표적인 문제는 사용자 인증(User Authentication)과 서비스 인가(Service Authorization)이다. 하지만 의료정보시스템은 유·무선 네트워크에서 동작한다는 특성뿐만 아니라 사용자 개인정보와 의료 행위에 관한 민감정보들을 다루기 때문에 그 중요성이 매우 높다[7]. 하지만 지금까지 스마트폰을 사용해서 편리하게 U-헬스케어시스템을 사용할 수 있도록 적합한 보안서비스를 제공하지 못하고 있는 실정이다[3, 4, 5, 8].

그러므로 우리는 앞서 나열한 의료정보 시스템이 갖는 특성들과 스마트폰 환경과 상호 동작하는데 문제가 발생하지 않도록 다중 인증기술을 이용한 의료정보 보호시스템을 제안하고자 한다. 본 연구에서 제안한 다중 인증 기술을 사용함으로써 스마트폰 환경에서 기존의 의료정보시스템에 접속하여 개인정보와 의료행위에 관한 민감정보들을 처리하는 과정 중에 사용자 신분위조, 의료행위에 대한 위변조 공격 등을 사전에 막을 수 있음을 보이고자 한다.

2. 관련연구

2.1 의료정보시스템의 특징

앞서 기술한 것과 같이, 의료정보시스템이란 병원에서 의료 행위들을 수행함에 있어 발생하는 모든 정보들을 기록, 유지, 보관하고, 이를 바탕으로 향후 발생할 수 있는 의료적 절차들에 대해서 참고, 검토, 확인할 수 있도록 데이터베이스를 구축해 둔 것을 의미한다[12, 13]. 이런 의료 정보시스템은 일반적인 사무용 데이터베이스와 다르게 <표 1>에 나타낸 것처럼 4가지 특징들을 갖는다[5].

<표 1> 의료 정보시스템 특징

구분	설명
개인정보 포함	- 의료정보시스템이 다루는 정보에는 반드시 개인정보를 포함함 - 개인정보를 다루는데 비밀성, 무결성 서비스보장되어야 함
민감정보	-의료정보는 대부분 민감정보임 -민감정보는 안전하게 수집, 저장, 수정해야만 함
제한된 접근	- 의료 당사자만이 의료정보시스템에 접근 가능해야 함 - 사용자 인증 및 접근제어가 반드시 필요함
권한 기반	-의료 당사자라고 하더라도 권한에 따른 알맞은 접근제어가 이루어져야 함

지금까지 의료정보 시스템의 대표적인 4가지 특징들에 대해서 기술하였다. 앞서 기술한 4가지 특징들 이외에도 여러 가지 의료정보 시스템의 특징들이 추가적으로 더 있지만 이는 본 연구의 범위에 포함되지 않아 간략히 앞서 설명한 4가지 특징들만을 기술하였다.

2.2 의료정보시스템의 보안 위협요소들

본 연구에서는 다양한 보안 위협요소들 중에서 스마트폰을 사용해 의료 정보시스템에 접근하는 환경에서 발생 가능한 5가지에 보안위협요소들을 정리하여 <표 2>에 나타냈다[4, 9, 10, 11].

<표 2> 의료정보시스템의 보안 위협요소들

구분	설명
기밀성	- 스마트폰과 의료정보시스템 사이의 통신에 기밀성 위협 - 스마트폰 환경에 적합한 암호 알고리즘 요구됨
접근제어	- 의료 정보시스템이 갖는 역할 기반 접근제어의 부족함 - 규칙 및 역할 기반 하이브리드 접근제어 기법 요구됨
정보 공개	- 내·외부 전산근로자의 실수 또는 고의에 의한 정보 공개 위협 - 환자 병력 정보 접근 시 인증 및 접근제어 요구됨
위·변조	- 민감정보에 대한 위·변조 발생 가능성이 높음 - 내부자에 대한 로그 이력 관리 요구됨
가용성	- 의료 정보시스템은 공개된 시스템으로 다른 정보시스템들보다 보안성이 낮음

위에서 설명한 것 이외에도 여러 가지 보안 위협요소들이 존재하지만, 본 연구에서는 위의 5가지 요소들에 대한 해결방안을 모색하고, 이를 해결하기 위한 시스템을 제안하고자 함이다.

2.3 사용자 인증 기술들

(1) 사용자 아이디와 패스워드

사용자 인증을 위한 가장 기본적인 방법은 사용자의 아이디와 패스워드를 사전에 등록해 두고 확인하는 방법이다. 가장 쉽고 빠르고 정확한 방법이다. 하지만 이것만으로는 최근의 컴퓨팅 환경을 고려할 때 이것만으로는 보안 서비스를 제공하는데 부족하다.

(2) SMS 추가정보 입력

기존에 사용자 아이디와 패스워드 방식을 보완하기 위해서 제안된 Two-factor 기법 중에서 스마트폰이 도입되면서 가장 빠르고 효과적인 방법으로 제안된 것이 SMS(Shortest Message Service)이다. 이를 위해서 먼저 SMS 서버에서 6자리 이하의 숫자 혹은 문자 조합들을 생성해 사용자의 스마트폰으로 전송한다. 그리고 이를 수신한 사용자는 스마트폰 화면에 수신된 6자리 이하의 메시지를 사용자 인증 서버에 추가로 입력해 사용자 아이디와 패스워드만을 사용하는 것보다 추가적인 사용자 인증 정보를 확인함으로써 사용자 신분을 위조 또는 변조하는 것을 방지할 수 있다.

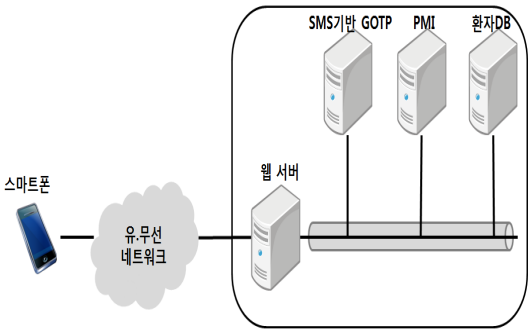
(3) GOTP(Graphical Onetime Password)

GOTP는 기존의 OTP(One Time Password)기법을 그래픽 정보를 활용해 처리하고자 하는 방법이다[14, 15]. OTP란 사용자 인증을 위해서 추가로 입력하는 정보이다. 기존의 사용자 아이디와 패스워드만으로는 부족한 인증 서비스를 보완하기 위해서 인증서버가 사전에 발급해 둔 정보 배열들 중에서 일부분을 입력받아 사용자 인증을 추가로 처리하는 기법이다.

3. 제안시스템

3.1 제안시스템 구조

(그림 1)은 본 연구에서 제안하는 스마트폰을 이용한 의료정보시스템의 전체구조를 나타내고 있다. 일반적으로 환자에 대한 정보를 검색하기 위해서 사용자는 첫 번째로 웹 서버에 접속해서 아이디와 패스워드 기반으로 일반적인 로그인을 수행한다.



(그림 1) 제안시스템 전체구조

그리고 환자에 대한 의료정보를 검색하기 위해서는 스마트폰 사용자가 지닌 권한에 따라 접속이 가능하도

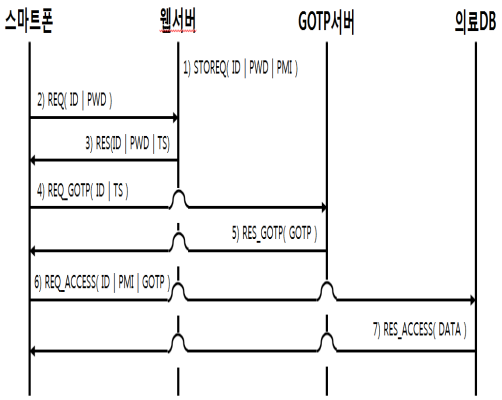
록 권한기반 PMI 서버의 인증을 추가로 수행한다.

추가로 민감정보를 열람 또는 확인하기 위해서는 환자 DB에 접속하기 전에 SMS를 기반으로 하는 GOTP 서버에 추가 인증 정보를 요청한다. GOTP서버는 추가 인증을 위한 그래픽 기반 원 타임 패스워드를 생성해 의료 근무자의 스마트폰으로 전송하고 이를 2분 이내에 서버에 전송해 검증토록 한다.

기존의 사용자 아이디와 패스워드만 사용하는 사용자 인증보다는 훨씬 안전한 다중 인증 기법을 사용함으로써 사용자 인증뿐만 아니라, 스마트폰을 사용해서 환자 데이터베이스에 접속을 요청한 경우에도 사용자가 지닌 권한을 기반으로 접속 가능한 데이터의 범위를 사전에 정책적으로 설정함으로써 권한기반 접근제어가 가능하도록 설계하였다.

3.2 제안시스템 동작절차

제안시스템은 (그림 2)와 같이 총 7개의 사용자 인증 및 서비스 권한 확인에 따른 접근제어 절차를 갖는다.



(그림 2) 제안시스템 동작절차

(1) 1단계 : 사용자 등록 및 사용자 권한 정보 저장

사용자는 사전에 웹 서버에 사용자 아이디와 패스워드, 그리고 사용자가 스마트폰을 사용해서 의료정보 시스템에 접근할 수 있는 권한 등급을 저장해 둔다.

(2) 2~3 단계 : 기초 사용자 인증

- 사용자는 사전에 등록해 둔 사용자 아이디와 패스워드를 전송해 사용자 인증을 요청하고 이를 웹 서버가 사전에 등록된 사용자 DB를 검토해서 인증 요청을 수행한다. 정상적인 사용자 인증 정보가 확인되면 웹 서버는 사용자 아이디와 함께 서버 타임스탬프 값을 응답한다.

(3) 4 ~ 5 단계 : GOTP 요청 및 추가 사용자 인증

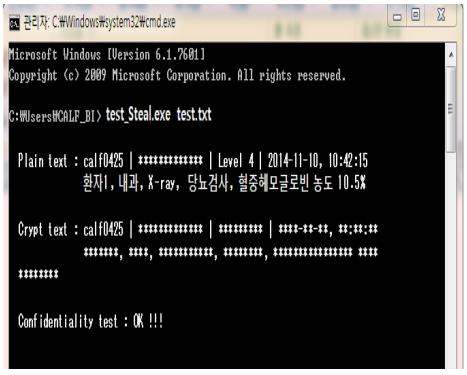
- 사용자는 자신이 민감정보를 열람 또는 사용하기 위해서 GOTP 서버에게 GOTP를 요청한 후, 사용자는 스마트폰에 수신된 GOTP 정보를 웹 서버에 입력해 추가 사용자 인증을 수행한다.

(4) 6~7 단계 : PMI 검증 및 환자 데이터 사용

사용자 추가 인증을 검토한 후, 의무 근로자는 자신이 가진 권한에 알맞은 PMI 정보를 추가로 전송해 환자에 대한 민감정보들을 등급에 맞게 처리한다.

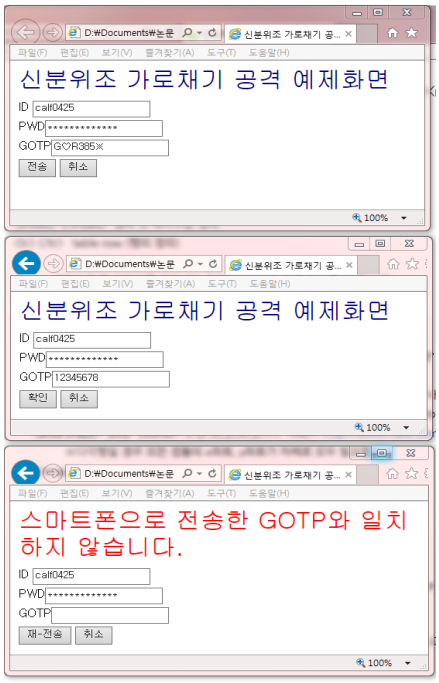
4. 실험 및 검토

사용자가 입력한 정보를 추가 GOTP와 함께 TS 값을 사용해서 SEED로 암호화를 수행함으로써 중간에 정보를 위조하거나 가로채어도 읽을 수가 없음을 (그림 3)에 나타냈다.



(그림 3) 기밀성 테스트 결과화면

그리고 제안시스템이 사용자 신분위조 공격을 막을 수 있음을 그림 4에 나타낸다. 그림 4에 나타낸 것처럼 사용자 아이디와 패스워드를 가로채어 입력하고 GOTP를 위조해서 입력하여도 정상적인 접근이 불가능함을 보였다.



(그림 4) GOTP 테스트 결과화면

5. 결 론

본 논문에서는 스마트폰을 이용한 의료정보시스템 접속 시 사용자 아이디와 패스워드를 사용해 1차 사용자 인증을 수행한 후, 사용자가 의료정보 중에서 민감정보에 대한 접근을 요청할 경우에는 추가로 GOTP 정보를 사용자에게 6문자 이상 8문자 이하의 그래픽 문자를 전송한다. 그리고 수신한 GOTP 정보를 웹 서버에 추가로 입력함으로써 다중 사용자 인증 서비스를 제공할 수 있도록 설계하였다.

그리고 사용자가 스마트폰을 사용해서 환자의 개인정보 및 의료정보, 그리고 민감정보에 접근하고자 하는 경우에도 사용자가 가진 접근 권한에 따른 PMI 정책에 알맞게 설계하였다. 이를 통해서 사용자 개인정보 침해, 사생활 침해, 위치정보 노출, 신분위조 공격 등을 사전에 방지할 수 있었다.

본 연구에서는 안드로이드 환경에서 동작하는 스마트폰에 대해서만 제안시스템을 설계하고 기밀성 및 무결성 서비스 확인만을 실험에서 수행하였다. 향후 본 연구를 확장해 의료정보 시스템에 대한 가용성과 추가 사용자 인증 시스템이 기존 사용자 인증 시스템과 비교해 우수성을 검토하는 연구를 수행하고자 한다.

참고문헌

[1] 윤은준, 유기영, “의료정보보호를 위한 RFID를 이용한 환자 인증 시스템”, 한국통신학회논문지, 제35권 제6호, pp.962-969, 2010년.

[2] 노시춘, 최진탁, “u-Healthcare 의료정보 시스템 네트워크 보안프레임워크 설계방법”, 융복합지식학회논문지, 제1권 제1호, pp.31-37, 2012년.

[3] 김경진, 홍승필, “e-Healthcare 환경 내 개인정보보호 모델”, 한국인터넷정보학회논문지, 제10권 제2호, pp.29-40, 2009년.

[4] 김봉회, 박진섭, “의료정보시스템 위협요소”, 한국멀티미디어학회 추계학술발표논문집, pp.68-76, 1998년.

[5] 김동수, 김민수, “u-Healthcare 환경에서의 정보보호 수준제고를 위한 보안 표준 개발”, IE Interfaces, Vol. 20, NO. 2, pp.177-185, 2007년.

[6] 김한나, “개인정보 누출의 시대, 개인의료정보의 보호”, 의료정책포럼, 제12권 제1호, pp.71-77, 2014년.

[7] 송지은, 김신효, 정명애, “u-헬스케어 서비스에서의 의료정보보호”, 정보보호학회논문지, 제17권 제1호, pp.47-56, 2007년.

[8] 전영주, “의료정보 유출의 문제점과 의료정보보호”, 한국컴퓨터정보학회논문지, 제17권 제12호, pp.251-258, 2012년.

[9] 송유진, 박광용, “의료데이터 공유 및 활용 서비스를 위한 보안/프라이버시 요구사항”, 정보보호학회논문지, 제20권 제3호, pp.90-96, 2010년.

[10] 이근호, 한상범, 서혜숙, 이상근, 황종선, “이동 Ad Hoc망을 위한 다중 계층 클러스터링 기반의 인증 프로토콜”, 정보과학회논문지: 정보통신 제33권 제4호, pp.310-323, 2006.

[11] 김한나, 이얼, 김계현, 이정찬, 이평수, “개인의료정보의 관리 및 보호방안”, 의료정책연구소 연구보고서 2013-04, pp.1-143, 2013.

[12] Anderson, Ross J and British Medical Association and others, “Security in clinical information systems”, London: British Medical Association, 1996.

[13] F. Cao, H. K. Huang, X. Q. Zhou, “Medical image security in a HIPAA mandated PACS environment”, Computerized Medical Imaging and Graphics vol. 27, Issues 2-3, pp.185-196, 2006.

[14] Chang, Ting-Yi, Cheng-Jung Tsai and Jyun-Hao Lin, 2012. "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices." Journal of Systems and Software, vol.85, no.5, pp.1157-1165, 2012.

[15] Dunphy, Paul and Jeff Yan, 2007. "Do background images improve Draw a Secret graphical passwords?." Proceedings of the 14th ACM conference on Computer and communications security. ACM.

[저 자 소 개]

김 진 묵 (Jin-Mook Kim)

1998년 2월 배재대학교 전자계산학과 공학사
2000년 2월 배재대학교 컴퓨터공학과 공학석사
2006년 2월 광운대학교 컴퓨터과학과 공학박사

email : calf0425@sunmoon.ac.kr

홍 성 식 (Seong-Sik Hong)

1989년 2월 광운대학교 전자계산학과 이학사
1992년 2월 광운대학교 전자계산학과 이학석사
2007년 2월 광운대학교 컴퓨터과학과 공학박사

email : sshong@hj.ac.kr