디바이스 인증 기반의 유·무선 통합 원격 의료 시스템

정회원 이 유 리*, 박 동 규**

A Telemedicine System Based on Device Authentication in the Wire and Wireless Environments

You ri Lee*, Dong gue Park** *Regular Members*

요 약

최근 우리 사회는 점차 고령화 사회로 접어들면서 건강한 삶과 삶의 질향상을 보장하는 "이상적인 의료 시스템"을 갈망하는 욕구와 더불어 첨단 IT 기술이 융합된 원격 진료 시스템을 선보이고 있다. 이러한 원격 진료 시스템이 안정적으로 서비스되기 위해서는 환자의 의료 정보 데이터가 보안 위협으로부터 안전을 보장 받을 수 있어야 한다. 특히 원격 진료 시스템에서 다루는 데이터는 환자의 질병 및 생명과 관련된 정보들임으로 데이터의 기밀성, 무결성, 인증, 부인봉쇄, 익명성, 감사기록 등의 보안 서비스는 의료 서비스의 신뢰성 및 안전성 보장을 위해서 반드시 지원 되어야 한다. 특히, 원격 의료 서비스를 제공 받기 위해 사용하는 모바일 단말기는 보안 위협이 높기 때문에 디바이스에 대한 인증은 필수적이라 할 수 있다. 따라서 본 논문에서는 유·무선 통합 환경에서의 신뢰있는 원격 의료 서비스 제공을 위하여 바이오 디바이스 인증 기반의 원격 의료 시스템을 설계한다.

Key Words : PKI, WPKI, PMI WPMI, Telemedicine, Device Authentication

ABSTRACT

Recently our society has a increasing desire for the ideal medical system to guarantee healthy and quality of life along with increasing number of elderly peoples, the new medical diagnostic system, powered by IT technology, is emerging. It is necessary to guarantee the safety of medical information data of patients against security threats, if we try to provide reliable telemedicine service. Considering the fact that the data, which is deal with telemedicine system, is highly related with patients' disease and life, the security service of data such as confidentiality, integrity, authentication, non-repudiation, anonymity, and inspection records needs to be supported to guarantee reliability and safety of medical services. Considering the mobile devices, which is used for telemedicine services, is vulnerable to security threats, the device authentication is considered as essential element for the services. The paper describes the design scheme of telemedicine services based on Biometric device authentication to provide reliable telemedicine services based on wired and wireless network environments.

Ⅰ. 서 론

정부는 의료 기관 선택권 확대와 시장 활성화를 위해 지난 2006년 원격 의료 시범 사업 추진 위원회를 구성하여 원격 의료 허용 방안을 지속적으로 검토해 왔다. 이는 최근 원격 의료 시범 사업으로 이어지고 있다. 원격 의료는 컴퓨터와 데이터 통신 기술을 이용하여 의료 서비스를 전달하는 기술을 통칭하는 말이다. 1970년대 원격 의료라는 용어가 처음 사용되었으며 이는 원거리에서 환자가 의료

* 순천향대학교 정보통신공학과 (thisglass@sch.ac.kr), ** 순천향대학교 정보통신공학과 (dgpark@sch.ac.kr)
논문번호 : 08054-0814, 접수일자 : 2008년 8월 14일

상담을 하는 활동만으로 제안되어 있었다.[1][2] 그러나 오늘날에서는 데이터 통신을 이용하여 의료의 제공, 진단, 자문, 의료 정보의 전달 그리고 건강 교육 등을 실행하는 모든 활동을 포함한다.

정부는 의료 기간 선택권 확대와 시장 활성화를 위해 지난 2006년 원격 의료 시범 사업 추진 위원회를 구성하여 원격 의료 허용 방안을 지속적으로 검토해 왔으며 현재에는 산간 오지나 낙도 등의 의료 사각 지대에 놓여있는 의료 취약 계층을 위한 의료 서비스 제공 및 응급 상황 발생 시 빠른 응급 처치를 위한 의료 서비스 제공을 위하여 원격 의료 시스템이 구축되고 있다. 이 시스템을 이용하면 환자와 환자에 대한 의료 정보가 먼 거리로 떨어져 있거나 시간적으로 많은 차이가 발생하여도 의료 정보 및 전문가의 조언을 원격으로 서비스 받을 수 있다. 그러나 원격으로 제공되는 의료 정보에 대한 보안 위협은 사람의 생명과 관련되는 정보이므로 다른 어떠한 정보보다 강력한 인증 체계가 필요하다. 현재 대표적인 원격 의료 시스템은 Ipath[3], OpenEmd[4], TeleCardio-FBC[5], Medintagra Web[6], Wireless Sensor Body Area Network(WSBAN)[7], CodeBlue [8]으로 이 시스템의 사용자 인증은 ID, Password 및 인증서를 사용하는 공개키 기반 구조를 사용하고 있다. 이러한 인증은 유·무선 통합 환경에 적합하지 않을 뿐 아니라 인증서의 개인키를 알고 있다면 본인이 아니더라도 원격 의료 시스템에 접근하여 서비스를 이용 받을 수가 있다.

따라서 본 논문에서는 유·무선 통합 환경에 적합하면서 지문, 홍채와 같은 인체 고유의 정보를 이용하여 시스템을 사용하는 사용자가 확실한 본인 인지를 인증하여 환자의 데이터 보안, 프라이버시 보장 및 신뢰 있는 원격 의료 시스템 서비스를 제공하고자 한다. 특히, 센서들에 의해 수집되는 정보들의 신뢰성 확보를 위하여 디바이스 인증 기반의 유·무선 통합 원격 의료 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구, 3장에서는 디바이스 인증 기반의 유·무선 통합 원격 의료 시스템 설계 4장에서는 제안 시스템과 기존 시스템을 비교 설명하고 끝으로 5장에서 결론과 향후 연구에 대해 설명한다.

Ⅱ. 관련 연구

유·무선 통합 환경에서의 원격 의료 시스템은 사람의 생명을 다루는 의료 정보 데이터를 다루게 된다. 따라서 원격 의료 시스템에서의 프라이버시, 접근제어, 무결성, 인증, 부인봉쇄의 다섯 가지 기본 보안 서비스를 제공하기 위하여 유선 환경에서의 공개키 기반구조, 무선 환경에서의 무선 공개키 기반구조를 기반으로 하고 사용자의 확실한 본인 인증을 위하여 바이오 인증 서비스를 사용하고 사용자의 속성 인증을 위하여 유선 환경에서의 권한 관리 기반 구조와 무선 환경에서의 무선 권한 관리 기반 구조를 기반으로 하는 유·무선 통합 환경에서의 원격 의료 인증 시스템의 구성은 다음 그림 1과 같다.[9]

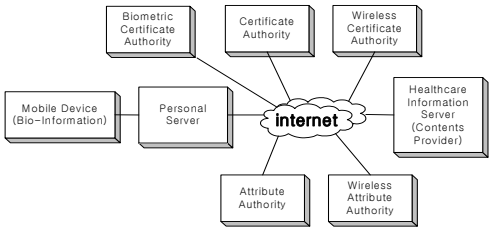

그림 1. 유·무선 통합 환경에서의 원격 의료 인증 시스템 구성도

본 논문에서 제안한 유·무선 통합 환경에서의 원격 의료 인증 시스템은 다음과 같은 요소들로 구성되어져 있다.

① 모바일 디바이스
무선 환경에서 의료 정보 서비스를 제공 받기 위해 사용되는 단말기 이며 무선 공개키 인증서 및 무선 속성 인증서를 포함하고 바이오 정보를 추출하는 디바이스 이다.

② 퍼스널 서버
유선 환경에서 사용자 인증을 위해 사용하는 공개키 인증서 및 속성 인증서를 포함한다.

③ 의료 정보 서버(컨텐츠 제공자)
유·무선 환경에서 컨텐츠와 원격 의료 관련 서비스 제공을 담당하며 사용자와 원격 의료 서비스가 이루어진다.

④ 인증기관
유선 환경에서 원격 의료 서비스를 사용하고자하는 사용자에게 공개키 인증서를 발급하고 인증서 검증시 공개키 및 인증서에 관한 정보를 제공한다.

⑤ 무선 인증기관
무선 환경에서 원격 의료 서비스를 사용하고자 하는 사용자에게 무선 공개키 인증서를 발급하고 인증서 검증시 공개키 및 인증서에 관한 정보를 제공한다. 또한 무선 환경에서는 제한

된 컴퓨팅 파워와 메모리를 가지고 있기 때문에 유선 환경에서 사용하는 것과 같이 디렉토리 서버로부터 인증서 폐기 목록을 주기적으로 다운받아서 사용할 수가 없기 때문에 실시간으로 인증서의 상태 검증하는 인증서 검증 방법(OCSP : Online Certificate Status Protocol)을 제공한다.

⑥ 바이오 인증기관
원격 의료 시스템을 사용하는 사용자에게 사용자의 바이오 정보에 대한 바이오 인증서를 발급하며 바이오 인증서 사용 시 바이오 정보 검증을 위한 바이오 템플릿을 저장하게 된다.

⑦ 속성 인증기관
유선 환경에서 원격 의료 시스템을 사용하는 사용자의 속성에 대한 속성 인증서를 발급하고 허가권을 가진 자원들에 대해 특정 사용자가 사용 할 수 있도록 자료를 생성하고 서명하여 디렉토리에 저장하는 자료들이 들어있는 사용자 정책 서버와 허가권을 가진 자원들을 사용자가 사용할 수 있도록 승인해주는 역할 정책 서버를 가진다.

⑧ 무선 속성 인증기관
무선 환경에서 원격 의료 시스템을 사용하는 사요자의 속성에 대한 무선 속성 인증서를 발급하고 속성 인증기관과 마찬가지로 사용자 정책 서버와 역할 정책 서버를 가진다.

Ⅲ. 제안 인증 시스템

3.1 디바이스 인증 기반의 유·무선 통합 원격 의료 시스템 구성도

위의 2장 관련 연구에서 살펴본 유·무선 통합 환경에서의 원격 의료 시스템에서는 생체 및 환경 정보를 센싱, 모니터링 하기 위한 의료 센서로부터의 의료 데이터 수집에 대한 보안에 대해서는 고려하지 않았다. 본 논문에서는 의료 데이터를 센싱하는 센서 디바이스 및 사용자 확인을 위한 바이오 디바이스에 대한 신뢰 있는 데이터 수집을 위하여 제 3의 신뢰기관인 바이오 디바이스 인증기관을 포함한 유·무선 통합 원격 의료 시스템을 제안한다. 다음 그림 2는 디바이스 인증 기반의 유·무선 통합 원격 의료 시스템의 구성을 보여준다.

본 논문에서 제안한 유·무선 통합 환경에서의 원격 의료 인증 시스템의 디바이스는 의료 환경에서 환자의 정보 및 환경과 같은 상황정보를 수집하는

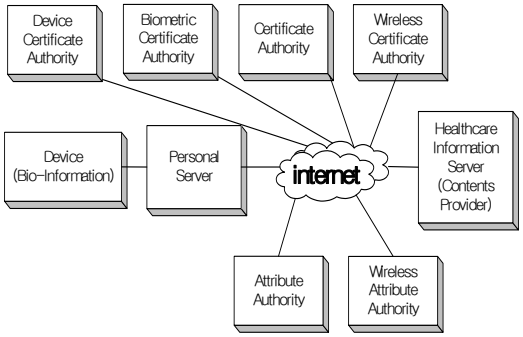

그림 2. 유·무선 통합 환경에서의 원격 의료 인증 시스템 구성도

센서 및 바이오 인증을 위해 사용되는 바이오 정보 추출을 위한 디바이스가 될 수 있다. 본 디바이스에는 의료 환경에 적합한 디바이스 인증서를 포함함으로써 신뢰된 데이터를 의료 정보 서버로 제공한다.

또한 신뢰된 제3의 인증기관인 디바이스 인증기관으로 구성된다. 원격 의료 시스템은 센서들을 통해 환자의 생체 정보나 환경 정보 등을 센싱하여 의료 정보 서버로 보내주게 된다. 이 때 센싱하는 센서들의 잘못된 데이터는 의료 정보를 사용하는 사용자로 하여금 타인의 생명까지 위협 할 수 있다. 따라서 신뢰있는 인증기관에 의해서 발급된 디바이스 인증서를 사용하여 의료 디바이스의 안정성을 유지해야 한다. 디바이스 인증기관은 디바이스 인증서를 발급하고 인증서 검증시 인증서에 관한 정보를 제공한다.

3.2 바이오 디바이스 인증서

신뢰 있는 제 3기관인 바이오 디바이스 인증기관(BDCA : Biometric Device Certificate Authority)에서 바이오 디바이스 인증서(BDC : Biometric Device Certificate)를 발급, 검증, 폐기, 인증서 관리 등의 기본적인 인증기관의 업무를 수행한다. 그리고 인증서 검증 위탁 서버를 두어 공개키 기반의 암호화 연산의 수행이 어려운 바이오 디바이스를 대신하여 공개키 연산을 수행 하게 된다. 바이오 디바이스 인증서는 기본적으로 홈 디바이스 인증서를 따른다. 따라서 홈 디바이스 인증서 프로파일 기본 구조와 같이 버전, 일련번호, 서명, 발급자, 유효기간, 소유자, 소유자 공개키 정보, 확장 필드들로 구성되며 다음 표 1과 같다.

다음 그림 3은 바이오 디바이스 인증서를 발급받는 과정을 보여준다. 의료 센서 또는 의료 디바이스 제작사는 바이오 디바이스 인증기관에 바이오 인증

표 1. 바이오 디바이스 인증서 프로파일 기본 구조

인증서 필드	필드 설명
버전	바이오 디바이스 인증서의 버전 정보
일련번호	인증기관이 발행한 바이오 디바이스 인증서에 부여하는 유일한 값
서명	바이오 디바이스 인증서 서명에 사용된 인증기관 알고리즘에 대한 식별자
발급자	바이오 디바이스 인증서를 발행한 인증기관정보
유효기간	바이오 디바이스 인증서 유효기간
소유자	바이오 디바이스 인증서를 소유한 바이오 디바이스 정보
소유자 공개키 정보	바이오 디바이스 인증서 소유자의 공개키 정보
확장필드	바이오 디바이스 인증서의 확장 필드들

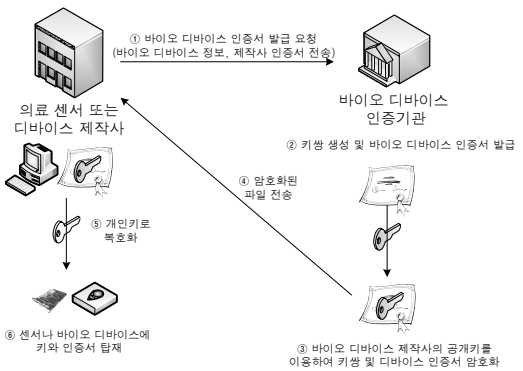

그림 3. 유·무선 통합 원격 의료시스템에서의 디바이스 인증서 발급 과정

서를 요청하게 되고 바이오 디바이스 인증기관은 인증서 발급을 위해서 바이오 디바이스 제작사의 공개키를 이용하여 키쌍을 생성하고 디바이스 인증서를 암호화하여 암호화된 파일로 전송한다. 의료 센서 또는 디바이스 제작사는 전송받은 바이오 디바이스 인증서를 개인키로 복호화하여 센서나 바이오 디바이스에 탑재 시키게 된다.

3.3 디바이스 인증 기반의 유·무선 통합 원격 의료 시스템 보안 프레임 워크

디바이스 인증 기반의 유·무선 통합 원격 의료 시스템 보안 프레임 워크는 다음 그림 4와 같다.

기존 유·무선 통합 원격 의료 시스템의 보안 프레임워크는 유선 환경의 공개키 기반구조[10], 권한 관리 기반구조[11]와 무선 환경의 무선 공개키 기반

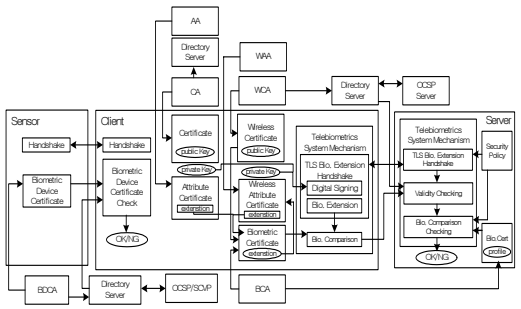

그림 4. 디바이스 인증 기반 유·무선 통합 원격 의료 시스템의 보안 프레임 워크

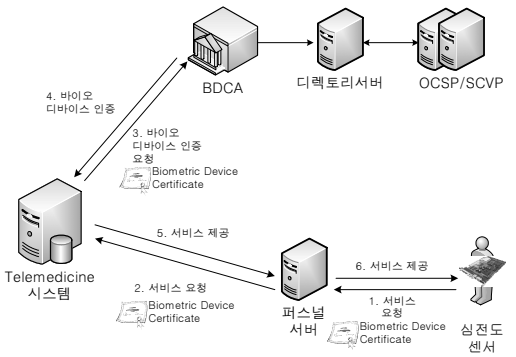

그림 5. 바이오 디바이스 인증서 기반의 유·무선 통합 원격 의료 시스템에서의 디바이스 인증 모델

구조[12], 무선 권한 관리 기반 구조[13]를 고려하여 클라이언트와 서버로 구성되었다. 그러나 원격 의료 시스템은 언제 어디서나 환자의 건강상태를 진단할 수 있는 휴대 가능하도록 소형화된 센서를 활용한 생체 계측기술과 측정된 정보를 무선으로 실시간으로 전달 할 수 있어야 한다.[14] 따라서 최초의 데이터는 센서들에 의해서 물리적, 화학적인 현상의 변화를 감지하는 센싱 과정에서 시작된다.

수집된 의료 정보들의 신뢰성 확보를 위해 센싱하는 모든 센서들은 바이오 디바이스 인증서를 가지게 된다. 따라서 사용자는 바이오 디바이스 인증서를 소유한 센서에 의해 수집되는 의료 정보는 신뢰 할 수 있게 되며 다음 그림 5와 같이 사용될 수 있다.

따라서 보안 프레임워크에 센서와 클라이언트 사이에 디바이스 인증서를 제공하고 센서의 디바이스 인증서의 인증서 상태 프로토콜(OCSP : Online Certificate Status Protocol)과 간단한 인증서 검증 프로토콜(SCVP : Simple Certificate Validation Protocol)을 통해 유효성을 체크하여 최초 의료 데이터 수집의 신뢰성을 가진다.

3.4 디바이스 인증 기반의 유·무선 통합 원격 의료 시스템 사용 예

환자로부터 수집된 심전도 데이터를 의사에게 전달하고 시험된 결과를 기반으로 환자가 의사의 진료를 받게 되는 시나리오이다.

① 환자는 심전도 센서 데이터를 수집하여 유·무선 통합 원격 진료 시스템으로 전달하기 위해서 센서의 바이오 디바이스 인증서를 사용하여 센서의 신뢰성을 체크한다.
② 환자는 자신의 공개키 인증서 또는 무선 공개키 인증서를 사용하여 사용자 인증을 받고 자신의 속성 인증서 또는 무선 속성 인증서를 통하여 환자라는 자신의 권한을 인증 받는다.
③ 환자 본인인지를 확인하기 위하여 자신의 생체 정보를 이용한 사용자 인증을 받는다. 이때 생체 정보를 캡처하는 의료용 디바이스는 바이오 디바이스 인증서를 사용하여 신뢰성을 체크한 후 사용자의 생체 정보를 추출하게 된다.
④ 환자는 ③에서 추출한 자신의 생체 정보와 자신이 발급받았던 바이오 인증서와 바이오 알고리즘 인증서를 제출하여 환자 자신임을 확인 받게 된다.
⑤ ④번까지의 모든 과정이 끝나면 환자는 심전도 센서 데이터를 원격 진료 시스템으로 전달한다.
⑥ 원격 진료 시스템은 의사에게 환자의 의료 데이터가 도착했음을 알린다.
⑦ 의사는 환자의 데이터를 확인하기 위해서 ②③④번과 같은 인증과정을 거친다.
⑧ 의사는 의사의 권한에 맞는 의료 서비스를 제공 받아 환자의 심전도 센서 데이터에 대한 소견서를 작성한다.
⑨ 원격 진료 시스템은 환자에게 소견서가 도착했음을 알려 환자는 먼 거리에 있음에도 자신의 심전도 센서 데이터에 대한 신뢰성 있는 의사 소견서를 제공 받게 된다.

Ⅳ. 비교 분석

기존 대표적인 원격 의료 시스템 6가지의 사용자 인증은 ID, Password를 이용한 방식이고 권한 인증은 접근제어를 통한 사용자 권한 제어 방식이다. 그러나 이러한 ID, Password 방식은 언제라도 유출될 수 있으며 이를 통한 보안 위협이 해결 되지 않는다. 또한 유선 환경 뿐 아니라 무선 환경에서도 보안 위협은 언제든지 노출되어 있다. 따라서 본 논문에서는 유·무선 통합 환경에서 기밀성, 무결성, 인증, 부인 봉쇄의 보안 서비스를 제공하기 위해서 공개키 기반구조와 무선 공개키 기반구조를 사용하였고 이를 통한 사용자 인증은 공개키 인증서와 무선 공개키 인증서를 사용하는 이러한 인증서 기반의 사용자 인증도 인증서의 개인키만 알고 있다면 본인이 아닌 누구라도 이용이 가능하다. 특히 원격 의료 시스템은 환자의 의료 데이터를 다룸으로써 본인이 아닌 다른 누군가에 의한 의료 데이터의 접속은 환자의 프라이버시 침해로 이어질 수 있다. 따라서 자신만의 고유한 생체 정보를 이용하여 두 번째 사용자 인증을 함으로써 프라이버시 침해의 위협으로부터 벗어날 수 있다.

또한 권한 관리 기반 구조와 무선 권한 관리 기반 구조를 이용함으로써 사용자가 자신의 권한에 적합한 서비스를 이용 받을 수 있도록 한다.

그러나 이 모든 사용자 인증과 사용자 속성인증은 최초로 이루어지는 환자의 데이터 센싱시 잘못된 정보가 전송된다면 모든 인증 과정과 상관없이 환자의 잘못된 의료 정보로 인하여 크게는 사람의 생명을 앗아갈 수 있다. 따라서 기존의 원격 시스템과 달리 센서의 센싱 과정에서부터의 의료 데이터 보안을 위하여 의료 센서에 바이오 디바이스 인증서를 이용하였고 이를 통하여 데이터 수집부터 의료 서비스 제공까지의 신뢰성 있는 원격 의료 시스템을 제공한다.

원격 의료 시스템은 환자의 생명을 다루는 정보를 사용한다. 기존의 인증 시스템과 같이 Id, Password로 이루어진 인증 방식을 사용한다면 사용자 입장에서 편리 할 수 있지만 사람의 생명을 다루는 데이터이므로 그 신뢰성은 다른 어떤 데이터보다 중요한다고 할 수 있다. 또한 본인이 아닌 Id, Password를 알고 있는 사람이라면 누구나가 본인의 의지와는 상관없이 사용될 수 있다. 그러나 본 논문에서 제안한 인증 시스템을 사용한다면 사용자의 생체 정보를 사용함으로써 디바이스를 통한 인증 단계를 거침으로 인해서 기존 인증 시스템보다 복잡할 수 있으나 센싱 단계부터 의료 데이터를 이용하는것 까지의 모든 단계에서의 신뢰성을 바탕으로 사용자의 프라이버시까지 보장 받을 수 있는 원격 의료 시스템 사용이 가능하다.

Ⅴ. 결 론

점차 고령화 사회로 접어들면서 건강한 삶과 삶의

질향상을 보장하는 "이상적인 의료 시스템"을 갈망하는 욕구와 더불어 첨단 IT 기술이 융합된 원격 진료 시스템을 선보이고 있다. 이러한 원격 진료 시스템이 안정적으로 서비스되기 위해서는 환자의 의료 정보 데이터가 보안 위협으로부터 안전을 보장 받을 수 있어야 한다.

따라서 본 논문에서는 의료 센서의 데이터 수집에서부터 의료 서비스 제공시까지의 모든 보안 위협으로 부터의 안정한 원격 의료 서비스 제공을 위하여 센서의 디바이스 인증, 유·무선 통합 환경에서의 사용자 인증, 사용자 본인 확인을 위하여 생체정보를 이용한 사용자 인증, 사용자의 권한 인증을 통한 신뢰성 있는 원격 의료 시스템을 제공 한다. 이를 통해 현재 대두되고 있는 프라이버시 문제를 해결 할 수 있다.

향후 의료센서에 적합한 디바이스 인증서 표준 및 유무선 통합 원격 의료 시스템 구축을 위한 기반 구조에 대한 표준화 연구가 더 수행되어야 할 것으로 사료된다.

참 고 문 헌

〔1〕 R.L.Bashshur, T.G.Reardon, and G.W.Shannon, "Telemedicine : a New Health Care Delivery System," Ann. Rev. Public Health, vol.21, 2000, pp.613-617.

〔2〕 R.S.H. Istepanian, E.Jovanov, and Y.T.Zhang, "Guest Editorial Introduction to the Special Section on M-Health: Beyond Seamless Mobility and Global Wireless Health-Care Connectivity," IEEE Trans. Info. Tech. Biomed., vol.8, no.4, 2004, pp.405-414.

〔3〕 http://www.ipath.ch/site.

〔4〕 http://www.openemed.org.

〔5〕 H. Bludau and A. Koop, Mobile Computing in Medicine, Second Conference on Mobile Computing in Medicine, Workshop of the Project Group MoCoMed, GMDS Fach-bereich Medizinische Infor-matik & GI-Fachaus- schuss 4.7, 11. 4. 2002, Heidelberg, vol.5 of LNI. GI, April 2002

〔6〕 Apollohospitals. http://www.apollohospitals.com, March 2 2006.

〔7〕 http://www.eecs.harvard.edu/mdw/proj/codeblue/.

〔8〕 http://www.ece.uah.edu/ jovanov/whrms/.

〔9〕 이유리, 박동규, "WPMI 기반 바이오 인증을 이용한 원격 의료 시스템", 한국 통신학회 논문지, 제 33권 8호, pp 279-284, 2008년 8월.

〔10〕 Alfred Arsenault and S.Turner. Internet X.509 Public Key Infrastructure PKIX Roadmap Work In Progress. Internet-draft 05, March 2000.

〔11〕 D.W.Chadwick "Privilege Management Infrastructure," Business Briefing : Global Security Systems Reference Section.

〔12〕 Wireless Application Protocol Wireless Transport Layer Security, WAP Forum 6th of April. 2001.

〔13〕 D.G.Park and Y.R.Lee, "The ET-RBAC based Privilege Management Infrastructure for Wireless Networks," EC-WEB Conference 2003.

〔14〕 안동인, 박무현, 신창선, 주수종, "헬스케어 상황정보 서비스를 위한 모바일 프락시 구현", 한국정보과학회 학술발표 논문집, 제33권 2호, pp.372-376, 2006년 10월.

이 유 리 (You-ri Lee) 정회원

2002년 2월 순천향대학교 정보통신공학과 공학학사

2004년 2월 순천향대학교 정보통신공학과 공학석사

2004년~현재 순천향대학교 정보통신공학과 박사과정

<관심분야> 접근제어, 유비쿼터스 컴퓨팅 보안

박 동 규 (Dong-Gue Park) 정회원

1992년 한양대학교 대학원 전자공학과 공학박사

1999~2003년 순천향대학교 정보기술공학부 부교수

2004년~현재 순천향대학교 정보통신공학과 교수

<관심분야> 네트워크 보안, 유비쿼터스 컴퓨팅 보안