WPMI 기반 바이오 인증을 이용한 원격 의료 시스템

정회원 이 유 리*, 박 동 규*

WPMI based Telemedicine System using Biometric Authentication

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

요 약

건강한 삶과 삶의 질 향상을 보장하는 이상적인 의료 시스템을 갈망하는 욕구로 인하여 의료 및 의료 정보 서비스를 이용할 수 있는 유비쿼터스 헬스케어에 대한 관심이 높아지고 있다. 이를 이용하면 환자와 환자에 대한 의료 정보가 먼 거리로 떨어져 있거나 시간적으로 많은 차이가 발생하는 등 여러 가지 문제로 인하여 도달 할 수 없는 경우 의료 정보 및 전문가의 조언을 원격으로 서비스를 제공 받을 수 있다. 그러나 원격으로 제공되는 의료 정보가 보안 위협을 당했을 시에는 사람의 생명과 관련되기 때문에 어느 무엇보다 강력한 인증 체계가 필요하며 인증 서비스의 신뢰성 보장은 필수적이라 할 수 있다. 따라서 본 논문에서는 원격 의료 시스템의 보안 위협에 대하여 기밀성, 무결성, 인증, 부인 봉쇄 서비스를 제공하기 위하여 무선 공개키 기반구조(WPKI)와 무선권한 관리 기반 구조(WPMI)를 사용하고 이 때 사용되는 인증서의 사용자의 인증 강화를 위하여 사람의 고유한 생체 식별 정보를 사용하는 원격 의료 시스템을 설계한다.

Key Words : WPKI, WPMI, Telemedicine, Biometric Authentication

ABSTRACT

The concern of Ubiquitous Health Care to use medical service or information has been increasing, due to the wish of the ideal medical system that provides the improvement of the healthy life and it's quality.

If you use it, when patients or their medical information are too far away, and it's hard to get medical service timely with many reasons, they could get the service of medical information or advices of experts remotely. However, if the information remotely provided is threaten, first of all the powerful authentication system is needed and it would be essential to secure the authenticity of authentication service.

Therefore, in this paper, Wireless Public Key Infrastructure(WPKI) and Wireless Privilege Management Infrastructure(WPMI) is utilized to service confidentiality, integrity, authentication, and non-repudiation, regarding to security threat of the telemedicine system. And then in order to strengthen the authentication of users' certificates in WPKI and WPMI, we design a telemedicine system , that utilizes the unique biometric information of users in this paper .

Ⅰ. 서 론

최근 우리 사회는 점차 고령화 사회로 접어들면서 건강한 삶과 삶의 질향상을 보장하는 "이상적인 의료 시스템"을 갈망하는 욕구와 더불어 첨단 IT 기술이 융합된 원격 또는 재택 진료 시스템을 선보이고 있으나, 아직 초보적인 단계이다. 1970년대에 원격 의료라는 용어가 처음 사용되었으며 이는 원거리에서 환자가 의료 상담을 하는 활동만으로 제안되어 있었다.[1][2] 그러나 현재는 환자와 환자에

* 순천향대학교 정보통신공학과 (thisglass@sch.ac.kr, dgpark@sch.ac.kr)
논문번호 : 08041-0612, 접수일자 : 2008년 6월 12일

대한 의료 정보가 먼 거리로 떨어져 있어서 위급 상황이 발생 했을 때 환자의 생명을 구하기 위하여 제공되는 환자의 의료 정보 뿐만 아니라 전문가의 조언, 의료 행정, 의학 교육, 자문 의뢰 등을 컴퓨터와 데이터 통신 기술을 이용하여 의학영상, 동영상, 환자 기록 등 각종 데이터를 주고받는 의료 서비스 기술을 포함한다.

이러한 원격 의료 시스템이 제대로 갖춰지게 되면 언제 어디서라도 응급 처치를 위한 치료가 가능하며 위급환자가 발생 했을 때에 환자에 대한 정확한 정보를 빠르게 제공 받음으로써 도중 필요한 조치를 미리 받을 수 있어 효과적인 응급처리가 가능하다. 그러나 반대로 환자에 대한 정보가 보안 위협을 당했을 시에는 사람의 생명과 관련되기 때문에 어느 무엇보다 강력한 인증 체계가 필요하며 인증 서비스에 신뢰성 보장은 필수적이라 할 수 있다.

기존 원격 의료 시스템에서의 사용자 인증은 ID와 Password 및 인증서를 사용한 공개키 기반 구조를 사용하고 있다. 이러한 인증은 원격 의료 시스템에 적합하지 않을 뿐 아니라 인증서의 개인키를 알고 있다면 본인이 아니더라도 원격 의료 시스템에 접근하여 서비스를 이용 받을 수 있다. 이는 의료 정보 즉, 사람의 소중한 생명을 다루는 시스템에서는 치명적이라고 할 수 있다.

따라서 본 논문에서는 원격 의료 시스템에서의 기밀성, 무결성, 인증, 부인 봉쇄와 같은 보안 서비스를 제공하기 위하여 무선 환경에 접합한 공개키 기반 구조인 무선 공개키 기반 구조를 기반으로 하고, 더 강력한 인증 체계를 위해서 무선 권한 관리 기반을 사용하여 원격 의료 시스템을 설계한다.[3][4] 또한 지문, 홍채와 같은 인체 고유의 정보를 이용하여 시스템을 사용하는 사용자가 확실한 본인 인지를 인증하여 환자의 데이터 보안, 프라이버시 보장 및 신뢰성 있는 원격 의료 시스템 서비스를 제공하고자 한다.

Ⅱ. WPMI 기반의 바이오 인증을 이용한 원격 의료 시스템 설계

2.1 기존 원격 의료 시스템의 보안 기술

현재 대표적인 원격 의료 시스템은 Ipath[5], OpenEmd[6], TeleCardio-FBC[7], CodeBlue[8], Wireless Sensor Body Area Network(WSBAN)[9], Medintagra Web[10] 이다. 위의 6가지 원격 의료 시스템에서는 표 1과 같은 보안 기술을 사용한다.

표 1. 원격 의료 시스템에 사용되는 보안 기술

시스템	보안 서비스
Ipath	의료정보를 위한 표준 보안, SSL을 통한 단대단 암호화, 사용자 기반 인증 및 권한 제어
OpenEMed	권한 제어를 위한 RADS, 인증을 위한 PIDS, 보안 기록을 위한 COAS, 단대단 암호화를 위한 SSL
TeleCardio -FBC	표준 보안 구현
WBASN	1계층을 위한 TinySec, 2,3계층을 위한 SSL, 인증방법으로 생체인증사용
CodeBlue	표준 보안 구현, 잉여 전송, 생체인증
Medintegra Web	인증을 위한 생체인증과 패스워드, 단대단 암호화를 위해 SSL, 역할과 사용자 기반 접근제어 정책

원격 의료 시스템은 개인의 중요한 의료 정보를 다루기 때문에 개인의 사생활 정보를 보호하기 위한 프라이버시 및 인증에 관련된 보안 기술은 필수적이라 할 수 있다. 그러나 기존 원격 의료 시스템의 위의 표 1에서 보여지는 바와 같이 사용자 인증으로 ID, Password, 인증서를 사용한 공개키 기반 및 생체 인증을 사용하고 있다.

ID, Password 또는 인증서의 개인키를 알고 있다면 본인이 아니더라도 서비스를 이용할 수 있으며 WBASN, CodeBlue는 ID, Password를 대신하여 생체 인증을 사용하고 있다. 이러한 인증은 ID, Password, 인증서의 개인키 분실시 본인이 아니더라도 서비스를 이용 할 수 있으며 생체 인증을 하여 사용자에 대하여 인증을 했더라도 사용자의 권한에 대한 인증을 하지 않음으로써 권한 없는 사람에게 환자의 정보가 노출 되었을 시에 환자의 프라이버시는 보장 받을 수 없게 되는 등 여러 가지 의료 데이터의 무결성을 보장 받지 못하여 보안에 치명적일 수 있다.

따라서 원격 의료 시스템을 사용하는 사용자가 신뢰 할 수 있는 인증 서비스를 제공하기 위하여 무선 환경에 적합한 의료 시스템 보안 기술이 필요하다.

2.2 WPMI 기반의 바이오 인증을 이용한 원격 의료 시스템

원격 의료 시스템을 사용하고자 하는 모바일 사용자에게 신뢰 할 수 있는 인증 서비스 제공을 위

하여 강화된 사용자 인증과 원격 사용자 권한 인증 서비스를 제공하기 위한 WPMI 기반의 바이오 인증을 이용한 원격 의료 시스템은 다음과 그림 1과 같다.

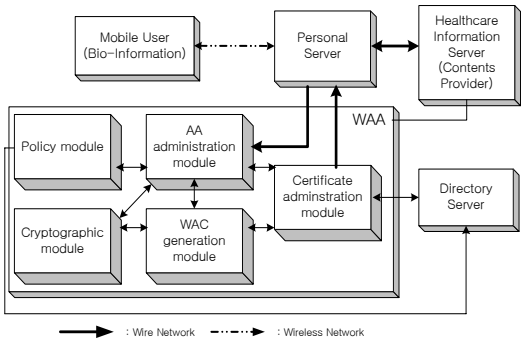

그림 1. WPMI 기반 바이오 인증을 이용한 원격 의료 시스템 구성도

2.2.1 무선 공개키 기반 인증서와 생체 정보를 이용한 사용자 인증

원격 의료 시스템의 서비스는 사용자가 오픈 네트워크를 통해 직접 대면하지 않고 이용 할 수 있는 서비스로 서비스를 제공 받는 사람이 인증된 사용자라는 것이 매우 중요하다. 따라서 원격 의료 시스템의 사용자 인증을 위하여 무선 환경에 적합한 공개키 기반 구조를 이용한다. 이는 휴대폰 및 PDA와 같은 이동 단말을 이용하여 인증기관에 의해 인증, 부인 방지, 무결성, 기밀성을 제공하는 기반 구조로써 제한된 컴퓨팅 파워와 메모리를 가지고 있는 원격 의료 시스템에 적합하다. 이는 사용자의 신원을 증명하기 위하여 사용되어 진다. 따라서 원격 의료 정보 시스템을 사용하고자 하는 사용자는 무선 공개키 인증서를 발급 받아 자신의 개인키를 이용하여 서비스를 제공 받으면 된다. 그러나 개인키를 알고 있는 사용자는 무선 공개키 인증서를 발급 받은 본인이 아니더라도 사용자 인증을 받을 수 있다. 즉, 사용자를 증명하는 수단이 개인키의 비밀성에 근거하는 것인데, 개인키의 오용에 대한 위협은 부인 될 수 없는 것이다. 이러한 위협은 원격 의료 시스템의 특성상 사용자의 프라이버시를 침해할 우려가 있고 또한 사람의 생명과 관련된 중요한 데이터임으로 한층 강화된 사용자 인증 방식이 필요하다. 따라서 사용자의 지문, 홍채와 같은 인체 고유의 바이오 정보를 전송하여 원격 의료 정보 서비스를 받고자 하는 사용자가 확실한 본인 인지를 인증 받는다.

2.2.2 무선 권한 관리 기반 구조를 이용한 사용자 권한 인증

원격 의료 시스템에서는 각 사용자 별로 서로 다른 서비스를 이용해야 할 경우들이 발생한다. 이 경우 각 사용자의 권한이나 임무 등의 사용자 속성을 관리할 필요가 발생한다. 이에 무선 환경에서 사용자의 속성을 정의하여 그 속성에 따라서 원격 의료 시스템을 사용하는 사용자 별로 권한 및 역할을 관리하는 방법인 무선 권한 관리 기반 구조[4]가 필요하다.

따라서 무선 공개키 인증서로 공개키 인증을 받은 사용자는 강력한 보안을 위해서 자신의 바이오 정보를 이용한 사용자 인증을 받는다. 이 사용자는 자신의 권한에 맞는 서비스를 이용하기 위하여 그림 2에서 보여지는 바와 같이 무선 속성 인증기관의 보안 정책 모듈을 통하여 정해진 사용자의 권한

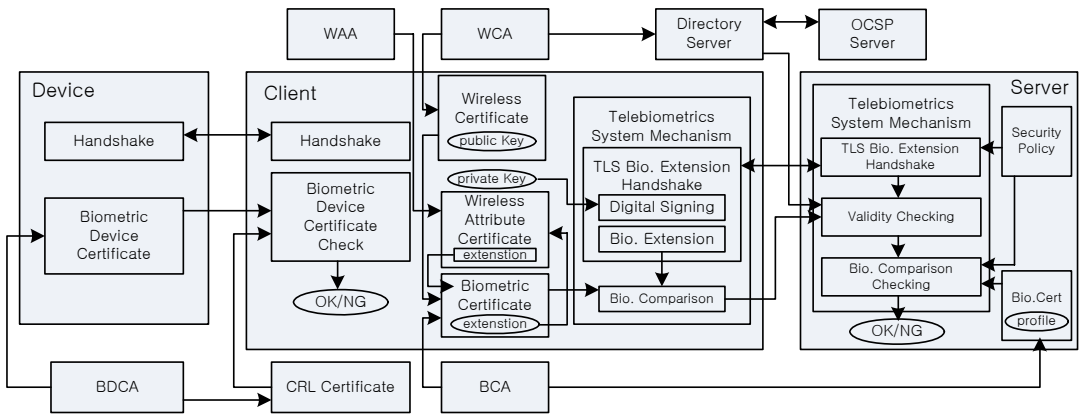

그림 2. WPMI 기반의 바이오 인증을 이용한 원격 의료 시스템 보안 프레임 워크

에 대한 무선 속성 인증서를 발급 받고 이를 이용하여 사용자 권한에 맞는 신뢰성 있는 원격 의료 서비스를 이용할 수 있다.

Ⅲ. WPMI 기반의 바이오 인증을 이용한 원격 의료 시스템 보안 프레임 워크

원격 의료 시스템에서의 인증은 크게 바이오 디바이스 인증, 무선 공개키 사용자 인증, 바이오 정보 사용한 사용자 인증, 사용자 권한 인증이 있다. 이를 위한 보안 프레임 워크는 그림 2에서 보여지는 바와 같이 크게 디바이스, 클라이언트, 서버로 구성되며 보안 프레임 워크는 ITU-T(International Telecommunication Union Telecommunication Standardization Sector) 산하 SG17 WP2 Q.8에서 생체 인식 시스템 표준 제정을 담당하게 되었고 이 표준 중에서 공개키 기반 구조에서 생체 인식 시스템 인증 프로토콜을 제공하는 표준 X.tsm (Telebiometrics system mechanism)과 권한 관리 구조 환경에서 생체 인증을 이용한 신원 및 권한 확인 시에 생체 정보 인증 프로토콜을 제공하는 표준 X.tai(Telebiometric authentication infrastructure)을 기반으로 무선 권한 관리 기반 구조와 무선 권한 관리 구조 환경에 적합하게 설계되었다.

3.1 디바이스 보안 프레임 워크

사용자 인증을 위한 바이오 디바이스의 신뢰성 확보를 위하여 디바이스는 바이오 디바이스 인증서(BDC : Biometric Device Certificate)를 가진다. 이때 사용되는 바이오 디바이스 인증서는 X.509 인증서를 따르는 홈 디바이스 인증서를 사용함으로써 디바이스에 의해 수집된 의료 정보는 신뢰하게 된다.

3.2 클라이언트 보안 프레임 워크

클라이언트는 무선 공개키 사용자 인증, 바이오 정보를 사용한 사용자 인증, 사용자 권한 인증의 보안 프레임 워크로 구성된다.

무선 공개키 사용자 인증을 위하여 X.509 인증서를 따르는 무선 공개키 인증서 또는 X.509에 비해 상대적으로 경량화된 무선 전송 계층 보안 프로토콜(WTLS : Wireless Transport Layer Security) 인증서[11]를 사용하여 원격 의료 시스템에서의 핸드폰이나 PDA와 같은 퍼스널 컴퓨터의 사용자 인증이 가능하다. 이런 무선 환경에서는 제한된 컴퓨팅 파워와 메모리를 가지고 있기 때문에 유선 환경에서 사용 하는 것과 같이 디렉토리 서버로부터 인증서 폐지 목록을 주기적으로 다운받아서 사용할 수가 없다. 따라서 인증서의 유효기간을 짧게 하는 short lived certificate를 사용하거나, 실시간으로 인증서의 상태를 검증 요청하는 (OCSP : Online Certificate Status Protocol)하는 인증서 검증 방법을 사용하여야 한다.

원격 의료 시스템의 강력한 인증 체계를 위하여 사용자를 확인하는 인증 방법이 필요하다. 무선 공개키 인증서만을 사용하여 사용자 인증을 했을 때 사용자의 개인키 유출시 의료 시스템에 심각한 위협을 초래 할 수 있다. 따라서 사용자의 변하지 않는 바이오 정보를 가지고 사용자 인증을 한다. 이때 사용하는 인증서(BC : Biometric Certificate)는 바이오 인증기관(BCA: Biometric Certificate Authority)로부터 발급이 가능하다. 바이오 인증서를 발급 받기 위해 인증기관에 가서 자신의 생체 정보에 대한 확인을 받는다. 이때 바이오 인증서 사용시에 생체 정보 검증을 위한 바이오 템플릿(Biometric Template)을 생성하게 된다.

원격 의료 시스템에서 가장 중요한 보안 요소 중의 하나는 프라이버시이다. 원격 의료 서비스를 이용하고자 하는 사용자의 속성과 권한에 맞는 서비스를 제공함으로써 의료 데이터의 노출로 인한 프라이버시 문제를 해결 할 수 있다. 따라서 원격 의료 시스템에 적합한 무선 속성 인증서(WAC : Wireless Attribute Certificate)를 사용하여 무선 환경에서의 사용자 속성 및 권한 인증이 가능하다.

3.3 서버 보안 프레임 워크

원격 의료 서비스를 제공 하는 서버에서는 바이오 정보를 사용한 사용자 인증 시 보안 정책들을 고려하여 사용자의 바이오 정보 및 바이오 인증서에 대한 검증을 진행한다.

Ⅳ. 원격 의료 서비스 제공을 위한 시나리오

WPMI 기반의 바이오 인증을 이용한 원격 의료 시스템에서 원격 의료 서비스 제공을 받기 위해 응급 상황 발생 시의 시나리오이다.

(1) 응급 환자 발생 시 환자의 진료 기록을 열람해야 되는 의사는 인증을 받기 위하여 자신의 핸드폰, PDA와 같은 퍼스널 서버를 사용하여 인증 정보를 원격 의료 시스템으로 전송한다.

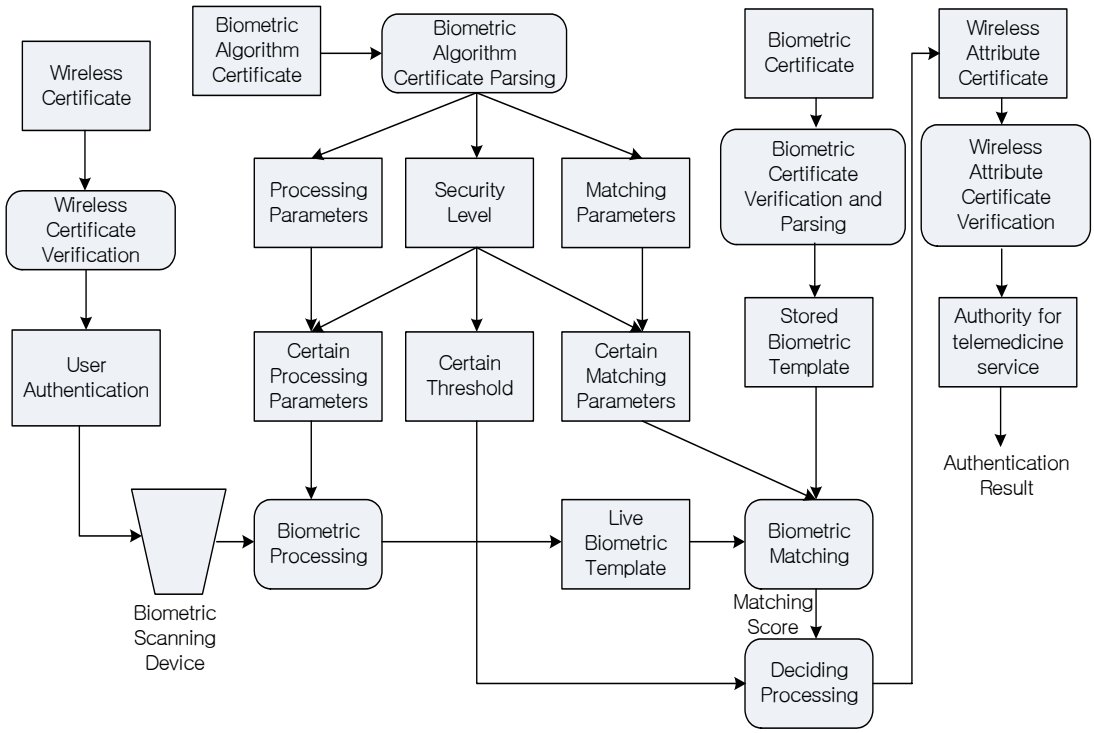

그림 3. WPMI 기반 바이오 인증을 이용한 원격 의료 시스템의 인증 프로세스

표 2. 제안 시스템과 기존 시스템의 비교분석

	사용자 인증	권한 인증	바이오 인증
Ipath	ID/Password 기반	접근제어 정책	
OpenEMed	인증서 기반	접근제어 정책	
TeleCardio-FBC			
WBASN	ID/Password 기반		바이오 인증 사용
CodeBlue			바이오 인증 사용
Medintegra Web	ID/Password 기반	접근제어 정책	바이오 인증 사용
제안 시스템	무선 환경을 고려한 인증서 기반	무선 환경을 고려한 속성 인증서 기반	바이오 인증 사용

(2) 원격 의료 시스템은 전송된 의사의 인증 정보를 이용하여 다음 그림 3와 같은 인증 과정을 통하여 사용자 및 속성 인증을 확인한다.
(3) 사용자 속성이 확인되면 의사에게 환자에 대한 진료 정보를 전송한다.
(4) 의사는 전송된 환자의 진료 정보를 확인하여, 응급 진료 및 처방을 하고 진료 및 처방 정보를 원격 의료 시스템으로 전송한다.
(5) 다른 의사로부터 진료 및 처방에 대한 정보를 받아야 하는 경우 상대방 의사는 동일한 인증 체계를 거친 후 메시지 송수신한다.

Ⅴ. 비교 분석

본 논문에서 제안한 시스템과 기존 원격 의료 시스템을 비교 분석한 결과는 다음 표 2와 같다. 기존 원격 의료 시스템에서의 사용자 인증은 ID와 Password 기반이며 사용자의 속성 인증은 이루어지고 있지 않으며 다만 접근제어를 통한 권한 관리만이 이루어지고 있다. 이것은 사람의 소중한 생명을 다루는 원격 의료 시스템의 치명적인 위협을 가져올 수 있다. 하지만 본 논문에서 제안한 시스템은 원격 의료 시스템에서의 기밀성, 무결성, 인증, 부인봉쇄와 같은 보안 서비스를 제공하기 위한 무선 환경에 적합한 무선 공개키 기반구조와 무선 권한 관리 기반을 사용함으로써 신뢰성 있는 원격 의료 시스템을 제공한다. 또한 개인키를 알고 있으면 누구나 본인이 아니더라도 원격 의료 시스템에 접근 하는 것을 막기 위해 자신의 생체 정보를 이용함으로써 더 강력한 인증 체계를 갖추고 있다.

Ⅵ. 결 론

유비쿼터스 헬스케어에 대한 관심이 높아지고 이를 이용하여 환자와 환자에 대한 의료 정보가 먼 거리로 떨어져 있을 시 또는 시간적으로 많은 차이가 발생하는 등 여러 가지 문제로 인하여 환자의 생명과 관련된 의료 정보를 원격으로 제공 받는 서비스 이용할 때 의료 정보에 대한 보안 위협은 사람의 생명을 다루므로 다른 어느 시스템보다 치명적이라 할 수 있다. 따라서 강력한 인증 체계가 필요하며 인증 서비스의 신뢰성 보장은 필수적이라 할 수 있다.

본 논문에서는 원격 의료 시스템에서의 기밀성, 무결성, 인증, 부인 봉쇄와 같은 보안 서비스를 제공하기 위하여 무선 환경에 접합한 공개키 기반 구조인 무선 공개키 기반 구조를 기반으로 하고, 더 강력한 인증 체계를 위해서 무선 권한 관리 기반을 사용하여 원격 의료 시스템을 설계하였다. 설계된 시스템은 사용자 인증시 사용자의 고유 바이오 정보를 이용함으로써 시스템을 사용하는 사용자가 확실한 본인 인지를 확인함으로써 강력한 인증 체계를 갖춤으로써 환자의 데이터 보안, 프라이버시 보장 및 신뢰 있는 원격 의료 시스템을 제공한다.

향후 연구 과제로는 무선 환경에서의 인증 시스템 및 디바이스 인증 시스템의 표준화에 대한 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〕 J.I.Lee and J.H.Park and J.S.Song, Domestic PKI model for WAP, Institute of Information Security & Cryptology Journal, October 2000.

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

〔5〕 http://www.ipath.ch/site

〔6〕 http://www.openemed.org

〔7〕 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, volume 15 of LNI. GI, April 2002

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

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

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

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

이 유 리 (You-ri Lee) 정회원

2002년 2월 순천향대학교 정보통신공학과 공학사

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

1999년~2003년 순천향대학교 정보기술공학부 부교수

2004년~현재 순천향대학교 정보통신공학과 교수

<관심분야> 네트워크 보안, 유비쿼터스 컴퓨팅 보안