情 報 保 護 學 會 誌
第 17 券 第 5 號, 2007. 10

원격의료 정보시스템의 바이오 인증 융합기술

황유동*, 이유리*, 박동규*, 신용녀**, 김재성**

요 약

언제 어디서나 예방, 진단, 치료, 사후 관리의 보건 의료 서비스를 제공하는 Ubiquitous-Healthcar(U-HC)는 최근 초보적인 단계로 IT 기술과 의료 시스템이 결합된 원격 또는 재택 진료 시스템이 선을 보이고 있다. 하지만 원격 의료 시스템의 개인 신상 및 바이오 유출은 환자의 프라이버시 침해의 가능성을 내포하고 있다. 따라서 본고에서는 원격 의료 정보 시스템의 인증을 강화하기 위하여 Telebiometrics X.tsm 과 X.tai 표준을 기반으로 하는 바이오 인식 기반 원격 의료 정보 시스템의 사용자 인증 모델의 예를 제시하고 Telebiometrics의 X.tpp를 기반으로 시스템에서 발생 할 수 있는 취약성 및 위협을 분석한다.

Ⅰ. 서 론

최근 우리 사회는 언제, 어디서나, 누구든지 서비스를 이용 할 수 있는 Ubiquitous에 대한 관심이 높아지고 있으며 이중에서도 건강한 삶과 삶의 질 향상을 보장하는 "이상적인 의료 시스템"을 갈망하는 욕구로 인해 의료 및 의료 정보 서비스를 이용 할 수 있는 Ubiquitous-Healthcare(U-HC)에 대한 관심이 높아지고 있다. 또한 세계 각국에서는 이를 위한 기반 조성에 경쟁적으로 나서고 있어 실현 시기는 빨라질 가능성이 높다. u-헬스케어를 연구하는 세계 각국에서는 아직 초보적인 단계로 첨단 IT 기술과 의료 시스템이 결합된 원격 또는 재택 진료 시스템을 선보이고 있으나, 아직 초보적인 단계로 본격적인 온라인을 통한 증상 예측, 진단, 치료는 좀 더 시간을 필요로 하고 있다.

u-헬스케어 서비스 시스템의 대표적인 예로는 로체스터 대학의 미래 스마트 메디컬 홈 프로젝트를 들 수 있다. 스마트 메디컬 홈 프로젝트는 스마트 의료 센서 부, 수집된 각종 생체 신호의 분석부, 지속적인 건강상태 모니터링 및 데이터 축적부, 응용 서비스를 위한 정보 교환 인터페이스 및 사설 방화벽 등으로 구성되며, 이와 같은 프레임워크를 기반으로 댁내에서 피부암 등의 피부상태를 상시 체크할 수 있는 smart mirror, 상처의 병원체 감염유무를 상시 감시·보고하는 smart bandage, 복용 약에 대한 정보와 복용 유무를 알려주는 smart drug 등의 서비스를 제공한다. 그리고 또 다른 시스템으로 GE 헬스케어는 의료용 단말과 병원 내 데이터베이스를 이용하여 원격지에서 임산부의 상태(태아의 심장박동, 산모의 자궁 수축도 등)를 살피고 원격지에서도 충분히 진찰할 수 있는 서비스를 제공하고 있다. 이 외에도 EU의 MobiHealth (Mobile Healthcare) 프로젝트는 고위험도의 임산부, 만성 질환자, 심장 질환자 등을 대상으로 일상 생활 속에서 지속적인 환자 모니터링을 통해 질병 판단 및 예측, 응급상황 대처 등의 서비스를 제공하는 플랫폼과 비즈니스 모델에 관한 연구를 진행하고 있으며, 지속적인 의료 케어(MCC) 프로젝트는 암, 신생 질병의 집중 치료를 받은 후, 댁내에서의 원격 모니터링 및 진단 서비스를 제공한다. 그리고 RFID를 응용하여 환자의 이동, 현 위치, 이상 징후 등의 데이터를 실시간으로 의료 기기에 전송하는 RFID 센서 응용 프로젝트 등도 활발히 진행 중이다[8].

원격 의료 시스템이 제대로 갖춰지면 언제 어느

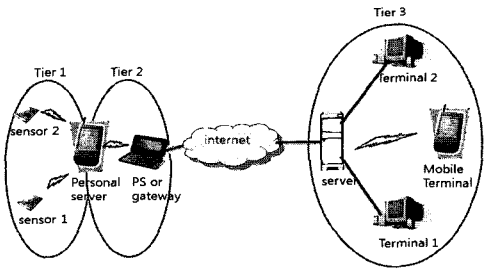
* 순천향대학교 정보통신공학과({coppemilk,thisglass,dgpark}@sch.ac.kr)
** 한국정보보호진흥원 보안성평가단 산업지원팀({jskim, ynshin}@kisa.or.kr)

곳이라도 의료 처치가 가능하며 위급한 환자 발생 시 환자의 위치와 현재 생체 신호를 전송, 빠른 시간 내 구급 팀의 도착을 유도하고 오는 도중 필요한 조치를 미리 준비 할 수 있도록 알려줘 효과적인 응급처치가 가능하게 한다. 하지만 이러한 장점을 가진 원격 의료 시스템도 유, 무선 네트워크와 각종 센서 및 유비쿼터스 단말기를 이용해 서비스가 이루어지므로 개인 신상 및 바이오 정보 유출 등 개인 프라이버시 침해의 가능성을 내포하고 있다. 따라서 이를 미연에 방지하기 위해 원격 의료 시스템 관련 서비스의 보안 기술이 필요하다. 따라서 본고에서는 원격 의료 시스템에서 발생할 수 있는 다양한 위협들 중 사용자 인증 관련 요구 사항들을 도출하고 이를 기반으로 신뢰 할 수 있는 다양한 서비스를 제공하기 위하여 바이오 인식을 기반으로 하는 사용자 인증 모델의 예를 제시하고자 한다.

Ⅱ. u-헬스케어를 위한 원격의료 시스템

u-헬스케어를 위한 원격의료 시스템의 구성도는 다음 그림과 같이 세 계층의 클라이언트 서버 프레임워크로 표현된다[1]. 모든 원격의료 시스템은 생체 및 환경 정보를 센싱, 모니터링 하기 위한 의료 센서로 부터 데이터를 수집하고, 수집된 데이터는 유무선 네트워크를 통해 생체 데이터 분석과 건강 피드백을 담당하는 의료 정보 서버로 전달된다. 전달된 데이터를 이용하여 의료 정보 서버는 건강상태, 생활패턴 등에 관한 건강 자료(wellness index)를 분석하고 이와 관련된 경고(alarm), 현장 진단처방(PoC), 단순 주지 등의 피드백(feedback)이 모바일 장치나 다른 사용자 터미널을 통하여 사용자에게 전달된다.

대표적인 원격의료 시스템으로 Ipath와 Open-EMed, TeleCardio-FBC, CodeBlue, Wireless Sensor Body Area Network (WSBAN), Medintagra Web등을 들 수 있으며, 원격으로 시스템은 크게 환자 기록 관리 시스템(Patient Record management System : PRS)과 환자 건강 원격모니터링 시스템(Patient Health remote monitoring Systems : PHS)로 구분할 수 있다. PHS는 환자에게 서비스를 편리하게 전달하는데 중점을 둔 시스템으로 원격으로 환자의 데이터를



〔그림 1〕 원격 의료 시스템 구성도

수집하고 헬스 케어 서비스를 원격으로 전달하는 기술들을 사용한다. 이 시스템은 ActiS 센서, Zigbee, GPRS, 블루투스 스마트폰과 같은 통신 기술들을 사용하여 원격으로 환자들의 건상 상태를 수집하고 통합한다. 수집된 데이터들은 리얼 타임으로 건강의료 서버에 전달되며, 수집되는 데이터들은 텍스트, 비디오, 그래픽, 멀티미디어데이터, 오디오등 모든 형태의 데이터들이 포함된다. 해당 시스템의 예로는 Code-Blue 시스템과 Medintegra Web 시스템 등을 들 수 있다. 이와 달리 PRS는 환자의 기록 관리에 중점을 둔 시스템으로 의료 전문가들이 서로 연동하여 사용하는데 중점을 두고 있다. 모든 PHS 시스템들은 PRS시스템의 기능들을 통합하여 사용할 수 있기 때문에 PRS시스템은 PHS 시스템의 서브시스템으로 간주될 수 있다. PRS 시스템의 예로는 Ipath 시스템[2]과 Open- Med[3] 시스템을 들 수 있다.

6개의 대표적인 원격의료 시스템들이 제공하는 서비스와 사용하는 기술, 그리고 안전한 서비스를 위해 사용하는 보안기술들은 다음 [표 1]과 같다.

원격 의료시스템에서도 [그림 2]와 같이 다양한 보안 취약점과 위협 요소들이 존재하며, 유무선 네트워크 기반 서비스에서 발생 가능한 보안상 취약점 및 공격이 원격 의료 시스템 환경에서도 유사하게 발생되는 형태를 보인다[8]. 따라서, 원격 의료 시스템의 기반 네트워크 및 시스템에 대한 안전성, 신뢰성 보장 및 데이터 보호를 위한 정보보호 기술의 개발이 절실히 필요한 상황이다. 그중에서도 원격 의료 시스템은 개인의 중요한 의료정보를 다루기 때문에 개인의 사생활 정보를 보호하기 위한 프라이버시 및 인증에 관련된 비중이 점차 증대하고 있는 추세이다.

〔표 1〕 원격의료 정보시스템이 제공하는 서비스

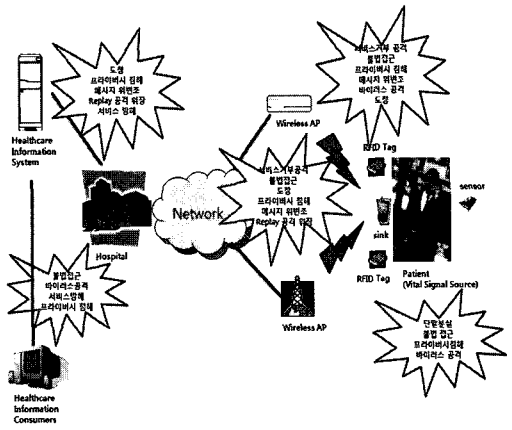
시스템	서비스
Ipath[2]	데이터 프라이버시 보장, 연구와 지속적인 교육
OpenEMed [3]	데이터 관리, 안전한 원격 컨설팅, 연구와 지속적인 교육
TeleCardio-FBC[4]	원격 컨설팅, 데이터 관리, 데이터 암호화
WBASN[5]	원격 실시간 모니터링, 전자처방, 데이터 암호화, 데이터 공유, 지속적인 교육과 연구
CodeBlue [6]	실시간 모니터링, 데이터 관리, 교육, 연구
Medintegra Web[7]	원격 컨설팅, 데이터 관리, 지속적인 교육

〔표 2〕 원격의료 정보시스템에 사용되는 기술

시스템	사용되는 기술
Ipath	PHP, mySQL, 웹 기술 (browsers, HTTP,HTML등), 인터넷기술(TCP/IP, 등), 디지털 사진 기술
OpenEMed	JavaTM, CORBA, 웹 기술 (browsers, HTTP,HTML등), 인터넷 기술(TCP/IP, 등),
TeleCardio - FBC	ASP, SQL, Java Serlet, Java beans, 웹, 인터넷 무선통신 기술 (GSM, Wi-Fi, WAP, CDMA등)
WBASN	Windows CE, VB .NET, Microsoft Access,웹, 인터넷 무선통신 기술
CodeBlue	Java, 인터넷, 웹, BlueTooth, Zigbee, Infrared, motion (accelerometers, gyroscopes 등) 기술
Medintegra Web	Java,웹, 인터넷 무선통신 기술

〔표 3〕 원격의료 정보시스템에 사용되는 보안 기술

시스템	보안 서비스
Ipath	의료정보를 위한 표준 보안, SSL을 통한 단대단 암호화, 사용자 기반 인증및 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



〔그림 2〕 원격의료 시스템의 보안 위협

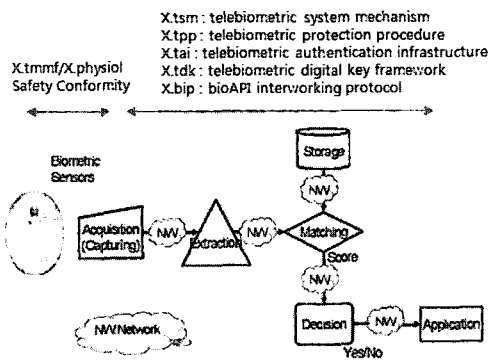
Ⅲ. Telebiometrics 관련 보안 표준

인증 방식에 대한 인증 서비스 신뢰성을 보장하기 위한 방안으로 바이오인식 정보를 이용한 사용자 인증과 암호화 기법이 연구되고 있으며, 유비쿼터스 환경에 적용하기 위한 방법으로 Telebiometrics가 활발히 연구되고 있다.

Telebiometrics란 Telecommunication과 biometrics의 합성어로, 네트워크를 통해 연결된 클라이언트와 서버 구조를 갖는 생체인식 시스템을 말하며, 유비쿼터스 환경과 같은 다양한 통신망과 다양한 단말, 서버 등의 기기를 이용하여 서비스하는 시스템에서 효과적인 보안 서비스를 제공하기 위한 방법이다.

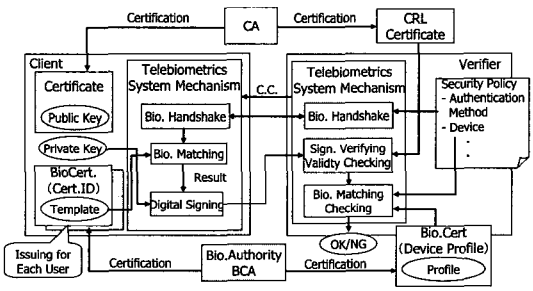
Telebiometrics는 2005년 새로운 연구과제로 ITU-T(International Telecommunication Union Telecommunication Standardization Sector) 산하 SG17 WP2 Q.8에서 Telebiometrics 표준 제정을 담당하게 되었다. Q.8에서 진행 중인 표준 과제는 X.tmmf, X.physiol, X.tpp, X.tsm 및 X.tai 등이 있으며, Telebiometrics 시스템 구조와 각 과제별 다루는 범위는 다음 [그림 3]과 같고, 각 과제에서 연구되는 내용은 다음 [표 4]과 같다.

Telebiometrics 표준들 중에 X.tsm (telebiometrics system mechanism)은 클라이언트와 서비스 제공자 사이에서 biometric 인증 프로토콜을 제공하는 표준으로 PKI 기반의 Telebiometrics 시스템의 다양한 모델과 메커니즘을 정의한다. 이 표준은 클



〔그림 3〕 Telebiometrics 시스템 구조와 과제별 범위

라이언트, 서버가 네트워크상에서 연결되어 있는 구조로 biometric 기준 템플릿이 존재하는 위치와 biometric 비교가 이루어지는 위치에 따라서 9개의 텔레바이오 인식 시스템 모델 및 프로파일을 정의하고 있으며 또한 각 모델별 위협 및 이를 해결하기 위한 바이오 인식기술과 데이터를 활용한 PKI 인증모델과 TLS 프로토콜을 제안하고 있다. 해당 표준안의 전체 시스템 구성도는 다음 [그림 4]와 같다. 이 표준을 기반으로 바이오 인식 기반 원격 의료 정보 시스템을 구성하는 것이 가능하게 된다.



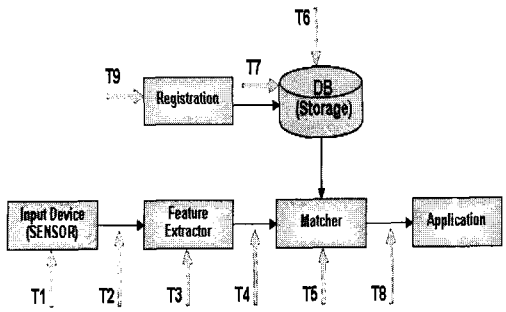
〔그림 4〕 TSM 구성도

그리고 Telebiometrics 표준들 중에 X.tpp (telebiometrics protection procedure)는 일반적인 Telebiometrics 환경 내에서 모든 가능한 위협으로부터 생체 자료와 정보를 보호하기 위한 가이드라인 및 프로토콜을 제시한 표준으로 Telebiometrics 시스템의 9가지 취약 포인트 정의 및 각 취약 포인트별 시스템 보호를 위한 가이드라인을 제시하고 있다. X.tpp는 Telebiometric 프로세스 모델을 바이오

〔표 4〕 Telebiometrics 표준 과제 내용

과제명	요약
x.bip	-. BioAPI interworking protocol 정의 -. ISO/IEC JTC 1 SC 37(Biometric)에서 진행중인 표준과 연계 -. SC37과 Q.8에서의 모달리티 정의 차이로 인해 발생하는 문제 해결 필요
x.tmmf	Telebiometrics의 물리적 운영 환경 내에서 시스템과 인간 사이의 다양한 상호작용을 정의
x.physiol	X.Tmmf에 정의된 상호작용들의 물리량, 단위, 안전 수치 등을 예시와 함께 정의
x.tsm-1/2	-. PKI 기반의 Telebiometric 시스템의 다양한 모델과 메커니즘을 정의 -. 클라이언트, 서버가 네트워크상에서 연결되어 있는 구조로 된 9개의 텔레바이오인식 시스템 모델 및 프로파일 정의 -. 각 모델별 위협 및 이를 해결하기 위한 바이오 인식기술과 데이터를 활용한 PKI 인증모델과 TLS 프로토콜을 제안
x.tpp-1/2	-. X.tpp-1과 X.tpp-2는 일반적인 Telebiometrics 환경 내에서 모든 가능한 위협으로부터 생 체 자료와 정보를 보호하기 위한 가이드라인 및 프로토콜을 제시 -. 텔레바이오메트릭 시스템의 9가지 취약 포인트 정의 및 각 취약 포인트별 시스템 보호를 위한 가이드라인 제시 -. 특히, 다중 바이오메트릭 시스템에서 두개 이상의 바이오 정보를 전송시 보호하기 위한 정책적/기술적 방법 제시 : X.tpp-2
x.tai	X.tsm의 특별한 경우로서 PKI와 동시에 PMI(Privilege Management Infrastructure) 환경에서 생체인증을 이용한 신원 및 권한 확인 시에 생체정보 인증을 모델 및 프로토콜을 정의
x.tdk	-. 인증 프로세스를 간단화 하고 안전한 통신 시스템을 구축하기 위한 프레임워크를 제시 -. 2006년 12월 시작

정보 입력과정, 특징점 추출과정, 저장과정, 바이오 정보 비교과정, 신원확인과정으로 재정의 하여 Telebiometric 콤포넌트에서 발생 가능한 취약점들을 재정의 하였다. Telebiometrics 시스템의 9가지 취약 포인트는 다음 [그림 5]와 같다.



〔그림 5〕 Telebiometrics 시스템의 9가지 취약 포인트

X.tpp 표준을 기반으로 바이오 인식 기반 원격의료시스템 구성 시 발생할 수 있는 각 부분별 취약성 정의 및 이에 대한 대응방안 구성이 가능하리라 사료된다.

Ⅳ. 바이오 인식 기반 원격의료 정보시스템

앞에서 설명한 바와 같이 신뢰할 수 있는 원격의료서비스를 제공하기 위하여 WBASN과 CodeBlue 시스템에서는 사용자 인증을 위하여 생체 식별 정보를 사용하고 있다. 이와 같이 u-헬스케어 환경이 되면서 종래의 ID/PWD나 공인 인증서 기반뿐 아니라, 다양한 생체 식별 정보를 사용하여 한층 강화된 사용자 인증 방식이 활용될 것으로 예상된다.

따라서 본고에서는 앞에서 설명한 Telebiometrics X.tsm 과 X.tai 표준을 기반으로 바이오 인식 기반 원격의료 정보 시스템의 사용자 인증 모델의 예를 제시하고자 한다.

4.1. 원격 의료 시스템의 보안 요구사항 분석

원격의료 시스템에 맞는 보안 모델을 설계하기 위하여 먼저 원격의료 시스템의 보안요구 사항을 분석해야 한다.

원격의료 시스템의 보안 요구 사항은 다른 유비쿼터스 관련 서비스들, 그리고 유, 무선 네트워크를 이용하는 모든 서비스와 동일한 보안 요구 사항과 원격의료 시스템만의 보안 요구 사항이 있다. 원격 의료 시스템과 다른 서비스와 다른 보안 요구 사항은 다음과 같다.

4.1.1. 원격의료 시스템에서 다른 서비스와는 다른 보안 요구 사항

① 의료서비스, 즉 정확한 진료를 받기 위해서는 생체 정보를 포함한 개인의 질병 내력, 가족력, 신체적 특징 등의 개인 의료 정보를 충분히 제공해야 하며, 이 정보는 환자가 이동함에 따라 중복된 검사와 의료 조치가 반복되는 것을 막기 위해 선택적으로 다른 의료 기관(병·의원 또는 보건소 등)에 위임 및 제공되어야 한다. 즉 개인 정보가 여러 기관들에 의해 공유되어야 하며 정확한 진료를 위해서는 정보 공유가 필수적이다. 그러나 개인의 입장에서는 이러한 개인 정보가 타당한 대상자에 의해 의료 서비스 목적에 맞게 최소한의 공유만 이루어지기를 기대할 것이다. 반면, 현 의료 정보 보안 정책 및 기술로는 정보 공유의 대상과 그 범위를 명확하게 파악하거나 결정할 수 없다는 큰 문제를 안고 있다. 따라서 의료 정보에 대한 프라이버시 보호적 차원에서의 개인 의료 정보권한 관리 및 위임, 활용에 관한 기술적, 법제도적 지원책이 요구된다.

② 불법적인 의료 정보 열람과 이용을 막고 그 책임 소재를 판단하기 위하여 보안 감사 체계가 보완되어야 한다. 현재, 대부분의 병원에서는 요청자의 단순 서비스 요청에 관한 로그만 남길 뿐, 데이터 습득 이후 활용, 폐기 등에 관한 의무사항 준수에 관련한 감사 체계가 부재한 상황이다. 이는 최근 심각한 보안 취약점으로 거론되고 있는 내부자에 의한 정보 유출의 위험성을 가중시킬 수 있다.

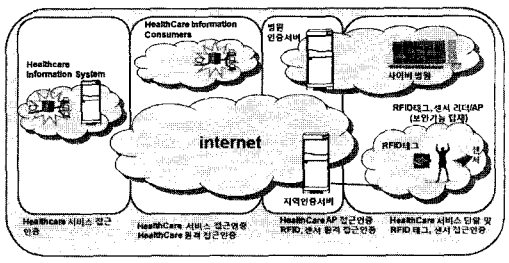
③ 보다 향상된 수준의 의료 서비스와 개인의 의료 건강 정보에 대한 접근성을 용이하게 하기 위하여 향후 이질적인 병원 정보 서버 간 환자에 대한 건강 정보 공유가 빈번하게 이루어질 것이다. 이와 같이 이질적 의료 도메인 간 개인의 건강/의료 정보를 교환 시, 인증된 도메인 간에 안전하게 가용한 정보만을 송수신하도록 지원할 수 있는 보안 기술이 필요하다. 즉, 이질적인 인증방식에 대한 인증 서비스 독립성을 보장하고 도메인 간에 교환 및 공유되는 트랜잭션에 대해 책임(accountability)을 부여하기 위한 기술이 필요하다. 뿐만 아니라, 원격의료 환경이 되면서 종래의 ID/PWD나 공인 인증

서 기반뿐 아니라, 다양한 생체 식별 정보가 사용자 인증 방식으로 활용될 것이다. 생체 인식/인증에 사용되는 유일무이한 생체 정보는 그 정보의 변경이 쉽지 않아 생체정보의 노출로 더 이상 사용이 불가능한 경우에 대한 대비책이 있어야 하며, 신체 손상으로 생체정보의 제공이 불가능한 경우에 대한 대체 수단의 제공 방법이 마련되어야 한다. 특히, 사용자 식별과 관련하여 지금까지 널리 사용되어 왔던 주민등록번호는 그 생성 특성상 번호만으로도 개인 정보 노출이 쉽고 주민번호 생성 및 유출 또한 용이하며, 중복된 번호 존재 등으로 국가적으로도 온라인 상거래나 전자정부 행정업무에서도 사용을 지양하고 있다.

④ 병원마다 서로 다른 환자식별 체계가 사용되고 있어 환자는 다양한 형태, 다수의 ID 정보를 기억 및 관리해야 하는 불편함을 감수하고 있다. 향후, 병원 간 건강/의료 정보 공유 시, 환자를 포함한 인가 받은 정보 소비 주체들이 불필요한 개인정보 노출 없이 익명성을 보장 받으면서도 정상적으로 인증 및 식별 가능하며, 소수의 ID 계정으로 의료 서비스 이용이 가능하도록 할 수 있는 통합된 ID 관리 체계가 필요하다. 통합된 ID 관리 시스템의 구축 범위는 정책에 따라 협소하게는 모(母)병원과 관련 협업 병원 간 구축할 수 있으며, 국가적으로 국내 모든 병원의 환자를 인증 및 관리하는 국가 통합형 ID 관리 시스템 모델이 존재할 수 있다.

4.2. 인증 프레임 워크에서 제공되는 보안 서비스

위와 같은 보안 요구 사항들에 대응하기 위한 인증 프레임워크는 다음 [그림 6]과 같다.



[그림 6] U-Healthcare 인증 프레임 워크

원격의료 서비스는 다음 4단계의 인증 프레임워크로 이루어지며, 각 단계별 인증 프레임워크에서 제공되는 보안 서비스는 다음과 같다.

-. 원격의료 서비스 접근 인증 :
원격의료 정보 시스템간의 접근 인증.
원격의료 지역 인증 서버와 원격의료 정보 시스템간의 인증.

-. 원격의료 서비스 접근 인증, 원격의료 원격 접근 인증 :
원격의료 정보 수요자와 지역 인증 서버간의 접근 인증.
원격의료 정보 수요자와 원격의료 정보 시스템 간의 원격 접근 인증.

-. 원격의료 AP(Access Point) 접근 인증, RFID · 센서 원격 접근인증 :
원격의료 서비스 단말을 통한 지역 인증 서버의 사용자 접근 인증.
원격의료 서비스 단말과 사이버 병원간의 접근 인증.
원격의료 서비스 단말을 통한 원격의료 정보 시스템에의 사용자 접근 인증.

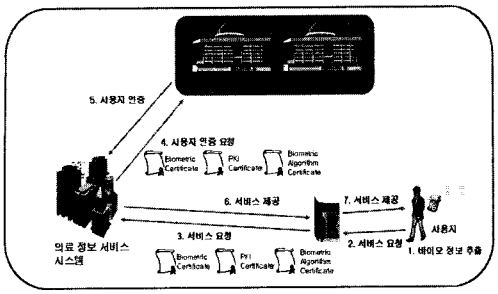
-. 원격의료 서비스 단말 및 RFID 태그 · 센서 접근 인증 :
RFID 태그 · 센서 부착자(사용자) 접근 인증.
RFID 태그 · 센서와 AP(Access Point)간의 기기 인증.
RFID 태그 · 센서와 원격의료 서비스 단말간의 기기 인증.
원격의료 서비스 단말에서의 사용자 인증.

각 인증 프레임워크 간에는 기존의 네트워크 보안에 적용되는 보안 프레임워크를 적용하여 기밀성과 무결성을 보장한다.

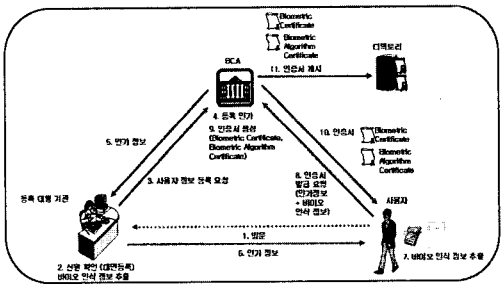
4.3. 원격 의료 시스템의 사용자 인증 모델

X.tsm 과 X.tai 표준을 기반으로 바이오 인식 기반 원격의료 정보 시스템의 사용자 인증 모델은 다음 [그림 7]과 같다.

그리고 바이오 인식 기반 원격의료 정보 시스템의 사용자 인증서 발급 모델 예는 다음 [그림 8]과 같다.



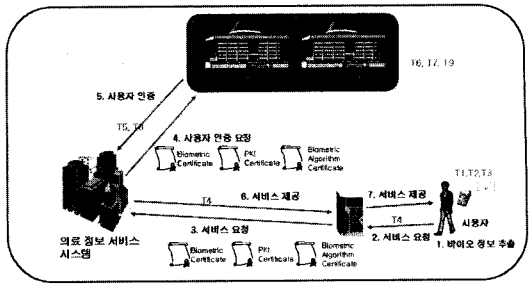
〔그림 7〕 바이오 인식 기반 원격의료 정보 시스템의 사용자 인증 모델 예



〔그림 8〕 바이오 인식 기반 원격의료 정보 시스템의 사용자 인증서 발급 모델 예

위 그림은 바이오 인식 기반의 원격의료 정보시스템의 사용자 인증 예이다. U-헬스케어에서 사용자는 서비스를 제공 받기 전 오프라인으로 사용자의 바이오 정보를 추출하여 추출된 바이오 정보는 BCA로 보내지고 BCA에서는 바이오 정보가 삽입된 인증서를 생성하여 저장소에 보관하고 사용자 등록 업무는 완료 된다. 사용자가 U-헬스케어 서비스를 제공받기 위하여 서비스 단말을 이용하여 접근하게 되면 서비스 게이트웨이는 인증서 등록 관리 시스템에 연결하여 정상적인 사용자임을 확인 받은 후 서비스 제공 시스템에 서비스 단말을 연결하여 서비스 한다. U-헬스케어 정보 수요자 또한 서비스 사용자와 동일한 형태의 인증 과정을 거친 다음, 의료 정보 데이터베이스에 접근 할 수 있다.

앞에서 설명한 바이오 인식 기반 원격의료 정보시스템도 다양한 취약성과 위협에 노출될 수 있다. 그런데 앞에서 제시한 바이오 인식 기반 원격의료 정보시스템은 Telebiometrics를 기반으로 한 것이기 때문에 이 시스템에서 발생할 수 있는 취약성 및 위협에 대한 분석 및 대응방안에 대한 연구는



〔그림 9〕 바이오 인식 기반 원격의료 정보시스템의 취약성 및 위협 분석 예

앞에서 설명한 Telebiometrics의 X.tpp를 적용하면 가능하리라 사료된다. 따라서 앞에서 설명한 Telebiometrics의 X.tpp를 기반으로 바이오 인식 기반 원격의료 정보시스템의 취약성 및 위협을 분석한 예는 다음 그림과 같다. 각 위협별로 이에 대처할 수 있는 대응 방안은 X.tpp에서 제시된 대응방안을 적용하면 가능하리라 사료된다.

V. 결 론

본고에서는 원격의료 정보시스템의 인증을 강화하기 위하여 바이오 인식 기반 원격의료정보시스템의 사용자 인증 모델 예를 제시하고, 이 시스템에서 발생할 수 있는 취약성을 분석하였다. 본고에서 제시한 바이오 인식 기반 원격의료정보시스템의 사용자 인증 모델은 Telebiometrics X.tsm과 X.tai 표준을 기반으로 하였으며, Telebiometrics의 X.tpp를 기반으로 바이오 인식 기반 원격의료 정보시스템의 취약성 및 위협을 분석하였다.

앞으로 원격의료정보 시스템의 바이오 인식 기반 사용자 인증시스템의 표준화에 대한 연구가 더 수행되어야 할 것으로 사료된다.

참고문헌

[1] [Drake Patrick Mirembe, 2006], "Design of a Secure Framework for the Implementation of Telemedicine, eHealth, and Wellness Services", Master Thesis, Radboud Uni- versity Nijmegen, July 2006

[2] http://www.ipath.ch/site

[3] http://www.openemed.org

[4] H. Bludau and A. Koop, editors. 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

[5] http://www.ece.uah.edu/ jovanov/whrms/

[6] http://www.eecs.harvard.edu/mdw/proj/co deblue/

[7] Apollohospitals. http://www.apollohospitals. com, March 2 2006.

[8] 송지은 외," u-헬스케어 보안 이슈및 기술 동향" , 전자통신 동향분석 제 22권 제 1호 2007년 2월

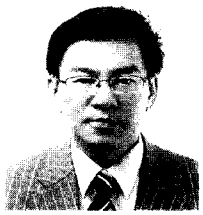
[9] 김재성 외,"바이오 정보를 이용한 U-HealthCare 인증방안 연구", 한국 정보보호학회지 제 17권 제 1호 2007년 2월

[10] 정윤수 외, "Telebiometric 융합 기술 및 국제 표준화 동향", TTA Journal No. 112

〈著者紹介〉

박 동 규 (Dong-Gue Park)
정회원

1992년 : 한양대학교 대학원 전자 공학과 공학박사
1999년~2003년 : 순천향대학교 정보기술공학부 부교수
2004년~현재 : 순천향대학교 정보통신공학과 교수
관심분야 : 네트워크 보안, 유비쿼터스 컴퓨팅 보안

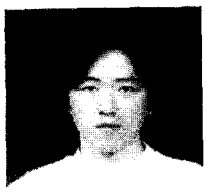


김 재 성 (Kim Jason)
정회원

1986년 2월 인하대학교 전산학과 학사
1989년 2월 동대학원 전산학과 석사
2005년 8월 동대학원 정보통신공학과 박사
1996년 7월 ~ 현재 한국정보보호진흥원 산업지원팀 팀장
<주관심분야 : 바이오인식, 인지과학, 정보보호>

신 용 녀 (Yong-Nyuo Shin)

1999년 2월 숭실대학교 컴퓨터과학과 학사
2001년 9월 고려대학교 컴퓨터과 학과 석사
2002년 1월 ~ 현재 한국정보보호진흥원 산업지원팀 연구원
<주관심분야 : 바이오인식, 정형기법, 정보보호>



황 유 동 (Hwang Yudong)

1998년 순천향대학교 제어계측공학과 공학사
2000년 순천향대학교 전기전자공학과 석사
2003년 순천향대학교 전기전자공학과 정보보호전공 박사과정 수료
<관심분야 : 네트워크 보안, 시스템 보안>

이 유 리 (Lee Youri)

2002년 2월 : 순천향대학교 정보통신공학과 공학학사
2004년 2월 순천향대학교 정보통신공학과 공학석사
2004년~현재 : 순천향대학교 정보통신공학과 박사과정
<관심분야 : 접근제어, 보안>