바이오 인증을 사용한 telemedicine 시스템 설계

정회원 이 유 리*, 황 유 동*, 박 동 규*, 임 황 빈**

Design of telemedicine system using Bio-Authentication

You-ri Lee*, Yu-dong Hwang*, Dong-Gue Park*, Hwang-Bin Yim** ***Regular Members***

요 약

환자 및 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 제공하기 위해 telemedicine 시스템이 선보이고 있다. 현재 telemedicine 시스템의 보안은 ID, Password 및 인증서로 이루어진다. 그러나 이는 정당한 사용자가 아니더라도 ID, Password 정보 및 인증서 비밀키를 알고 있다면 사용이 가능하다. 불법적인 사용자의 telemedicine 시스템의 사용으로 환자의 생명을 다루는 의료 정보들은 여러 가지 보안 위협에 노출 될 뿐 아니라 환자의 프라이버시 침해의 가능성을 내포한다. 따라서 본 논문에서는 telemedicine 시스템의 인증을 강화하기 위해서 고유한 생체 식별 정보를 이용하여 인증하는 시스템을 설계 한다. 이를 위하여 telemedicine 시스템의 보안 요구 사항을 도출하고 신뢰 할 수 있는 telemedicine 시스템을 제공하기 위하여 telebiometrics X.tsm과 X.tai 표준을 기반으로 하여 사용자 및 바이오 디바이스 인증을 강화하는 telemedicine 시스템을 설계한다.

Key Words : Telemedicine, Bio-Authentication

ABSTRACT

Patient and medical information are away to far distance or can not do arrival by time because of various problem , telemedicine system appeared for remote offer of medical information and expert consultation. The security of telemedicine system is currently composed ID, Password and Certificate. But, it's possible to use if user know that it's ID, Password information and certificate key, even if it's not a justifiable user. The medical information dealing with about patient's life are to be exposed to a variety of security threats, as well as the possibility of infringing on the privacy of the patient in using telemedicine system of illegal user. Therefore, in this paper design authentication system using biometric identification information for enabling authentication. we design telemedicine system that reinforcement user and bio-device authentication based on telebiometrics X.tsm and X.tai standard for offer of telemedicine system service that have trust and security requirement elicitation of telemedicine system.

Ⅰ. 서 론

최근 우리 사회는 언제, 어디서나, 누구든지 서비스를 이용 할 수 있는 유비쿼터스에 대한 관심이 높아지고 있으며 이중에서도 건강한 삶과 삶의 질 향상을 보장하는 "이상적인 의료 시스템"을 갈망하는 욕구로 인해 의료 및 의료 정보 서비스를 이용할 수 있는 유비쿼터스 헬스케어에 대한 관심이 높아지고 있다. 또한 세계 각국에서는 이를 위한 기반 조성에 경쟁적으로 나서고 있어 실현 시기는 빨라

* 순천향대학교 정보통신공학과 (thisglass@sch.ac.kr, hwangyudong@gmail.com, dgpark@sch.ac.kr)
** 강원도립대학교 정보통신공학과 (hbinyim@gw.ac.kr)
논문번호 : 07105-1220, 접수일자 : 2007년 12월 20일

질 가능성이 높다. 또한 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.

1970년대 처음으로 telemedicine이 제시되었다.[1] 현재의 telemedicine은 상호 작용하는 정보 통신 기술을 이용하여 원거리에 의료 정보와 의료 서비스를 전달하는 모든 활동을 지칭하고 있으나 이 때는 단지 환자가 의료 상담을 하는 활동만으로 제한되어 있었다.[2] 현재는 환자 및 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 제공하는 시스템을 말하며 환자의 진료뿐만 아니라 의료 행정, 의학 교육, 자문 의뢰 등을 포함하는 포괄적인 개념으로 컴퓨터와 데이터 통신 기술을 이용하여 의학영상, 동영상, 환자 기록 등 각 종 데이터를 주고받은 의료 서비스 기술을 포함한다.

telemedicine 시스템이 제대로 갖춰지면 언제 어느 곳이라도 의료 처치가 가능하며 위급한 환자 발생시 환자의 위치와 현재 생체 신호를 전송, 빠른 시간 내 구급 팀의 도착을 유도하고 오는 도중 필요한 조치를 미리 준비 할 수 있도록 알려주어서 효과적인 응급처리가 가능하다. 하지만 이런 장점을 가진 telemedicine 시스템도 유·무선 네트워크와 각 종 센서 및 유비쿼터스 단말기를 이용해 서비스가 이루어지므로 개인 신상 및 바이오 정보 유출 등 개인 프라이버시 침해의 가능성을 내포하고 있다. 이를 위해서는 암호화 기법을 적용하는 것이 필요하다. 그러나 telemedicine 시스템의 센서 노드에 복잡한 알고리즘을 구현하는 것은 큰 오버헤드가 발생하게 될 뿐만 아니라 보안을 위한 적절한 암호화 키를 분배하는 것이 어렵다.

또한 기존 telemedicine 시스템에서의 사용자 인증은 Id, Password 및 인증서를 사용한 공개키 기반 구조를 사용하고 있다. 그러나 이 또한 인증서의 개인키를 알고 있다면 본인이 아니더라도 서비스를 이용 할 수 있게 된다. telemedicine 시스템은 환자의 소중한 생명을 다루는 시스템이다. 개인키 유출로 인해 권한 없는 사람에게 환자의 정보가 노출되었을 시에 환자의 프라이버시는 보장 받을 수 없게 되며 여러 가지 의료 데이터의 무결성을 보장 받지 못하는 등 보안에 치명적일 수 있다.

따라서 본 논문에서는 지문, 홍채와 같은 인체 고유의 정보를 이용하여 시스템을 사용하는 사용자가 확실한 본인 인지를 인증하여 환자의 데이터 보안, 프라이버시 보장 및 신뢰있는 telemedicine 시스템 서비스를 제공하고자 한다.

Ⅱ. telemedicine 시스템 보안 요구사항

telemedicine 시스템은 개인의 생체 정보 및 주변 환경에 관한 모니터링 정보 등 개인적인 정보를 주로 다루고 있고 유무선 네트워크와 절대적으로 밀접한 연관을 맺고 있다. 따라서 의료 정보 권한과 관련된 다양한 이해 당사자가 존재할 수 있다는 점에서 보안 및 프라이버시 측면의 충분한 보안 서비스가 이루어져야 한다.

telemedicine 시스템에서 제공되어야 하는 보안 서비스는 다음과 같다.

(1) 데이터 기밀성(Data confidentiality)

기밀성은 권한이 없는 사용자로부터 데이터 접근을 보호하는 보안 서비스로 환자 개인적인 비밀 정보와 보안 유지, 개인 프라이버시 보장을 위해 telemedicine 시스템에서 꼭 필요한 서비스이다.

(2) 데이터 무결성(Data integrity)

무결성은 의료 데이터 전송시 또는 저장시에 데이터를 인가하지 않은 방법으로 변경 할 수 없도록 보호하는 보안 서비스로 의료 기록과 의료 데이터의 무결성은 서로 분리될 수 없는 중요한 서비스이다.

(3) 인증(Authentication)

telemedicine에서의 인증이랑 의료 정보의 주체가 되는 송신자와 수신자간에 교류되는 정보의 내용이 변조 또는 삭제되지 않았는지 그리고 주체가 되는 송 수신자가 정당한지를 확인하는 보안 서비스이다. telemedicine 시스템에서는 의료 데이터 서버의 이용 및 정보 교환이 빈번해짐에 따라 의료 데이터 및 그 주체가 적법한지를 확인하는 과정은 필수 불가결한 요소로서 그 필요성은 절대적이다.

(4) 부인봉쇄(Non-repudiation)

부인 봉쇄는 제 삼자에게 어떤 사실의 발생을 증명 할 수 있는 인증 서비스와 무결성 서비스가 결합된 서비스라고 볼 수 있다. 이는 의료 데이터를 송신한 적이 있는 송신자가 해당 데이터가 자신으로부터 데이터가 왔음을 부인하는 것을 봉쇄하는

보안 서비스이다.

(5) 익명성(Anonymity)

익명성은 의료 정보의 주체가 되는 송신자가 보낸 데이터에 의해서 제 3자가 그 데이터로부터 개인에 관한 어떤 정보도 얻을 수 없는 상태를 말한다. 즉, telemedicine 시스템에서 의료 정보 활용 시에 개인 정보를 통해서 개인을 식별하지 못하도록 하는 보안 서비스이다.

(6) 감사기록(auditing)

감사기록은 telemedicine 시스템에서 의료 데이터를 이용하는 모든 행동에 대한 책임을 추적하기 위해 모든 사건을 기록하고 유지 및 검토하는 보안서비스이다.

telemedicine 시스템의 보안 위협에 대해서 기밀성, 무결성, 인증, 부인 봉쇄 서비스를 제공하기 위해서 공개키 기반 구조(PKI : Public Key Infrastructure)를 사용한다. 또한 익명성 보장을 위해서 권한 관리가 이루어져야 하며 이를 위해 권한 관리 기반 구조(PMI : Privilege Management Infrastructure)를 사용하여야 한다. 또한 의료 데이터에 모든 행위에 대하여 책임을 추적하기 위해 이루어지는 감사기록을 위하여 로깅 서비스를 제공하여야 한다.

위의 모든 서비스들을 제공하기 위해 우선적으로 이루어져야 하는 서비스는 인증 서비스이다.

telemedicine 시스템에서 보안 서비스를 제공하기 위해서 사용자 인증 메커니즘, 생체 및 환경 정보를 센싱, 모니터링 하기 위한 의료 센서 인증 메커니즘과 같은 인증 메커니즘이 필요하다. 특히, telemedicine 시스템은 사람의 생명과 관련된 의료 데이터를 다루기 때문에 어느 무엇보다 강력한 인증 체계가 필요하며 인증 서비스에 신뢰성 보장은 필수적이다. 현재 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. 이 표준들 중에 X.tsm (telebiome- trics system mechanism)은 클라이언트와 서비스 제공자 사이에서 biometric 인증 프로토콜을 제공하는 표준으로 공개키 기반 구조 기반의 Telebiometrics 시스템의 다양한 모델과 메커니즘을 정의하고 바이오 인식 기술과 데이터를 활용한 공개키 기반구조 인증 모델과 TLS 프로토콜을 제안하고 있다. 이를 기반으로 바이오 인증을 사용한 telemedicine 시스템을 구성하는 것이 가능하게 된다.

Ⅲ. 바이오 인증을 사용한 telemedicine 시스템

바이오 인증을 사용한 telemedicine 시스템은 현재 대표적인 telemedicine 시스템 Ipath[3]와 OpenEmd[4], TeleCardio-FBC[5], CodeBlue[6], Wire Sensor Body Area Network(WSBAN)[7], Medintagra Web[8] 을 고려하였다.

바이오 인증을 사용한 telemedicine 시스템에서는 위의 7가지 telemedicine 시스템에서 사용하는 ID/Password나 공인 인증서 기반 뿐 아니라, 지문과 홍채와 같은 다양한 생체 식별 정보를 사용하여 사용자 인증을 함으로써 한층 강화된 보안 서비스를 제공 받을 수 있다.

3.1 바이오 인증을 사용한 telemedicine 시스템 구성도

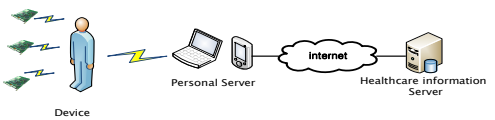

그림 1. 바이오 인증을 사용한 telemedicine 시스템 구성도

바이오 인증을 사용한 telemedicine 시스템 구성도는 그림 1과 같이 디바이스, 퍼스널 서버, 의료정보 서버로 이루어진다. telemedicine 시스템은 생체 및 환경 정보를 센싱, 모니터링 하기 위한 의료 센서로부터 의료 데이터와 바이오 인증을 위한 인증 데이터를 디바이스로부터 수집하고, 수집된 데이터는 유무선 네트워크를 통해서 생체 데이터 분석

과 건강 피드백을 담당하는 의료 정보 서버로 전달된다. 전달된 인증 데이터를 이용하여 신뢰성 있는 사용자 인증을 하고, 전달된 의료 데이터를 이용하여 의료 정보 서버는 건강 상태, 생활패턴 등에 관한 건강 자료를 분석하고 이와 관련된 경고, 현장진단처방, 단순 주지 등의 피드백이 모바일 장치나 다른 사용자 터미널을 통하여 사용자에게 전달된다.

3.2 바이오 인증을 사용한 telemedicine 시스템 보안 프레임 워크

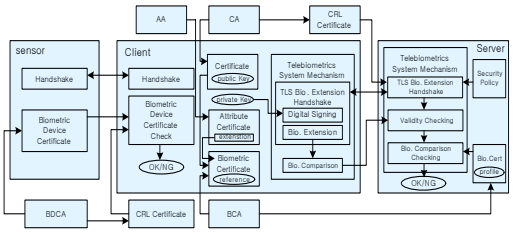

그림 2. 바이오 인증을 사용한 telemedicine 시스템 보안 프레임 워크

바이오 인증을 사용한 telemedicine 보안 프레임 워크는 위 그림 2와 같다. telemedicine 시스템에서 센서들은 환자의 생체 정보나 환경 정보 등을 센싱하여 의료 정보 서버로 보내주는 의료 데이터 수집 단계의 역할을 하게 된다. 이때 수집된 의료 정보들의 신뢰성을 확보하기 위하여 센싱하는 모든 센서들은 바이오 디바이스 인증서(BDC: Biometric Device Certificate)를 가지게 된다. 이때 사용되는 바이오 디바이스 인증서는 X.509 인증서를 따르는 홈디바이스 인증서를 사용한다. 따라서 사용자는 바이오 디바이스 인증서를 소유한 센서에 의해서 수집된 의료 정보는 신뢰하게 된다. 또한 사용자는 사용자 인증을 위한 공개키 기반구조 인증서와 사용자의 권한 인증을 위한 속성인증서 그리고 홍채, 지문과 같은 생체 정보 인증을 위한 바이오 인증서를 발급 받아야 한다. 발급 받은 공개키 인증서를 사용하여 사용자 인증을 받고, 의료 데이터를 사용하기 위해 신뢰성 있는 인증을 위하여 자신의 바이오 정보를 이용하여 자신의 대한 인증을 받게 된다. 모든 사용자 인증이 끝난 후에 사용자가 이용하고자하는 서비스에 대한 권한 인증을 위하여 속성 인증서를 이용한 속성 인증 과정을 거치게 된다. 이를 통하여 자신의 권한에 맞는 안전한 의료 서비스를 제공 받을 수 있다.

3.3 바이오 인증을 사용한 telemedicine 인증 과정

바이오 인증을 사용한 telemedicine 인증 과정을 크게 나누면 세 가지로 볼 수 있다. 센서들에 의해서 수집되는 정보들의 신뢰성을 확보하기 위한 디바이스 인증, 의료 데이터에 접근하기 위하여 바이오 정보를 이용한 사용자 인증, 그리고 자신의 권한에 맞는 의료 데이터에 접근하기 위한 사용자 권한 인증으로 나눌 수 있다. 바이오 인증을 사용한 telemedicine 시스템의 각 인증 과정은 다음과 같다.

(1) 디바이스 인증

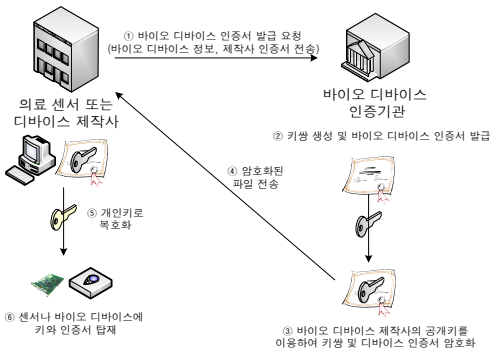

그림 3. 바이오 인증을 사용한 telemedicine 시스템에서의 디바이스 인증서 발급 과정

telemedicine 시스템에서 디바이스 인증을 위해서 디바이스 사용자는 바이오 디바이스 인증기관(BDCA : Biometric Device Certificate Authority)에서 바이오 디바이스 인증서(BDC : Biometric Device Certificate)를 발급 받게 된다. 바이오 디바이스 인증서는 홈네트워크 디바이스 인증서를 사용하며 홈 네트워크 디바이스 인증서는 X.509의 기본 골격을 따라서 크게 tbsCertificate, signature Algorithm, signatureValue의 세 가지 필드로 구성된다. tbsCertificate 필드는 버전(Version), 일련번호(Serial Number), 발급자(Issuer), 유효기간(Validity), 소유자 공개키 정보(Subject Public Key Info), 확장(Extension) 필드로 구성된다. 발급된 바이오 디바이스 인증서를 통하여 신뢰성 있는 의료 데이터의 수집이 가능하다.

(2) 사용자 인증

telemedicine 시스템을 사용하는 사용자는 기밀성, 무결성, 인증, 부인 봉쇄의 보안 서비스를 제공받기 위해서 인증기관으로부터 인증서를 발급 받아

야 한다. 이는 공개키 기반의 X.509 인증서로 사용자는 등록기관(RA : Registration Authority)에 가서 사용자 확인을 받은 후 인증기관(CA : Certificate Authority)으로부터 인증서를 발급 받게 된다. 이를 통하여 사용자 인증이 가능하다. 다음 그림 4는 공개키 기반 구조 인증서 발급 과정을 보여준다.

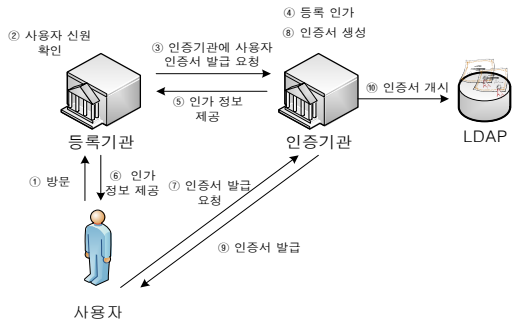

그림 4. 바이오 인증을 사용한 telemedicine 시스템에서의 공개키 기반 구조 인증서 발급 과정

또한 telemedicine 시스템의 특성상 공개키 기반 인증서를 통한 사용자 인증 뿐 아니라 한층 강화된 사용자 인증 방식이 필요하다. 따라서 사용자의 다양한 생체 식별 정보를 사용하는 인증 방식을 사용한다. 이 인증 방식을 사용하기 위해서 사용자는 바이오 인증서를 발급 받아야 한다. 다음 그림 5는 바이오 인증서 및 바이오 알고리즘 인증서 발급 과정을 보여준다.

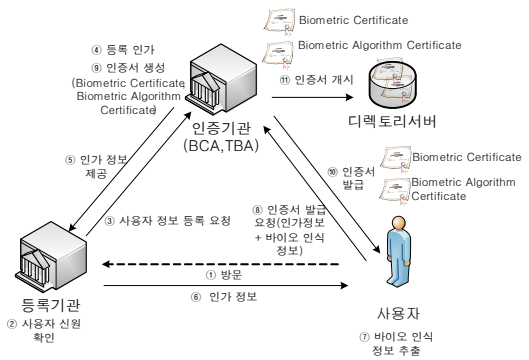

그림 5. 바이오 인증을 사용한 telemedicine 시스템에서의 바이오 인증서 및 바이오 알고리즘 인증서 발급 과정

바이오 인증서는 바이오 인증기관(BCA : Biometric Certificate Authority)으로부터 발급이 가능하다. 바이오 인증이 필요한 사용자는 바이오 인증기관으로 가서 자신의 생체 정보에 대한 확인을 받고 바이오 인증기관에서는 생체 정보 검증을 위해 바이오 템플릿(Biometric Template)을 생성하고 검증한 다음 템플릿 저장소에 등록하면서 바이오 인증서(BC : Biometric Certificate)를 생성하고 서명을 한 후 저장하게 된다. 또한 사용자는 텔레바이오 메트릭 인증기관(TBA : Telebiometric Authority)로부터 바이오 알고리즘 인증서(BAC : Biometric Algorithm Certificate)를 발급 받아야 한다. 바이오 알고리즘 인증서는 바이오 알고리즘, 매칭 알고리즘, 한계값, 보안 레벨 그리고 바이오 관련 요소 정보들이 포함되어 있다. 즉 telemedicine 시스템에서 사용자 생체 정보를 이용한 인증을 위해서는 다음 그림 6과 같은 과정이 이루어져야 한다.

그림 6. 바이오 인증을 사용한 telemedicine 시스템에서의 생체 정보를 이용한 인증 과정

① 사용자가 소지하고 있는 바이오 알고리즘 인증서를 인증을 받기 위한 의료 정보 시스템으로 보낸다.
② 의료 정보 시스템은 바이오 보안 레벨 리스트로부터 바이오 인증 요소들을 추출한다.
③ 추출해야 되는 바이오 인증 요소들을 사용자에게 전달한다.
④ 사용자는 ③번을 통해 받은 바이오 인증 요소에 따라 바이오 정보를 추출한다.
⑤ ④번 과정을 통해 추출된 정보를 의료 정보 시스템으로 보낸다.
⑥ ⑤번 과정을 통해 받은 바이오 정보와 바이오 인증서의 검증을 통해 저장되어있던 바이오 템플릿을 가져와 비교한다.
⑦ 인증 결과를 사용자에게 반환한다.

(3) 사용자 권한 인증

telemedicine 시스템에서 사용자는 자신임을 증명해야 할 뿐 아니라 자신이 이용하는 서비스에서의 자신의 역할에 대한 권한을 인증 받아야 한다. 이를 위해서 사용자 속성 인증서(AC : Attribute Certificate)를 발급 받아야 한다. 사용자는 속성 기관(AA : Attribute Authority)에 가서 자신의 권한을 인증 받

게 된다.

바이오 인증을 위한 telemedicine 시스템에서 바이오 알고리즘 인증서와 바이오 인증서 및 사용자 권한을 인증하기 위한 사용자 속성 인증서를 사용한 사용자 인증 프로세스 흐름도는 다음 7과 같다. 이 과정을 통하여 사용자는 신뢰성 있는 telemedicine 시스템 서비스를 제공 받을 수 있다.

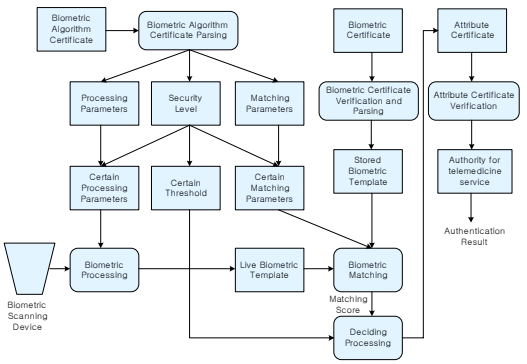

그림 7. 바이오 인증을 사용한 telemedicine 시스템에서의 인증 프로세스 흐름도

V. 바이오 인증을 사용한 telemedicine 시스템 서비스 사용 예

바이오 인증을 사용한 telemedicine 시스템에서 서비스 제공을 위한 시나리오는 다음 8과 같다.

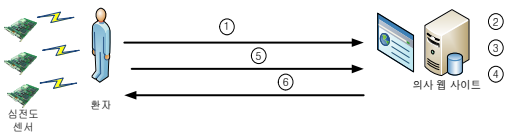

그림 8. 바이오 인증을 사용한 telemedicine 시스템 서비스 제공을 위한 시나리오

① 환자가 의사 웹사이트에 심전도 센서로부터 얻어온 자신의 심전도 상태에 대한 상담을 요청한다.
② 의사 웹 사이트는 환자의 인증을 확인한 후
③ 의사에게 환자의 심전도 상태에 대한 소견서를 요청하고,
④ 의사로부터 서명된 응답 메시지를 전송받는다.
⑤ 환자는 의사 웹사이트 접근을 위해 다시 사용자 인증과 의사의 응답 메시지를 요청한다.
⑥ 저장된 의사의 응답메시지를 환자에게 제공한다.

위 서비스를 제공받기 위해서 우선 디바이스 인증 및 사용자 인증이 필요하다. 다음 그림 9는 디바이스 인증 모델을 보여준다.

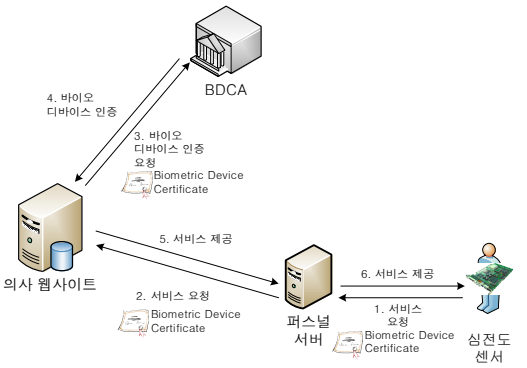

그림 9. 바이오 인증을 사용한 telemedicine 시스템에서의 디바이스 인증 모델

환자는 심전도 센서를 통하여 얻어진 데이터를 의사에게 심전도 상태에 대한 상담을 요청하려고 한다. 따라서 심전도 센서에 대한 바이오 디바이스 인증 단계가 필요하다. 심전도 센서에 대한 인증이 끝났으면 환자 개인의 인증 단계가 이루어져야 한다. 다음 그림 10과 같이 바이오 인증을 사용하여 환자는 자신의 심전도 상태에 대한 데이터를 의사 웹 사이트에 전송 하게 된다.

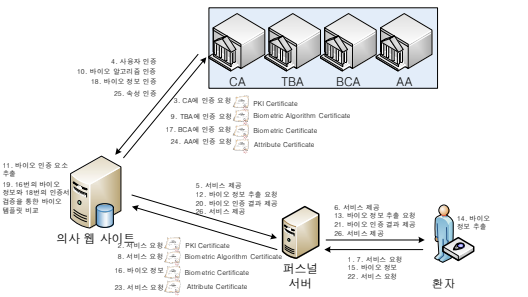

그림 10. 바이오 인증을 사용한 telemedicine 시스템에서의 사용자 및 권한 인증 모델

의사 웹 사이트는 의사에게 환자의 심전도 상태에 대한 응답을 요청하고 의사에 대한 응답 메시지를 전송 받게 된다. 의사 또한 환자의 인증 단계와 같은 인증 단계를 거쳐서 의사의 속성을 인증 받은 후 서명된 응답 메시지를 전송하게 된다. 이후 환자는 위와 같은 바이오 인증 단계를 다시 거친 다음에 의사 웹 사이트에 자신의 심전도 검사 결과 확인 요

청시에 의사 웹사이트는 의사의 소견서를 환자에게 제공하게 된다. 이를 통하여 환자는 신뢰 할 수 있는 telemedicine 서비스를 이용 할 수 있게 된다.

Ⅵ. 결 론

본 논문에서는 telemedicine 시스템에 필요한 보안 요구사항을 도출하고 이 요구사항들을 만족 할 수 있는 telemedicine 서비스를 제공하기 위하여 기존의 ID, Password 및 인증서 기반의 인증 뿐 아니라 인체 고유 정보를 이용하는 바이오 인증을 사용한 telemedicine 시스템을 설계하였다.

설계된 시스템은 인증시 인체 고유의 정보를 이용함으로써 시스템을 사용하는 사용자가 확실한 본인 인지를 확인 할 수 있다. 이를 통한 환자의 데이터 보안, 프라이버시 보장 및 신뢰 있는 telemedicine 시스템 서비스를 제공한다.

또한 본 논문에서 제시한 바이오 인증을 사용한 telemedicine의 디바이스 인증 모델은 홈네트워크 디바이스 표준을 기반으로 하였으며 사용자 인증 모델은 Telebiometrics X.tsm과 X.tai 표준을 기반 설계되어 구현이 가능하다.

앞으로 바이오 인증을 사용한 telemedicine 시스템에서의 사용자 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〕 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, volume 15 of LNI. GI, April 2002

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

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

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

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

황 유 동 (Yu-dong Hwang) 정회원

1998년 2월 순천향대학교 제어계측 공학과 공학사

2000년 8월 순천향대학교 전기전자공학과 석사

2003년~현재 순천향대학교 전기전자공학과 정보보호전공 박사과정

<관심분야> 네트워크 보안, 시스템 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

임 황 빈 (Hwang-Bin Yim) 정회원

2003년 순천향대학교 정보통신공학과 공학박사

2003년~현재 강원도립 대학 정보통신과 조교수

<관심분야> 통신응용시스템, 광통신 , 정보 보호