한국지능시스템학회 논문지 2010, Vol. 20, No. 5, pp. 659-664

바이오인식을 이용한 원격의료에서의 개인정보보호

Personal Information Protection for Biometric Verification based TeleHealth Services

신용녀* · 전명근*+

Yong-Nyuo Shin* and Myung Geun Chun*+

* 한양사이버대학교 컴퓨터공학과

*+ 충북대학교 전자공학부

요 약

본 논문에서는 바이오인식기반 원격의료시스템에 있어서 바이오정보를 포함한 개인 프라이버시 정보를 보호하기 위한 프레임워크를 제시한다. 바이오인식은 편의성 및 의료 환경의 특수성으로 원격의료시스템에 적합한 인증수단 일수 있지만 바이오정보가 분실되거나 다른 사람에 의해서 도용되었을 경우 비밀번호나 ID처럼 사용자 요구에 따라 쉽게 변경하기가 어렵다는 치명적인 단점을 지니고 있기 때문에, 바이오정보를 이용한 인증시스템 구축 시 민감한 프라이버시 정보의 한 유형인 개인 바이오정보를 보호하기 위한 정보보호 프레임워크에 기반 하여 원격의료시스템이 구축되어야 한다.

먼저 바이오인식 시스템의 구성요소와 동작을 살펴보고 바이오인식기반 원격의료 시스템이 만족해야할 특화된 보안 요구사항 대한 정의를 내린다. 이어서 바이오인식기반 원격의료 시스템의 모델을 정의하고 프라이버시 정보와 바이오정보가 공격당할 수 있는 보안 위협과 이에 대처할 수 있는 대응방안을 제시한다. 본 논문에서는 다양한 보안 위협 요인들에 대처하기 위하여 2단계인증 프로토콜을 제시한다. 마지막으로 바이오 인식기반 원격의료 프레임워크를 적용한 시스템의 구성요소에 대한 기능 요구사항을 기술함으로서 바이오인식기반 원격의료 보안 대책에 기반 시스템 구축 시 사용자의 개인정보를 보호함과 동시에 높은 보안능력을 갖는 고성능의 개인인증용 바이오인식 시스템을 구축에 도움을 줄 수 있다.

키워드 : 바이오 인식, 원격의료, 정보보호, 프라이버시

Abstract

This paper provides an integrated framework for biometric data and private information protection in TeleHealth. Biometric technology is indispensable in providing identification and convenience in the TeleHealth environment. Once biometric information is exposed to mallicious attacker, he will suffer great loss from the illegferuse of his biometric data by someone else because of difficulty of change not like ID and password. We have to buil by someone esystem data bon the integrated framework for biometric data and private information protection in TeleHealth. First, we consider the structure of the biometric system and the security requirements of y someone esystem data bon the biometrics. And then, we define the TeleHealth system model and provide the vulnerabilities and countermeasures of the biometric-data by someone eintegrated model.byhe TeleHealth sse bec requires two-phata authentication for countermeasure. Finally, we made some functionferrequirements for main componenets of biometric-data bintegrated TeleHealth system framework to protect biometric data.

Key Words : Biometrics, Telehealth, Information Security, Privacy

1. 서 론

바이오인식 기술은 인터넷 뱅킹, 금융서비스, 인터넷을 통한 비대면 거래에 있어서 중요한 정보보호 기법의 하나로 이용되고 있으며[1], 원격의료에 있어서도 사용자 인증에 있어 환자, 의사, 연구원 등 사용자의 정보 및 사생활 침해를 막고 정확한 의료정보의 전달을 위하여 바이오인식 기반의 인증 서비스를 제공하는 사례가 많아져 주목받고 있다.[2-3].

사용자의 건강과 생명에 관련된 의료서비스를 제공하기 위한 원격의료에 있어서도 사용자 인증에 오류가 있는 경우 치명적인 의료문제가 발생할 수 있기 때문에 본인확인을 강화하기 위하여 바이오인식을 사용하는 사례가 많아지고 있다[4]. 원격의료 서비스를 만성질환자가 사용하는 경우 기존의 패스워드, PKI 기반의 사용자 인증은 비밀번호를 입력해야 하는 불편함이 있다. 이런 경우, 바이오인식을 채택하여 안면, 지문 등의 신체정보를 이용하기 때문에 사용자 편의성을 제공할 수 있다. 그러나, 바이오정보가 분실되거나 다른 사람에 의해서 도용되었을 경우에 비밀번호나 ID처럼

접수일자 : 2010년 8월 13일
완료일자 : 2010년 10월 8일
이 논문은 2010년도 정부(교육과학기술부)의 재원으로 "한국연구재단의 기초연구사업(No. 2010-0024037)" 지원을 받아 연구되었음
+ : 교신저자

사용자가 원하는 경우에 쉽게 변경하기가 어렵다는 치명적인 단점을 지니고 있기 때문에, 바이오정보를 이용한 인증 시스템을 구축하기 위해서는 프라이버시 정보인 바이오정보를 보호하기 위한 보안 프레임워크 구축이 필수적이다.

이에, 본 논문에서는 원격의료 환경에서 바이오정보 전송에 있어서의 보안 위협으로부터 안전한 원격의료 서비스를 제공하기위한 사용자 인증과, 통신상에서의 정보 획득, 변조, 불법접근 등과 같은 다양한 보안위협으로부터 바이오정보를 보호하기 위한 통합 보안 프레임워크를 제시한다. 원격의료 환경에 통합 보안프레임워크를 적용하는데 있어서, 원격의료환경 만이 가질 수 있는 바이오정보 전송상의 보안 문제에 대한 대처방안을 제시함으로써, 바이오인식기반 원격의료 시장 활성화에 기여할 수 있다.

2. 바이오인식기반 원격의료 보안 요구사항

바이오인식 시스템은 신원인증을 바라는 대상자의 바이오정보를 기초로 신분확인을 원하는 대상자가 본인이 맞는지의 여부를 확인하는 시스템이라고 할 수 있다. 보통 많이 사용되고 있는 바이오정보로는 지문, 얼굴, 홍채, 손등정맥, 지정맥 등의 정적 바이오정보와 서명, 음성, 걸음새와 같은 대상자의 동적 바이오정보를 이용하는 것으로 나눌 수 있다. 이러한 생체인식시스템의 구성도를 국제표준기구(ISO)의 기준에 따라 나타낸 것이 그림 1이다.

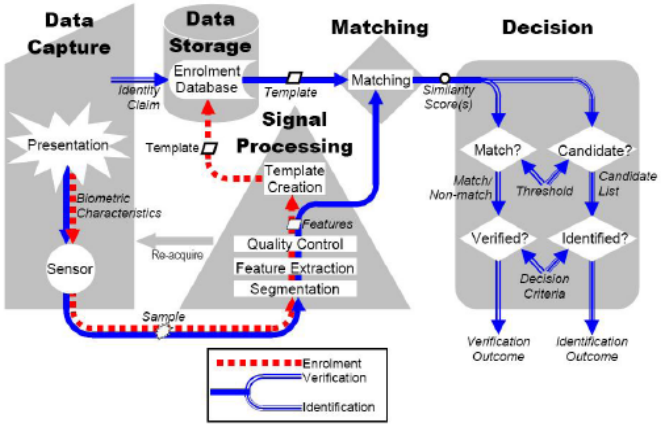

그림 1. 바이오인식 시스템의 구성도[9]
Fig. 1. Biometric System Diagram

상기의 그림에서 볼 수 있듯이 바이오인식 시스템의 크게 3가지의 역할로 나누어서 생각해 볼 수 있다. 첫 번째로 등록(enrollment)과정이다. 이 기능은 제시되는 대상자의 바이오정보로부터 개인식별(identification)과정이나 개인인증(verification)과정에서 필요로 하는 바이오인식 템플릿을 생성하고 저장하는 과정을 의미한다. 개인식별과정은 주어진 바이오인식 템플릿에 대해서 이것이 누구의 것인지 신원을 밝히는데 목적이 있다. 이때 바이오인식시스템은 저장장치내의 모든 바이오인식 템플릿과의 비교를 통하여 가장 유사도가 높은 대상자의 식별정보를 제공하게 된다. 이러한 이유로 이를 1:N 비교라고도 부른다. 한편, 개인인증과정은 대상자가 본인의 바이오인식 템플릿과 함께 개인식별용 ID를 제시하게 되면, 주어진 바이오인식 템플릿에 대해서 이것이 주장하고 있는 본인이 맞는지의 여부를 판별하는데 목적이 있다. 이때 바이오인식시스템은 저장장치내의 해당 ID의 바이오인식 템플릿과의 비교를 통하여 대상자의 인증여부를 결정하게 된다. 이러한 이유로 이를 1:1 비교라고도 부른다[15].

위와 같은 바이오인식 시스템을 응용한 원격의료 시스템이 만족해야할 보안 요구사항은 일반적인 보안 요구사항인 정보의 기밀성, 무결성, 가용성의 측면을 포함하여 의료정보가 실수나 고의로 공개되지 않도록 하는 한편, 변조되지 않고 언제나 접근이 용이하도록 하는 일련의 활동이라 볼 수 있다. 한편 바이오인식기반 원격의료서비스를 위한 보안 측면에서는 특화된 다음과 같은 부가적인 보안 요구사항을 고려해야 한다.

- 바이오인식기반 원격의료 환경은 사용자의 생명을 다루는 의료서비스를 제공하기 때문에 속도가 보장되어야 한다. 또한 원격의료 센서와 단말기에서 취합되는 의료정보가 대용량이기 때문에 경량화된 인증이 요구된다. 일반적인 인증서 기반의 단말기 인증의 경우, 키 분배와 인증서 상태확인이 필요하기 때문에 유무선 환경에 적합하지 않다. 따라서 경량화된 단말기 인증이 제공됨으로써 응급처리 서비스가 가능하며 대용량의 의료정보의 송수신이 가능하다.

- 바이오인식기반 원격의료 환경에서 송수신하는 의료정보는 디바이스 인증서 기반으로 인한 키 관리 및 인증서 상태확인에 대한 통신부하를 최소화하면서 무결성을 제공하기 위해 전자서명 방식이 아닌 경량화를 위해 MAC(Message Access Control) 방식의 무결성을 제공해야 한다.

- 바이오인식기반 원격의료 환경에서 송수신하는 의료정보는 디바이스 인증서 기반으로 인한 키 관리 및 인증서 상태확인에 대한 통신부하를 최소화하면서 비밀성을 제공하기 위해 Diffie-Hellman 방식의 키 교환을 이용한 비밀성을 제공해야 한다.

- 바이오인식기반 원격의료 환경에서 송수신하는 의료정보는 민감한 개인정보로써 유출되는 경우, 개인에 대한 많은 피해가 예상된다. 따라서 TeleHealth 서비스에서는 개인정보에 대한 워터마킹, 디지털 권한 관리 등을 제공하여 유출시 유출경로를 추적할 수 있어야 한다.

- 바이오인식기반 원격의료 센터에 수집된 개인의 의료정보는 생성, 전송, 저장, 폐기되는 전과정에 걸쳐서 로그 형태의 감사기록을 제공해야 하며 의료인, 운영자 등의 개인 의료정보 열람하는 경우, 권한관리와 감사추적을 통해 안전성이 보장되어야 한다.

- 바이오인식기반 원격의료 센터에 수집된 개인의 의료정보는 생성, 전송, 저장, 폐기되는 전과정에 걸쳐서 로그 형태의 감사기록을 제공해야 하며 의료인, 운영자 등의 개인 의료정보 열람하는 경우, 권한관리와 감사추적을 통해 안전성이 보장되어야 한다.

- 바이오인식기반 원격의료 정보에서 나오는 데이터 중

특히 수치 데이터는 환자의 생명과 직접적인 연관 관계가 있는 데이터 이므로 측정치, 투약량 등 전송 데이터의 정확성이 보장되어야 한다.

3. 바이오인식기반 원격의료 통합 프레임워크

원격의료 바이오정보 전송에 있어서의 위협으로부터 안전한 원격의료 서비스를 위한 사용자 인증과, 통신상에서의 정보 획득, 변조, 불법접근 등과 같은 다양한 위협으로부터 바이오정보를 보호하기 위한 프레임워크를 제시한다. 바이오인식기반 원격의료는 사용자의 건강에 관련된 의료서비스를 제공하기 때문에 본인 확인 여부가 가장 중요한 요소이다. 기존의 패스워드 기반의 사용자 인증방식은 오픈 네트워크에서 노출될 수 있는 취약성을 가지고 있다. 인증서 기반의 사용자 인증은 키 관리 문제와 전자서명 비밀번호를 입력해야 하는 불편함이 있다. 몸이 불편한 만성질환자에게 바이오인식기반 원격의료 단말기에 접속할 때마다 전자서명 비밀번호를 입력해야 하는 것은 어려움이 따른다. 따라서 바이오인식기반 원격의료 환경에서 본인확인과 편의성을 제공하기 위해서는 바이오인식 도입이 필수적이다.

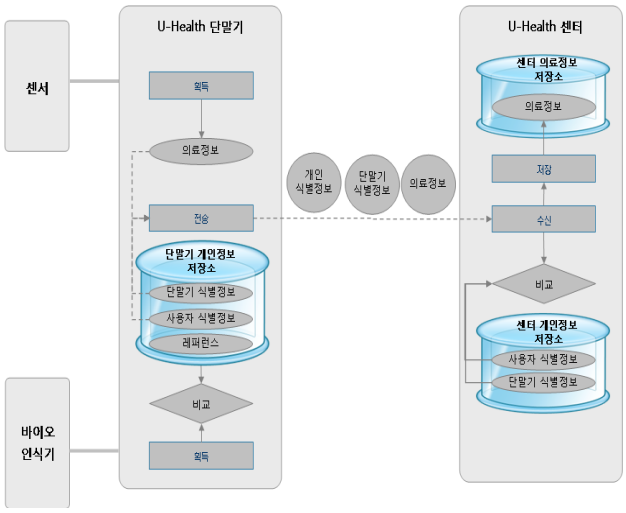

그림 2. 바이오인식기반 원격의료 통합 모델[12]
Fig. 2. Integrated Framework for Telebiometric data protection in TeleHealth Services

바이오인식기반 원격의료 환경 서비스는 2단계 인증이 요구되며 환경은 사용자, 바이오인식 센서, 바이오인식기반 원격의료 센서, 바이오인식기반 단말기, 바이오인식기반 원격의료 센터의 5가지 구성요소를 가진다. 바이오인식기반의 바이오인식기반 원격의료 통합 모델의 취약점은 그림 3과 같다.

1단계는 사용자가 바이오인식 센서를 통해 TeleHealth 단말기에 바이오인증을 한다. 2단계는 TeleHealth 단말기는 TeleHealth 센터에 사용자 인증과 TeleHealth 단말기 인증을 한 후 건강정보를 TeleHealth 센터로 전송한다. 통합모델의 위협은 그림 3과 같이 정의될 수 있다[12].

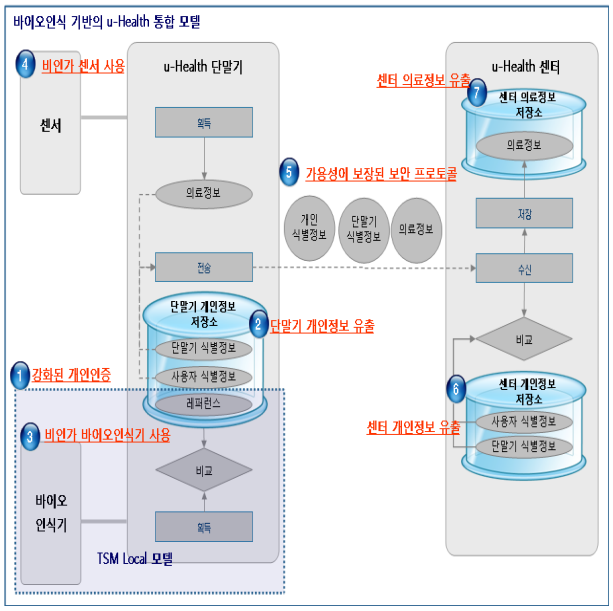

그림 3. 통합모델의 위협 분석[12]
Fig. 3. Analysis on threats of integrated model

바이오인식기반 원격의료 보안 프레임워크가 만족해야하는 요구사항들은 기밀성 무결성과 같은 전통적인 보안 요구사항을 비롯하여 프라이버시 보호를 위해, 본 논문에서 제안하는 통합모델에서 각 보안 위협별 대응 방안은 표1과 같이 대응이 가능하다. TSM(Telebiometric System Mechanism) 로컬(Local) 모델, ACBio(Authentication Context for Biometrics), 기기인증서 표준, DB보안의 기존 표준 및 기술로 대응이 가능하며 단말기 개인정보 유출, 센터 개인정보 유출, 가용성이 보장된 보안 프로토콜에 대하여 정의한다.

표 1. 통합모델의 위협 대응방안[12]
Table 1. Definition of threats of the integrated model

보안대상	보안위협	대응방안
u-Health 단말기	1 강화된 개인 인증	• 바이오인식 기반의 개인인증 제공 • TSM Local 모델 표준 채택 - 바이오정보 레퍼런스의 본인통제권 강화(프라이버시 보호) - u-Health 센터의 바이오인식 부하 감소(가용성 보장)
	2 단말기 개인정보 유출	• 단말기 개인정보 저장소 보호 기술 • TSM Local 모델은 보안 프로토콜이 정의되어 있지 않으며 바이오정보 레퍼런스 저장에 대한 보호 기술이 명시되지 않음
바이오인식기	3 비인가 바이오인식기 사용	• ACBio 표준 채택(인증서 기반의 신뢰성 제공)
u-Health 센서	4 비인가 센서 사용	• 기기인증서 표준 채택(인증서 기반의 신뢰성 제공)
통신 프로토콜	5 가용성이 보장된 보안 프로토콜	• 경량화된 통신 프로토콜 기술 • u-Health 서비스의 경량화된 개인인증 및 기기인증
u-Health 센터	6 센터 개인정보 유출	• 센터의 개인정보 저장소 보호 기술 제안 • 개인 식별정보와 기기 식별정보에 대한 연관 기술
	7 센터 의료정보 유출	• 상용화된 DB보안 기술 도입

4. 바이오인식기반 원격의료에서의 인증 및 응용

TeleHealth 환경에서 사용자 인증과 TeleHealth 서비스 측면이 고려되어야 한다. TeleHealth는 원격에서 사용자의 건강에 관련된 의료서비스를 제공하기 때문에 본인 확인 여부가 가장 중요한 요소이다. 따라서 TeleHealth 환경에서 본인확인과 편의성을 제공하기 위해서는 바이오인식 도입이 필수적이다. TeleHealth 환경에서 바이오인식이 통합되어야 하는 이유는 다음과 같다. 첫째, TeleHealth는 사용자의 건강과 생명에 관련된 의료서비스를 제공하기 때문에 사용자 인증에 오류가 있는 경우 치명적인 의료문제가 발생할 수 있기 때문에 본인확인을 강화하기 위하여 바이오인식으로 해야 한다. 둘째, TeleHealth를 만성질환자가 사용하는 경우 기존의 패스워드, PKI 기반의 사용자 인증은 비밀번호를 입력해야 하는 불편함이 있다. 바이오인식을 채택하여 안면, 지문 등의 신체정보를 이용하기 때문에 사용자 편의성을 제공해야 한다.

TeleHealth 환경은 사용자, 바이오인식 센서, TeleHealth 센서, TeleHealth 단말기, TeleHealth 센터의 5가지 구성요소를 가진다. 본 연구에서는 그림 4와 같이 TeleHealth 환경에서 2단계 인증구간을 구성하였다.

- 1단계 : 사용자는 바이오인식 센서를 통해 TeleHealth 단말기에 바이오인증을 한다.

- 2단계 : TeleHealth 단말기는 TeleHealth 센터에 사용자 인증과 TeleHealth 단말기 인증을 한후 건강정보를 TeleHealth 센터로 전송한다.

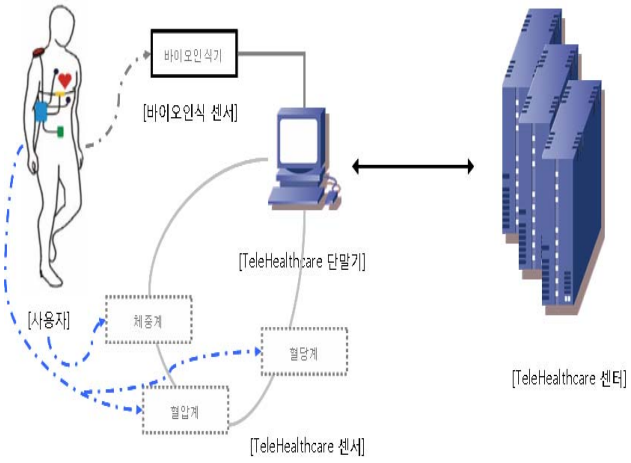

그림 4. TeleHealth 2단계 인증
Fig. 4. TeleHealth 2-step authentication

TeleHealth 단말기에는 사용자 정보를 개별적으로 등록, 관리하도록 한다. 사용자와 TeleHealth 단말기간 인증 절차는 다음과 같다.

(a) 등록된 사용자는 바이오인식 센서를 통해 안면, 지문을 입력한다.
(b) TeleHealth 단말기는 획득된 바이오인식 샘플에서 특징점을 추출한 후 순차적으로 단말기내의 사용자 정보의 참조 바이오인식과 1:N 매칭을 수행한다.
(c) 매칭이 성공된 사용자에 대하여 TeleHealth 센서에 접근인가를 제공한다.

사용자에 대하여 바이오인식이 완료된 TeleHealth 단말기를 이용하여 TeleHealth 센터에 접속하기 위한 User Profile 기반의 인증방식을 제공한다. TeleHealth 단말기에 안전하게 저장되어 있는 User Profile 내에 인증 키(Authentication Key)를 기반으로 식별 및 인증 서비스를 제공한다. TeleHealth 환경에서 TeleHealth 단말기는 TeleHealth 센터에 등록되어 있다. 사용자 인증 및 TeleHealth 단말기 인증를 위하여 경량화된 인증 값(Authentication Value)을 통해서 이루어진다. TeleHealth 단말기와 TeleHealth 센터의 보안 채널을 확립하기 위한 암호 키 관리 프로토콜은 효율적으로 시스템 자원을 활용하기 위하여 ECDH(Elliptic Curve Diffie-Hellman) 키 교환 암호 알고리즘을 사용한다. TeleHealth 단말기와 TeleHealth 센터는 공개키 쌍을 생성하고 생성된 공개키 정보를 상호 교환하여 Master Key를 생성한다. TeleHealth 단말기에 적용되는 공개키 생성 메커니즘은 제약된 환경을 고려하여 Static Key 쌍 생성 메커니즘으로 공개키를 생성한 후 지속적으로 사용하게 된다. 반면에 TeleHealth 센터는 TeleHealth 단말기가 접속 시 마다 생성해서 쓰는 Ephemeral Key 쌍 생성 메커니즘을 적용한다. 암호키 관리 프로토콜은 그림 5와 같다.

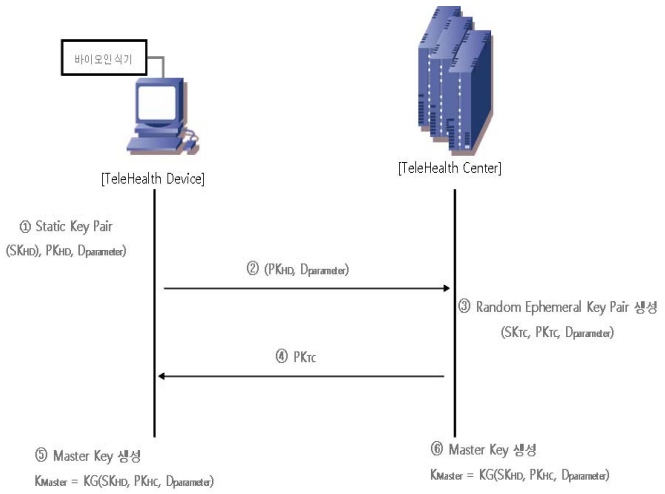

그림 5. 암호 키 관리 프로토콜
Fig. 5. Key exchange protocol for encryption

① TeleHealth 단말기는 공개키 쌍을 생성하여 개인키, 공개키, 키쌍 생성 인자를 구성한다. 각 TeleHealth 단말기는 (SK_{TD}, PK_{TD}, $D_{parameter}$)를 생성하고 개인키는 시스템에 안전하게 저장한다.
② 생성된 공개키와 키 생성 인자 (PK_{TD}, $D_{parameter}$)를 TeleHealth 센터에 전달한다.
③ TeleHealth 센터는 TeleHealth 단말기에서 송신한 (PK_{TD}, $D_{parameter}$)를 기반으로 공개 키는 저장하고 키 생성 인자를 이용해서 공개키 쌍을 생성한다. TeleHealth 센터는 개인 키, 공개키, 키쌍 생성 인자인 (SK_{TD}, PK_{TD}, $D_{parameter}$)를 생성한다. 개인키는

TeleHealth 센터에 안전하게 저장 관리한다.

④ TeleHealth 센터에서 생성된 공개키를 (PK_{TD})를 TeleHealth 단말기에 전송한다.

⑤ TeleHealth 단말기는 송수신 키 정보를 기반으로 Mater Key를 생성한다.

⑥ TeleHealth 센터는 송수신 키 정보를 기반으로 Mater Key를 생성한다.

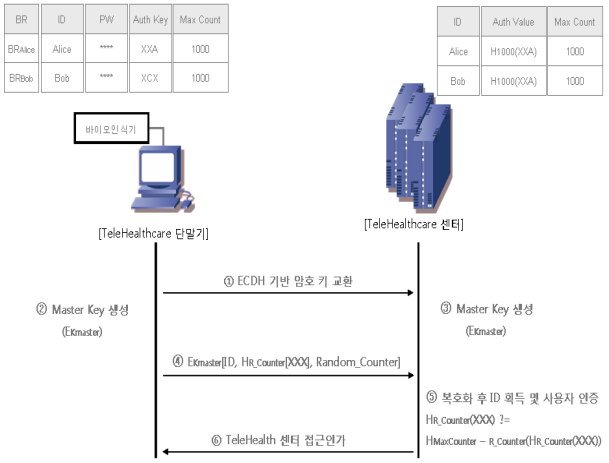

그림 6. 사용자 및 TeleHealth 단말기 인증 프로토콜
Fig. 6. Authentication protocol for user and terminal

한편, 사용자 및 TeleHealth 단말기간의 인증 프로토콜은 그림 6과 같이 정리되며, 다음과 같이 기술할 수 있다.

① TeleHealth 단말기와 TeleHealth 센터의 인증 정보는 ECDH 암호 키 교환 프로토콜을 통해서 공유된 암호키로 안전하게 송수신되어진다.

② ECDH 암호 키 교환 프로토콜을 통해 TeleHealth 단말기는 Master Key를 생성한다.

③ ECDH 암호 키 교환 프로토콜을 통해 TeleHealth 센터는 Master Key를 생성한다.

④ TeleHealth 단말기는 TeleHealth 센터 접속 시 바이오인증을 완료한 사용자의 식별정보와 해당 TeleHealth 단말기의 Auth Key를 기반으로 Max_Counter 보다 작은 Random 값을 인자로 해서 Authentication Value를 생성한 $E_{Kmaster}[ID, H_{R\_Counter}[XXX], Random\_Counter]$)을 전송한다.

⑤ TeleHealth 센터는 수신한 $E_{Kmaster}[ID, H_{R\_Counter}[XXX], Random\_Counter]$ 정보를 $E_{Kmaster}$를 이용하여 복호화 한 후 해당 ID를 획득한다. User Profile에 저장된 인증값인 Auth Value $AV_{koops} = H_{1000}[XXX]$를 수신한 $H_{R\_Counter}[XXX]$ 값과 One Way Function을 통해 일치 여부를 검증 처리($H_{R\_Counter}(XXX)?=H_{MaxCounter-R\_Counter}(H_{R\_Counter}(XXX))$)한다.

⑥ TeleHealth 단말기의 인증이 완료되면 TeleHealth 센서에 접근인가를 제공한다.

본 논문에서 제안하는 사용자 인증 및 TeleHealth 인증 프로토콜의 핵심은 TeleHealth 단말기에 대한 사용자의 바이오인식을 통한 1단계와 TeleHealth 단말기와 TeleHealth 센터를 인증하는 2단계 인증 절차로써 의료환경을 고려하여 사용자의 본인확인을 강화하고 인증방식을 경량화하여 실시간 제공이 가능하도록 제안한다. 안전 및 신뢰성이 보장되지 않는 네트워크 상에서의 식별 및 인증 정보를 매번 생성하여 일회용으로 사용함으로 안전성을 확보하고 시스템이나 네트워크 자원 제약으로 인한 효율적인 알고리즘 및 프로토콜로 구성된다.

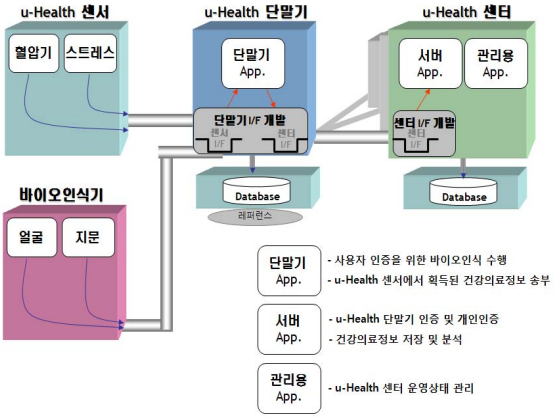

그림 7. 바이오인식기만 원격의료 프레임워크의 주요 구성요소
Fig.7. Components for TeleHealth based on the biometrics

그림 7에 표시된 바와 같은 바이오인식을 이용한 원격의료 시스템의 주요 구성요소의 기능 요구사항은 다음과 같다.

- TeleHealth 단말기 : TeleHealth 단말기는 홈네트워크와 연결되어 사용자 인증으로 ID/PW 또는 바이오인증 방식을 제공한다. 또한 TeleHealth 센서로부터 획득된 건강의료정보를 획득하고 TeleHealth 센터로 전송을 해야 한다.
- 바이오인식기 : TeleHealth 단말기가 바이오인식을 제공하는 경우, 얼굴인식 또는 지문인식을 제공하여 사용자의 편의성과 개인식별의 강화할 수 있다. 바이오인식은 사용자에게 ID/PW를 이용한 인증보다 속도가 빠르고 보안강도가 높기 때문에 TeleHealth에 적합한 인증방식을 제공한다.
- TeleHealth 저장소 : TeleHealth 단말기에서 관리되며 단말기 식별정보, 사용자 식별정도, 바이오인식용 레퍼런스를 저장한다. 단말기 식별정보로는 단말기용 기기인증서 또는 기기인증정보인 MAC, 제품일련번호 등을 사용한다. 사용자 식별정보는 ID/PW를 사용한다. 바이오인식용 레퍼런스는 얼굴 또는 지문의 레퍼런스를 저장하여 사용자 인증에 이용된다.
- TeleHealth 센서 : TeleHealth 센서틉 유무선으로 통신하며 TeleHealth 단말기에 사용자의 체중, 혈압, 혈당, 지방치, 체온, 운동량 등의 건강의료정보를 측정한다.
- TeleHealth 센터 : TeleHealth 단말기와 사용자 인증을 수행하고 송부된 건강의료정보를 저장한 후 기존의 정보와 함께 분석을 수행하여 종합적 건강상태를 확인한 후 처방 및 조치를 수행한다. 만약 사용자에게 이상증후가 발생하며 사용자와 연락을 수행하거나 응급처리 프로세스를 수행한다.

- TeleHealth 의료정보 저장소 : TeleHealth 센터내에 사용자의 건강의료정보를 이력별로 저장하여 관리함으로써 사용자의 종합건강정보를 분석하도록 제공한다.
- TeleHealth 개인정보 저장소 : TeleHealth 센터내에 저장되며 TeleHealth 단말기와 개인인증을 수행하기 위한 식별정보를 저장한다. TeleHealth 센터 내에서는 사용자의 바이오인식용 레퍼런스를 저장하지 않음으로써 개인정보 보호를 제공하기 위하여 레퍼런스는 TeleHealth 단말기에만 저장하도록 한다.

5. 결 론

원격의료에 있어서도 사용자 인증은 환자, 의사, 연구원 등 사용자의 정보 및 사생활 침해를 막고 정확한 의료정보의 전달을 위하여 바이오인증을 사용하는 사례가 많아져 주목받고 있다. 그러나, 바이오정보가 분실되거나 다른 사람에 의해서 도용되었을 경우에 비밀번호나 ID처럼 사용자가 원하는 경우에 쉽게 변경하기가 어렵다는 치명적인 단점을 지니고 있다. 이와 더불어 바이오인식 데이터를 취득하기 위해서는 개인의 신체적 프라이버시를 침해할 수 있는 소지가 많을 수 있다.

이에 본 논문에서는 바이오인식기반 원격의료시스템에 있어서 바이오정보를 포함한 개인 프라이버시 정보를 보호하기 위한 프레임워크를 제시한다. 바이오인식기반 원격의료 시스템이 만족해야할 특화된 보안 요구사항 대한 정의를 내리고, 바이오인식기반 원격의료 시스템의 모델을 정의하고, 프라이버시 정보와 바이오정보가 공격당할 수 있는 보안 위협과 이에 대처할 수 있는 대응방안을 제시하였다. 본 논문에서는 이를 위하여 다양한 보안 위협 요인들에 대처하기 위하여 2단계인증 프로토콜을 제시하고 마지막으로 바이오 인식기반 원격의료 프레임워크를 적용한 시스템의 구성요소에 대한 기능 요구사항을 기술하였다..

본 논문에서 제시한 바이오인식기반 원격의료 보안 대책에 기반 시스템 구축 시 사용자의 개인정보를 보호함과 동시에 높은 보안능력을 갖는 고성능의 개인인증용 바이오인식 시스템을 구축할 수 있다.

참 고 문 헌

[1] 전명근, *생체인식(Biometrics) 총론*, 한국정보통신교육원, 2004.

[2] S.Y. Kung, M.W.Mak, S.H. Lin, *Biometric Authentication*, Prentice Hall, 2005.

[3] Arun A. Ross, K. Nandakumar, Anil K. Jain, *Handbook of Multibiometrics*, Springer, 2006.

[4] IDC, "IDC Expects Healthy Worldwide Investmentsin IT with Highest U.S. Growth Rates in Healthcare and Communications and Media," 2006.

[5] MobiHealth 프로젝트, http://www.mobihealth.org

[6] GE 헬스케어, http://www.gehealthcare.com

[7] HIPAA, "Summary of the HIPAA Privacy Rule," http://www.hhs.gov/ocr/hipaa/privrulepd.pdf

[8] 박건희, "보건의료정보화와 개인정보보호," 서울대의대 2006년 상반기 토픽 리뷰, 2006. 6.

[9] ISO/IEC JTC1 SC37 N2486, Standing Document 2, Harmonized Biometric Vocaburuary, 2008

[10] FIDIS(Future of Identity in the Information Society), D3.10: Biometrics in identity management, 2007."

[11] ITU-T Recommendation X.tsm-part1: Telebiometric system mechanism -General biometric authentication protocol and system model profile for telecommunication systems, ITU-T SG17 Q.9, 2009.

[12] ITU-T Recommendation X.tif: TeleHelath Integrated framework, ITU-T SG17 Q.9, 2009.

[13] 신용녀, 전명근, "개인정보 보호를 위한 바이오인식 템플릿 보안", *한국지능시스템학회논문지*, Vol.18, No.4, pp 437~444, 2008.

[14] 전명근, 문기영, "생체정보 이용과 프라이버시 보호", *정보보호학회지*, 제 15권 6호, pp.11~18, 2005.

[15] 신용녀, 전명근, 개인 식별 정보와 바이오인식정보의 보호기법, *한국지능시스템학회논문지*, Vol.19, No.2, pp 160-167, 2009

[16] ISO/IEC JTC1 SC27, Information technology-security techniques - A privacy reference architecture, 2007

저 자 소 개

신용녀(Yong-Nyuo Shin)
2009년 제19권 2호 참조

전명근(Myung Geun Chun)
2010년 제20권 3호 참조