The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 5, pp.117-123, Oct. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2016.16.5.117
JIIBC 2016-5-18

응급 상황 처리를 위한 안전한 개인건강기록 시스템

A Secure Personal Health Record System for Handling of Emergency Situations

이명규*, 황희정**

Myung-Kyu Yi*, Hee-Joung Hwang**

요 약 최근 개인건강기록(PHR)은 환자중심의 건강정보교환 모델로 각광받고 있다. PHR 소유자는 언제 어디서나 쉽게 자신의 기록을 저장하고 회수할 수 있는 접근 권한을 누릴 수 있다. 하지만, PHR의 민감성과 신뢰성 특성 때문에 PHR은 개인이 접근할 수 있는 권한을 결정할 수 있도록 안전하게 유지되어야 한다. 본 논문에서는 응급상황에서 사용자의 PHR에 접근할 수 있는 시스템을 제안하였다. 환자가 의식이 없는 응급상황에서 응급센터요원은 PHR에 대해 미리 정의된 권한에 의하여 PHR 서버에 응급접근을 요청한 응급 정보를 사용할 수 있다. 제안된 시스템에서 PHR 사용자는 응급상황에서 좀 더 정교한 접근제어를 명세화 할 수 있다.

Abstract In recent years, Personal Health Record (PHR) has emerged as a patient-centric model of health information exchange. The Personal Health Record (PHR) owners enjoy the full right of accessing their records anywhere and anytime making storage and retrieval more efficient. Due to the sensitivity and confidential nature of the PHR, however, the PHR is maintained in a secure and private environment with the individual determining rights of access. In this paper, we propose a system which enables access to the user's PHR in the event of emergency. In emergency situation where the user is unconscious, the emergency staff can use the PHR information to request a emergency access to the PHR server based on the predefined rights of access for PHR. Under the proposed system, the PHR owner can specify a fine grain access control policy during emergency situations.

Key Words : PHR, personal health record, security, privacy, healthcare

Ⅰ. 서 론

최근 스마트폰의 급속한 발전과 함께 스마트밴드와 같은 웨어러블 디바이스가 대중화됨에 따라 생체 및 건강정보를 측정하고 분석하여 건강 상태를 관리하는 개인건강기록 서비스가 등장하고 있다[1-5]. 심박수를 측정하는 반지, 수면패턴을 분석하는 손목시계 등 다양한 웨어러블 디바이스가 대중화됨으로써 모바일 기기와 건강관리를 접목시켜 개발된 헬스케어기기들이 쏟아지고 있으며, 개인 스스로가 직접 운동량, 심박수, 수면시간, 섭취한 음식의 칼로리 등과 같은 자신의 건강에 관한 정보를 수집 및 관리할 수 있게 되었다. 또한, 수집된 개인건강정보를 바탕으로 제공되는 다양한 운동 및 식이요법과 같은 개인 맞춤형 건강관리 서비스 제공이 가능할 것으로 전망된다. 이와 같은 헬스케어 관련 기술 발전의 속도로 미루어 볼 때 개인의 건강관리는 물론 전문 의료기록

*정회원, 가천대학교 IT대학 컴퓨터공학과
**정회원, 가천대학교 IT대학 컴퓨터공학과(교신저자)
접수일자 : 2016년 8월 30일, 수정완료 : 2016년 9월 30일
게재확정일자 : 2016년 10월 7일

Received: 30 August, 2016 / Revised: 30 September, 2016 / Accepted: 7 October, 2016
**Corresponding Author: hwanghj@gachon.ac.kr
Dept. of Computer Engineering, Gachon University, KOREA

까지 스마트폰에서 관리할 수 있는 시대가 열릴 것으로 기대되고 있다. 현재는 칩과 센서를 이용한 운동량 계측이나 자가 측정을 통한 건강관리 수준에 머물고 있으나, 병원 전자의료기록(Electronic Medical Record, 이하 EMR)과 연동한 개인건강기록(Personal Health Record, 이하 PHR)을 통해 개인의 건강검진이나 투약정보, 진료기록까지 스마트폰에 담겨 건강관리에 유용하게 활용될 것으로 보인다. PHR은 '다양한 의료기관으로 부터 제공되는 개인의 진료정보와 개인 스스로 기록한 건강기록을 통합적이고 포괄적인 관점에서 바라본 개인의 평생건강기록과 그 기록을 관리할 수 있는 도구'를 의미한다[2]. PHR은 건강에 관련된 생체신호, 진료, 치료 등의 여러 정보를 환자 개인이 관리할 수 있도록 하는 개인 건강의 기록 표준이 된다. PHR 시스템은 의료기관에 흩어져 있는 진료/검사정보와 스마트폰 등으로 수집한 데이터 등을 사용자 스스로 열람하고 관리할 수 있도록 구축한 건강기록시스템이다. PHR 시스템의 목적은 개인 의료 기록을 완전하고 정확하게 요약하여 온라인에서 사용할 수 있게 할 뿐 아니라 개인별로 최적화한 맞춤형 건강관리 서비스를 제공하는데 있다.

PHR 서비스의 경우 매우 민감한 사용자의 데이터를 관리하기 때문에 보안이 매우 중요하다. 환자, 보호자, 병원과 같은 PHR 주체와 정보 전송 및 저장과정에서 위·변조, 외부의 침입, 바이러스 감염 등 다양한 보안위협들이 존재하며 PHR 데이터를 부적절하게 이용될 경우 개인의 프라이버시 침해로 이어질 수 있다[6,7]. 또한, 환자가 의식이 없는 응급상황에서 PHR의 활용과 보안은 매우 중요하지만 관련 연구는 거의 전무한 상황이다. 응급상황에서 환자의 PHR 데이터를 안전하게 활용하고 공유하기 위해서는 반드시 기술적인 보안 및 프라이버시 보호 장치가 마련되어야 한다[8,9]. 본 논문에서는 응급상황에서 안전하게 사용하기 위한 응급 PHR 시스템을 제안하고자 한다. 본 논문의 구성은 다음과 같다. 2장은 제안된 응급 PHR 기법에 대하여 설명하고, 3장은 제안된 기법에 대한 보안성을 분석한다. 마지막으로 4장에서는 결론을 도출한다.

II. 제안된 응급 PHR 시스템

본 장에서는 제안된 응급 PHR 시스템에 대해서 설명한다.

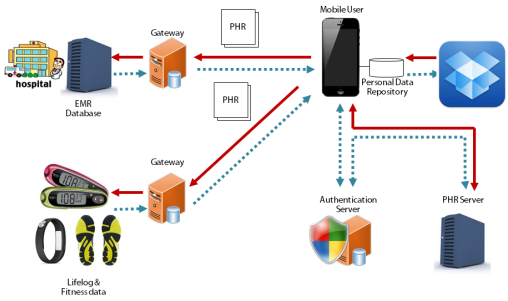

그림 1. 제안된 PHR 시스템 구성도
Fig. 1. The architecture of the proposed system

본 논문에서 제안하는 응급 PHR 시스템은 그림 1과 같이, 단말기, 인증서버, PHR 서비스를 위한 PHR 서버로 구성되어 있다. 인증서버의 공개키는 사용자, PHR서버, 인증서버에서 안전한 채널을 통하여 공유하고 있다고 가정한다. 또한, 응급상황을 위하여 환자와 응급센터 요원의 식별자(ID)와 공개키는 인증서버에 미리 등록되어 있다고 가정한다.

PHR 데이터는 반드시 개인의 건강관리를 목적과 의료진과 보호자 등의 속성을 고려하여 사용범위를 설정되어야 한다. 응급상황의 환자의 치료를 목적으로 하는 경우 개인의 사전 정의가 필요하며, 이러한 경우 개인정보는 익명화되어서 사용해야 하는 조건이 필요하다. 개인의 프라이버시 보호를 위하여 PHR 데이터를 접근하는 사람에 대한 기밀성 유지가 필요하며 PHR 서비스 내역 및 서비스 사용자에 대한 프라이버시 보호와 권한관리 유지가 필요하다. 따라서, 본 논문에서는 그림 2와 같이 3단계로 응급 PHR 등급을 나누고자 한다.

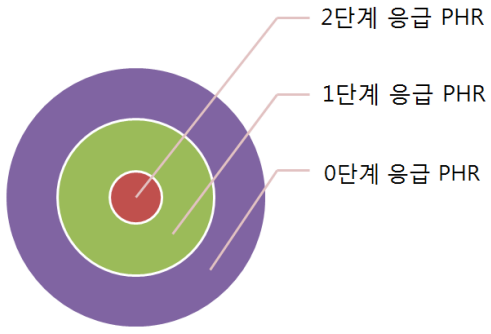

그림 2. 응급 PHR의 자료구조
Fig. 2. The data structure of emergency PHR

0단계 응급 PHR은 응급상황에서 응급센터요원이면 누구나 접근할 수 있는 PHR 정보를 의미한다. 예를 들면, 혈액형, 키, 체중, 나이, 보호자 연락처와 같은 정보가 될 수 있다. 1단계 응급 PHR은 응급상황에서 응급센터요원이라 하더라도 보호자의 동의가 필요한 PHR 정보를 의미한다. 예를 들면, 과거병력, 알러지, 복약기록, 예방접종 기록, 혈당, 혈압, 간수치 등 민감한 의료정보가 될 수 있다. 마지막으로 2단계 응급 PHR은 환자 본인이 아니라면 공개가 불가능한 민감한 의료정보를 의미한다. 본 논문에서는 0단계와 1단계 응급 PHR에 대하여 안전하게 등록하고 응급상황에서 응급 PHR를 안전하게 수신할 수 있는 기법을 제안하고자한다.

제안된 기법에서 PHR 서버에 0단계 응급 PHR를 등록하는 과정은 그림 3과 같다.

1-1) 사용자는 PHR 서버와 보안 연결을 설정하기 위하여 인증서버로부터 PHR 서버의 공개키를 획득해야 한다. 따라서, 사용자는 사용자 식별자 ID_U와 PHR 서버 식별자 ID_{PHR}를 사용자의 비밀키로 암호화하여 인증서버로 전송한다.

1-2) 인증서버는 PHR 서버의 공개키 인증서의 복사본 PU_{PHR}을 인증서버의 비밀키 PR_{auth}로 암호화 한 후 다시 사용자의 공개키 PU_U를 이용하여 이중 암호화하여 사용자에게 반송한다.

1-3) 사용자는 PHR 서버와 보안연결 설정을 위해 사용자 식별자와 응급 PHR 등록요청, 그리고 사용자의 임시비표 N_U를 1-2)에서 수신 받은 PHR 서버의 공개키로 암호화하여 전송한다.

1-4) PHR 서버는 사용자의 공개키를 획득하기 위하여 인증서버에게 사용자 식별자, PHR 서버 식별자, 그리고 사용자의 임시비표를 인증서버의 공개키로 암호화하여 전송한다.

1-5) 인증서버는 PHR 서버에게 사용자의 공개키 인증서 사본을 인증서버의 비밀키로 암호화하여 전송한다. 또한, PHR 서버와 사용자 사이에 안전한 연결을 위한 세션 키 K_s를 생성하고, 사용자 임시비표, PHR 서버 식별자, 사용자 식별자 정보를 인증서버의 비밀키로 암호화하여 PHR 서버에게 반환한다.

1-6) PHR 서버는 인증서버의 비밀키로 암호화된 사용자의 임시비표, 세션 키, 사용자 식별자, PHR 식별자를 응급 PHR 등록승인 메시지와 PHR 서버에서 생성된 비표 N_{PHR}와 함께 사용자의 공개키로 암호화하여 사용자에게 전송한다.

1-7) 사용자는 사용자의 비밀키로 암호화한 사용자 식별자, 0단계 응급 PHR와 함께 PHR 임시비표를 세션 키로 암호화하여 PHR 서버에 등록한다.

1-8) PHR 서버는 응급 PHR이 정상적으로 PHR 서버에 등록되었음을 표시하는 ACK 메시지를 사용자의 공개키와 세션 키로 암호화하여 사용자에게 반환한다.

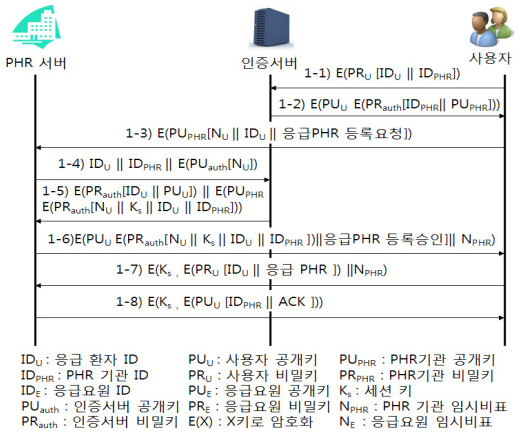

그림 3. 0단계 응급 PHR 등록절차
Fig. 3. The registration process of emergency PHR for level 0

제안된 기법에서 응급상황에서 PHR 서버를 통해 0단계 응급 PHR를 수신 받는 과정은 그림 4과 같다.

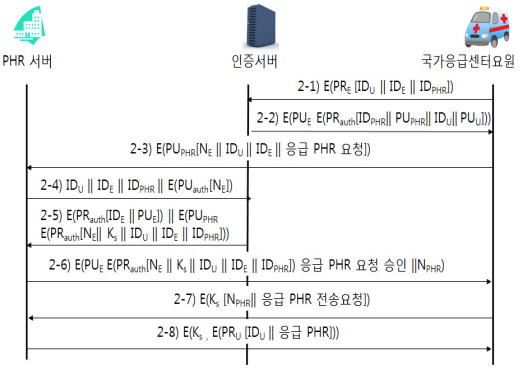

그림 4. 0단계 응급 PHR 전송절차
Fig. 4. The delivery process of emergency PHR for level 0

2-1) 응급상황이 발생한 경우, 현장에 도착한 응급센

터요원은 PHR 서버와 보안 연결을 설정하기 위하여 PHR 서버의 공개키를 획득해야 한다. 따라서, 응급센터 요원 식별자 ID_E와 사용자 식별자 ID_U를 자신이 비밀키로 암호화하여 인증서버에게 전송한다.

2-2) 인증서버는 응급센터요원 식별자를 통해 응급상황이 발생하였음을 인지하고, 사용자의 공개키 인증서 복사본과 PHR 서버의 공개키 인증서의 복사본을 인증서버의 비밀키와 응급센터요원의 공개키를 이용하여 이중으로 암호화하여 응급센터요원에게 반송한다.

2-3) 응급센터요원은 PHR 서버와 보안연결 설정을 위하여 응급센터요원 식별자, 사용자 식별자, 응급 PHR 요청, 그리고 응급센터요원의 임시비표 N_E를 2-2)에서 수신 받은 PHR 서버의 공개키를 이용해서 암호화하여 전송한다.

2-4) PHR 서버는 응급센터요원의 공개키를 획득하기 위하여 인증서버에게 응급센터요원 식별자, 사용자 식별자, PHR 서버 식별자, 그리고 응급센터요원의 임시비표를 인증서버의 공개키로 암호화하며 전송한다.

2-5) 인증서버는 PHR 서버에게 응급센터요원의 공개키 인증서 사본을 인증서버의 비밀키로 암호화하여 전송한다. 또한, PHR 서버와 응급센터요원 사이에 안전한 연결을 위한 세션 키 K_s를 생성하고, 사용자 임시비표, PHR 서버의 식별자, 응급센터요원의 식별자, 사용자 식별자 정보를 인증서버의 비밀키로 암호화하여 반환한다.

2-6) 인증서버의 비밀키로 암호화된 응급센터요원의 임시비표, 세션 키, 응급센터요원의 식별자, 사용자의 식별자, PHR 식별자는 응급 PHR 요청 승인 메시지와 PHR 서버에서 생성된 비표 N_{PHR}와 함께 응급센터요원의 공개키를 이용해서 암호화하여 사용자에게 전송된다.

2-7) 응급센터요원은 PHR 서버에서 수신한 임시비표와 응급 PHR 전송요청 메시지를 세션 키로 암호화하여 PHR 서버에 보낸다.

2-8) PHR 서버는 사용자의 비밀키로 암호화된 0단계 응급 PHR을 세션 키로 암호화하여 응급센터요원에게 반환한다.

세션키와 사용자의 비밀키로 암호화 되어있는 0 단계 응급 PHR은 2-2)에서 수신한 사용자의 공개키와 2-6)에서 수신한 세션키를 이용하여 복호화한 후 응급상황에 있는 환자를 위해 사용된다.

제안된 기법에서 PHR 서버에 1단계 응급 PHR를 등록하는 과정은 그림 5과 같다.

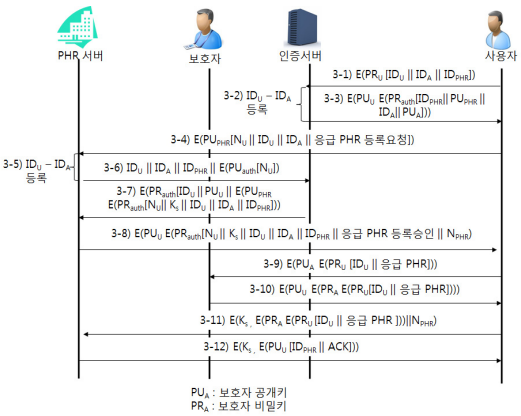

그림 5. 1단계 응급 PHR 등록절차
Fig. 5. The registration process of emergency PHR for level 1

3-1) 사용자는 PHR 서버와 보안 연결을 설정하기 위하여 인증서버로부터 PHR 서버의 공개키를 획득해야 한다. 따라서, 사용자는 사용자 식별자 ID_U, 보호자 식별자 ID_A, 그리고 PHR 서버 식별자 ID_{PHR}를 사용자의 비밀키로 암호화하여 인증서버로 전송한다.

3-2) 인증서버는 3-1)에서 수신한 메시지를 통하여 응급상황에서 사용자 ID_U를 대신하여 응급 PHR에 접근할 수 있는 보호자가 ID_A임을 인식하고 ID_U-ID_A의 값을 저장한다.

3-3) 인증서버는 PHR 서버의 공개키 인증서의 복사본 PU_{PHR}과 보호자의 공개키 인증서의 복사본 PU_A를 인증서버의 비밀키 PR_{auth}와 사용자의 공개키 PU_U를 이용하여 이중으로 암호화하여 사용자에게 반송한다.

3-4) 사용자는 PHR 서버와 보안연결 설정을 위하여 사용자 식별자, 보호자 식별자, 응급 PHR 등록요청, 그리고 사용자의 임시비표 N_U를 3-2)에서 수신 받은 PHR 서버의 공개키로 암호화하여 전송한다.

3-5) PHR 서버는 응급상황에서 사용자 ID_U를 대신하여 응급 PHR에 접근할 수 있는 보호자가 ID_A임을 인식하고 ID_U-ID_A의 값을 저장한다.

3-6) 인증서버는 사용자의 공개키를 획득하기 위하여, 사용자 식별자, 보호자 식별자, 그리고, 3-4)에서 수신한 사용자의 임시비표를 인증서버의 공개키로 암호화하여 인증서버에 전송한다.

3-7) 인증서버는 PHR 서버에게 사용자의 공개키 인증서 사본을 인증서버의 비밀키로 암호화하여 전송한다. 또한, PHR 서버와 사용자 사이에 보안 연결 설정을 위한

세션 키 K_S를 생성하고, 사용자 임시비표 , PHR 서버 식별자, 사용자 식별자, 보호자 식별자 정보를 인증서버의 비밀키로 암호화하여 반환한다.

3-8) 인증서버의 비밀키로 암호화된 사용자의 임시비표, 세션 키, 사용자 식별자, 보호자 식별자, PHR 식별자는 응급 PHR 등록승인 메시지와 PHR 서버에서 생성된 비표 N_{PHR}와 함께 사용자의 공개키를 이용해서 암호화하여 사용자에게 전송된다.

3-9) 사용자는 사용자의 비밀키로 암호화한 사용자 식별자와 1단계 응급 PHR를 보호자의 공개키로 암호화하여 보호자에게 전송한다.

3-10) 보호자는 수신된 3-9)에서 수신된 메시지(즉, 사용자의 비밀키로 암호화한 사용자 식별자와 1단계 응급 PHR)를 보호자의 비밀키로 이중 암호화한 후에 사용자의 공개키로 암호화하며 사용자에게 반환한다.

3-11) 사용자는 3-10)에서 수신된 메시지(즉, 사용자의 비밀키로 암호화한 사용자 식별자와 1단계 응급 PHR를 보호자의 비밀키로 이중 암호화한 메시지)와 3-8)에서 수신한 PHR 임시비표를 세션 키로 암호화하여 PHR 서버에 등록한다.

3-12) PHR 서버는 응급 PHR이 정상적으로 PHR 서버에 등록되었음을 표시하는 ACK 메시지를 사용자의 공개키와 세션 키로 암호화하여 사용자에게 반환한다.

제안된 기법에서 응급상황에서 PHR 서버를 통해 1단계 응급 PHR를 수신 받는 과정은 그림 6과 같다.

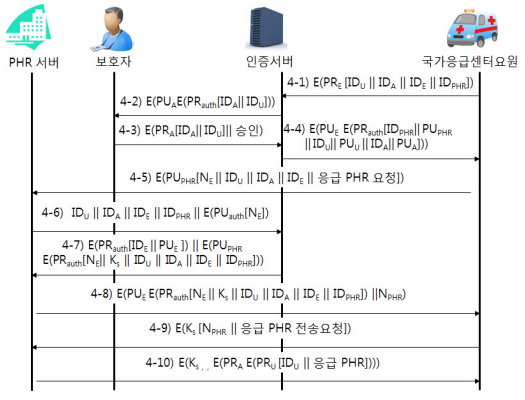

그림 6. 1단계 응급 PHR 전송절차
Fig. 6. The delivery process of emergency PHR for level 1

4-1) 응급상황이 발생한 경우, 현장에 도착한 응급센터요원은 PHR 서버와 보안 연결을 설정하기 위하여 PHR 서버의 공개키를 획득해야 한다. 따라서, 응급센터요원 식별자 ID_E, 사용자 식별자, 보호자 식별자, PHR 서버 식별자를 자신이 비밀키로 암호화하여 인증서버에게 전송한다.

4-2) 인증서버는 응급센터요원 식별자를 통해 응급상황이 발생하였음을 인지하고, 미리 저장된 사용자 식별자-보호자 식별자 값을 통해 보호자의 승인이 필요함을 인지하게 된다. 따라서, 사용자 식별자와 보호자 식별자를 인증서버의 비밀키로 암호화하고 보호자의 공개키로 이중 암호화하여 보호자의 승인을 요청한다.

4-3) 보호자는 수신된 메시지를 통해 사용자의 응급상황이 발생하였음을 인지하게 되고 승인메시지를 보호자의 비밀키로 암호화하여 인증서버에게 전송한다.

4-4) 인증서버는 보호자의 승인을 획득한 후에, PHR 서버의 공개키 인증서의 복사본, 보호자의 공개키, 사용자의 공개키를 인증서버의 비밀키와 응급센터요원의 공개키를 이용하여 이중으로 암호화하여 응급센터요원에게 반송한다.

4-5) 응급센터요원은 PHR 서버와 보안연결 설정을 위하여 응급센터요원 식별자, 사용자 식별자, 보호자 식별자, PHR 서버 식별자, 응급 PHR 요청, 그리고 응급센터요원의 임시비표 N_E를 4-4)에서 수신 받은 PHR 서버의 공개키를 이용해서 암호화하여 전송한다.

4-6) PHR 서버는 응급센터요원의 공개키를 획득하기 위하여 인증서버에게 응급센터요원 식별자, 사용자 식별자, 보호자 식별자, PHR 서버 식별자, 그리고 응급센터요원의 임시비표를 인증서버의 공개키로 암호화하며 전송한다.

4-7) 인증서버는 PHR 서버에게 응급센터요원의 공개키 인증서 사본을 인증서버의 비밀키로 암호화하여 전송한다. 또한, PHR서버와 응급센터요원 사이에 보안연결 설정을 위한 세션 키 K_S를 생성하고, 사용자 임시비표, PHR 서버 식별자, 응급센터요원 식별자, 사용자 식별자 정보를 인증서버의 비밀키로 암호화하여 반환한다.

4-8) 인증서버의 비밀키로 암호화된 응급센터요원의 임시비표, 세션 키, 응급센터요원 식별자, 사용자 식별자, PHR 식별자를 응급 PHR 요청 승인 메시지와 PHR 서버에서 생성된 비표 N_{PHR}와 함께 응급센터요원의 공개키를 이용해서 암호화하여 사용자에게 전송된다.

4-9) 응급센터요원은 PHR 서버에서 생성된 임시비표와 함께 응급 PHR 전송요청 메시지를 세션 키로 암호화하여 PHR 서버에 보낸다.

4-10) PHR 서버는 사용자의 비밀키와 보호자의 비밀키로 암호화된 응급 PHR을 세션 키로 암호화하여 응급센터요원에게 반환한다.

응급센터요원은 4-4)에서 수신한 보호자의 공개키, 사용자의 공개키, 그리고 4-8)에서 수신한 세션키를 이용하여 응급 PHR을 복호화하여 응급상황에 있는 사용자를 치료하는데 활용한다.

III. 제안방식 분석

본 장에서는 제안한 응급 PHR 등록 및 전송기법의 안정성을 패스워드 추측공격, 전방향 안전성(Forward secrecy), 위장공격(Impersonation attack), 중간자 공격(Man-in-the-middle attack)측면에서 분석하고자 한다. 패스워드 추측공격은 사용자와 서버간의 통신 내용을 도청한 후, 이를 특정 보안 알고리즘에 대입하여 사용자의 패스워드를 획득하는 방법이다. 하지만, 사용자, 보호자, PHR 서버 모두 공개키 정보만 획득할 수 있고, 공개키로부터 비밀키를 획득하는 것은 이산대수의 어려움에 근거한다. 따라서, 본 논문에서 제안한 인증 기법은 패스워드 추측 공격에 안전하다. 전방향 안전성은 공격자가 오랜 기간동안 사용하는 비밀키를 알고 있을 때 이전 세션키를 회득할 수 있는지 여부를 통해 결정한다. 본 논문에서 제안한 기법에서 세션키는 세션이 유지되는 기간만 유효하고 세션이 종료된 이후에는 새로운 보안연결을 통해 세션키가 생성되므로 전방향 안정성을 제공한다. 위장공격을 분석하기 위해서는 사용자 위장공격과 PHR 서버 위장 공격 관점을 제시한다. 사용자 위장공격의 경우, PHR 공개키를 획득하기 위한 사용자 식별자 전송은 인증서버의 공개키로 암호화되어 인증서버가 소유한 비밀키 외에는 복호화 할 수 없으므로 기밀성을 보장한다. 또한, 인증서버에 의해 복사된 PHR의 공개키는 인증서버의 개인키로 암호화됨으로 인증서버에 의해 생성되었음을 보장하므로 기밀성을 보장한다. 마지막으로, PHR서버에서 인증서버에 전송되는 사용자 임시비표도 인증서버의 공개키로 암호화됨으로써 기밀성을 보장한다. 따라서, 제안한 기법은 사용자 위장 공격에 안전하다고 말할 수 있다. PHR 서버 위장공격의 경우, 사용자 공개키를 획득하기 위한 PHR 서버 식별자 전송은 인증서버의 공개키로 암호화되어 인증서버가 소유한 비밀키 외에는 복호화 할 수 없으므로 기밀성을 보장한다. 또한, 인증서버에 의해 복사된 사용자의 공개키는 인증서버의 개인키로 암호화됨으로 인증서버에 의해 생성되었음을 보장하므로 기밀성을 보장한다. 마지막으로, PHR서버에서 사용자에게 전송되는 PHR 서버의 임시비표도 PHR서버의 비밀키로 암호화됨으로써 기밀성을 보장한다. 따라서, 제안한 기법은 PHR 서버 위장 공격에 안전하다고 말할 수 있다. 마지막으로, 중간자 공격을 분석해보면 사용자에서 발행한 임시비표와 세션키, PHR 서버에서 발행한 임시비표와 세션키의 결합은 세션 키가 투명하다는 것을 보장한다. 또한, 세션 키와 임시비표는 공개키로 암호화되어 이산대수의 어려움에 근거하므로 중간자 공격에 안전하다고 말할 수 있다.

IV. 결 론

PHR 서비스는 환자의 병원기록뿐 아니라 밴드나 스마트워치와 같은 웨어러블 장치로부터 얻은 개인 정보를 기록을 바탕으로 건강상태를 분석하고 개인 맞춤형 건강정보를 제공해주는 서비스를 의미한다. PHR 서비스의 활성화를 위해서 보안이 필수적인 요소가 되고 있며, 환자의 의식이 없는 응급상황에서 보안은 더욱 중요한 문제가 되고 있다. 본 논문에서는 응급 상황 처리를 위한 안전한 개인건강 기록 시스템을 제안하였다. 제안한 PHR 시스템을 통해 환자의 민감한 건강기록정보를 단계별로 구분하였고 응급상황에서 환자에게 활용되기 위하여 단계별 응급 PHR 기록의 등록 및 전송방법을 제안하였다. 제안한 기법은 패스워드 추측, 전방향 안전성, 위장공격, 중간자공격에 안전하다. 제안된 기법은 향후 응급의료현장에 유용하게 활용될 것 기대된다.

References

[1] https://www.patientslikeme.com
[2] https://www.microsoft.com/microsoft-health
[3] http://www.microsoft.com/microsoft-band/

[4] https://www.healthvault.com/
[5] Chimezie Ogbuji, Karthik Gomadam, and Charles Petrie, "Web Technology and Architecture for Personal Health Records", IEEE Internet Computing, Vol. 15, No 4, pp. 10-13, July, 2011.
[6] Myung-Kyu Yi, Hee-Joung Hwang, "A Study on Security Weakness and Threats in Personal Health Record Services", The Journal of The Institute of Internet, Broadcasting and Communication, Vol.15, No. 6, pp.163-171, Dec. 31, 2015.
[7] Personal Health Records and the HIPAA Privacy Rule.
[8] Myung-Kyu Yi, Hee-Joung Hwang, "Design of Secure Personal Health Record Management Systems", Journal of Korean Institute Of Information Technology, Vol. 13(8), pp. 71-80, 2015.8
[9] Myung-Kyu Yi, Done-sik Yoo, Taeg-Keun Whangbo, "A Security Labeling Scheme for Privacy Protection in Personal Health Record System", The Journal of The Institute of Internet, Broadcasting and Communication, Vol.15, No. 6, pp.173-180, Dec. 31, 2015.

저자 소개

이 명 규(정회원)

- 2005년 2월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 10월 ~ 현재 : 가천대학교 IT 대학 컴퓨터공학과 연구교수
- TTA 유헬스 프로젝트그룹 개인건강정보 표준화 전담반 위원

<주관심분야 : u-Health, Big Data, Medical Informatics, Security, Ubiquious Computing>

황 희 정 (정회원)

- 2000년 9월 : 인하대학교 컴퓨터공학과 (공학석사)
- 2008년 2월 : 인천대학교 컴퓨터공학과 (공학박사)
- 2000년 10월 ~ 현재 : 가천대학교 IT 대학 컴퓨터공학과

<주관심분야 : Software Engineering, u-Health, Big Data, Medical Informatics, Ubiquious Computing>

※ 이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.B0101-16-0247, 개인 건강정보 기반 개방형 ICT 힐링 플랫폼 기술 개발)