The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 4, pp.109-115, Aug. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2016.16.4.109
JIIBC 2016-4-16

개인 건강 라이프로그 서비스에서 보안 참조 모델에 관한 연구

A Study on Security Reference Model in Personal Health Lifelog Services

이명규*, 황희정**

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

요 약 라이프로그는 개인차원에서 일상생활을 오랫동안 기억하거나 공유하기위한 단순한 기록목적으로 시작되었지만 최근 다양한 기업들이 각각의 전문성을 활용한 분석방법을 도입함으로써 개인의 삶의 질이 향상되는 새로운 라이프로그 비즈니스가 형성되고 있다. 이러한 중요한 장점에도 불구하고 개인 건강 라이프로그 서비스는 데이터의 보안에 관련된 사용자 입장에서는 피할 수 없는 중요한 도전을 제기하고 있다. 개인 건강 라이프로그 서비스가 활성화되면서 사용자 개인정보 침해가 발생하고 사용자의 민감한 의료정보가 유출되는 문제가 증가되고 있다. 본 논문에서는 개인 건강 라이프로그 서비스를 위한 보안 참조모델을 제시하고자 한다. 제안된 보안 참조모델은 건강 라이프로그 서비스 제공을 위한 개인 정보 보호 방안에 명확한 지침을 제시하여 관련 분야의 산업 활성화 및 신 시장 개척을 이끌어 낼 수 있을 것으로 예상된다.

Abstract Life log started with the simple purpose of recording or sharing mainly data regarding one's personal life, but with the introduction of advanced specialized analytic methods by many corporations, a new type of business based on the life log recently emerged, with an aim of improving the quality of people's personal lives. In spite of the indispensable advantages, however, personal health lifelog service brings critical challenges that cannot be avoided from user side if the security of the data is concerned. The problem of user's privacy infringement and leaking user's sensitive medical information is increasing with the revitalization of personal health lifelog services. In this paper, we propose an information security reference model for the personal health lifelog services. Our proposal can contribute to increase the related industry to cultivate new market by suggesting the clear announcement of the guidelines using privacy protection reference model for user-specific healthcare services which uses personal lifelog

Key Words : lifelog, lifelogging, personal health lifelog, healthcare, wearable computer

Ⅰ. 서 론

최근 스마트폰 카메라, 웹캠, 웨어러블 디바이스, 비디오와 스트리밍 데이터와 같은 방대한 디지털 정보를 처리할 수 있는 데이터 저장장치, 클라우드, 기가비트 속도의 네트워크의 발전으로 사용자는 언제 어디서나 생활을

*정회원, 가천대학교 IT대학 컴퓨터공학과
**정회원, 가천대학교 IT대학 컴퓨터공학과(교신저자)
접수일자 : 2016년 6월 15일, 수정완료 : 2016년 7월 15일
게재확정일자 : 2016년 8월 5일

Received: 15 June, 2016 / Revised: 15 July, 2016 /
Accepted: 5 August, 2016
**Corresponding Author: hwanghj@gachon.ac.kr
Dept. of Computer Engineering, Gachon University, Korea

편리하게 기록할 수 있게 되었다. 삶을 의미하는 '라이프(Life)'와 접속을 의미하는 '로그(Log)'의 합성어인 '라이프로그(Lifelog)'는 '인생이나 일상의 기록'이라는 의미로 개인이 일상생활에서 경험하는 모든 정보를 기록하고, 수집된 기록을 사용하기 편리하도록 분류 및 가공한 후 필요한 경우 활용할 수 있도록 하는 기술이다. 라이프로그는 단지 개인의 삶에 대한 기록 뿐 아니라 수집된 기록의 분석을 통해 일정한 패턴을 발견하고 다양한 방법으로 활용하는 일련의 과정을 포함한다. 수집된 기록의 분석을 통해 어떤 옷을 자주 입는지, 어떤 음식을 좋아하는지 어렵지 않게 알 수 있으며, 기업은 이를 마케팅에 활용해 맞춤형 제품을 추천하고 개인에게 어울리는 특정한 광고를 내보임으로써 효과적으로 수익을 얻을 수 있다. 이러한 배경을 바탕으로 최근 라이프로그를 활용한 다양한 서비스가 등장하고 있다. 라이프로그 서비스를 통하여 사용자는 직접 메모나 사진으로 기록을 저장할 뿐 아니라 스마트폰에 저장된 위치정보와 사진, 운동량 등을 종합해 체계적 기록을 자동적으로 볼 수 있고, 운동과 건강 정보 등과 결합한 맞춤형 서비스로 새로운 가치를 만들 수 있다. 또한, 쇼핑몰 사이트 등에서 흔히 볼 수 있는 개인화 추천 서비스도 가능하다. 개인화 추천 서비스는 소비자의 행동이나 소비 패턴을 분석하여 현재 관심 분야와 앞으로의 관심분야를 파악하고, 분석한 결과를 바탕으로 일반화된 대중이 아닌 개인에게 특화된 정보와 상품을 추천해주는 서비스를 말한다. 대표적인 사례로 미국 최대 온라인 스트리밍 서비스 기업인 넷플릭스의 경우 영화, 드라마와 같은 '콘텐츠에 대한 개인화 추천' 서비스를 제공하고 있으며, 콘텐츠 장르를 76,800개 이상으로 세밀하게 분류하고 분류된 결과를 개인화 추천에 활용해서 80% 이상의 놀라운 추천 적중률을 자랑하고 있다. 하지만, 건강관련 라이프로그는 개인의 프라이버시와 관련된 민감한 정보를 포함하고 있어서 보안이 필수적이다. 본 논문은 개인 건강 라이프로그 서비스를 제공함에 있어서 발생할 수 있는 보안 위협요소을 분석하고, 이를 토대로 보안 참조 모델을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장은 건강 라이프로그 관련 연구를 설명하고, 3장은 건강 라이프로그 보안 참조모델을 위한 보안 위협요소에 대해서 기술한다. 4장은 분석된 결과를 토대로 건강 라이프로그 보안 참조모델을 제안하고, 마지막으로 5장은 제안된 건강 라이프로그 서비스 보안 참조모델에 대한 결론을 도출한다.

II. 관련 연구

최근 국외 및 국내에서는 건강 라이프로그 정보를 기록하고, 기록된 라이프로그 정보를 의료나 운동에 활용하는 건강 라이프로그 서비스가 주목을 받고 있으며 건강 라이프로그를 활용한 연구들은 다음과 같다.

그림 1. 개인 건강 라이프로그 서비스 사례
Fig. 1. An Example of personal health lifelog service

나이키는 애플의 아이팟과 연동하여 개인의 걸음걸이, 운동량, 거리 등의 운동량에 관한 정보를 지속적으로 수집저장 할 수 있는 '나이키플러스' 운동화를 개발하여 시판 중이다[1]. 사용자가 운동화를 신고 달리는 동안 사용자의 운동 데이터는 아이팟으로 전송이 되며, 이동거리, 칼로리, 속도 등 정보를 실시간으로 확인할 수 있다. 또한, 운동 후 기록을 저장할 수 있어서 체계적인 관리가 가능하다. 스웨덴의 스타트업 기업 메멘토는 30초마다 자동으로 사진을 촬영하는 아주 작은 크기의 라이프로깅 카메라를 개발하였다. '메모토(Memoto)'라고 이름 붙인 이 제품은 SD 카드 정도의 크기이지만 카메라, GPS, 가속도계가 탑재되어 있으며, 30초마다 자동적으로 카메라에서 5메가 픽셀의 사진을 촬영한다. 메모토에 담긴 사진은 클라우드에 저장되며 GPS를 사용해 사진의 타임스탬프에 위치를 기록할 수 있다. 사생활 보호를 위해 모든 사진은 암호화 되며, 애플리케이션을 통해 장소, 시간, 가속도, 빛의 레벨에 따라 검색과 추출이 가능하다. 하피라브스는 사용자의 음식 먹는 속도를 자동으로 분석하여 체계적인 식습관 조절을 돕는 스마트 포크를 개발하였다. '해피포크(HAPIfork)'라는 이름의 스마트 포크에는 내부에 내장된 센서를 통해서 음식 먹은 숫자를 자동으로 카운트 할 수 있도록 설계되어 있다[2]. 측정된 속도가 건

강한 식사를 위한 속도보다 빠르면 포크 머리 부분에서 진동이 울려서 사용자로 하여금 음식 먹는 속도를 줄이도록 유도해준다. 스마트 포크와 연동되는 스마트폰 애플리케이션에 수면 시간과 식사량 등의 데이터가 기록돼 본인의 식습관에 대한 정보를 확인할 수 있으며 친구들과 속도를 비교할 수도 있다. 소니는 심박 센서를 탑재한 스마트밴드2 SWR12를 개발하였다[3]. 스마트밴드2 SWR12는 걷기, 달리기, 수면 등 일상 활동을 실시간 기록하고, 심박수 변화를 파악해 일상생활에서 발생하는 스트레스 및 회복 수준을 상시 모니터링해주는 도구이다. 소니의 라이프로그 애플리케이션과 연동해 심박수와 스트레스 수준, 칼로리 소모량뿐 아니라, 사용자의 수면 주기, SNS 사용량, 운동량, 음악 및 영상 감상, 게임 등 사용자의 생활패턴과 활동을 체크하고 기록할 수 있다. 국내의 라이프로그 서비스의 경우, 파수닷컴은 개인이 기록한 모든 정보를 연결해 필요한 정보를 찾기 전에 보여주는 '디지털페이지'를 개발하였다. '디지털페이지'는 업무와 관련된 정보, 일정, 할일, 아이디어 등 일상에 관한 어떤 정보든 형식 없이 자유롭게 기록하고, 기록한 정보들을 연결하여 찾기 전에 보여준다. 또한, 머신 러닝 기술을 적용하여 작성된 페이지와 연관된 페이지를 함께 제시함으로써, 관련된 기록을 일일이 찾지 않아도 연관된 모든 정보를 손쉽게 관리할 수 있으며 인라인 태그를 이용하면 연락처, 지도, 캘린더 앱 등과 연동되어 하나의 앱에서 일상의 기록을 관리할 수 있다. 하지만, 기존에 제시된 건강 라이프로그 서비스는 가장 중요한 보안에 대해서는 연구가 미흡한 상황이다[4,5]. 따라서, 본 논문에서는 건강 라이프로그 서비스를 제공함에 있어서 필요한 보안 위협요소를 분석하고, 그 결과를 토대로 보안 참조모델을 제시하고자 한다.

III. 건강 라이프로그 보안위협 요소 분석

본 장에서는 건강 라이프로그 서비스 보안 참조 모델을 위한 보안위협 요소들을 분석하고자한다. 먼저 건강 라이프로그 서비스의 구성요소를 살펴보자. 건강 라이프로그 서비스는 대부분 그림 1과 같이 건강라이프로그 단말부, 건강라이프로그 중계부, 건강라이프로그 서버, 건강라이프로그 분석부의 구성요소를 가진다.

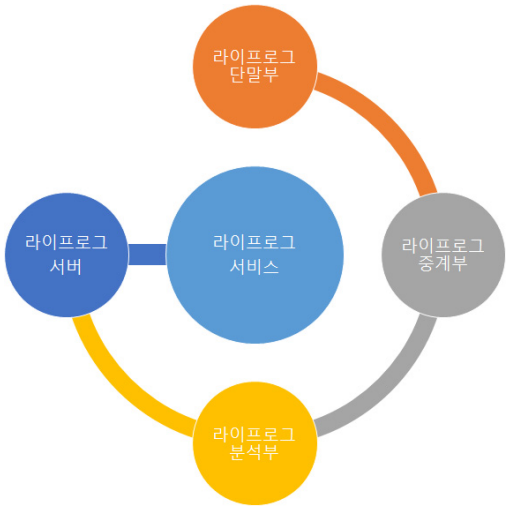

그림 2. 건강 라이프로그 서비스 참조모델
Fig. 2. An reference model of health lifelog service

건강 라이프로그 단말부는 건강 라이프로그 디바이스를 포함하는 건강 라이프로그를 측정 및 수집하는데 이용되는 전용기기 혹은 스마트 기기를 말한다. 건강 라이프로그 중계부는 건강 라이프로그 단말부를 통해 수집된 데이터를 표준데이터로 전송하기 위해 표준 포맷으로 변환하고 전송하는 기기이다. 건강 라이프로그 서버는 사용자의 라이프로그 정보를 전달받아 데이터베이스로 저장하고 저장 및 검색을 지원한다. 건강정보 분석부는 건강 라이프로그 데이터의 분석된 결과를 바탕으로 유저에게 다양한 건강관리를 위한 가이드라인을 제공한다. 건강라이프로그 디바이스들은 다수의 건강라이프로그 디바이스 공급자들에 의해 수집되고 있으며, 이를 위해 공통의 표준화된 프로토콜을 통해 디바이스 공급자 서버와 서비스 제공자 서버 간에 데이터 교환이 이루어진다. 또한, 디바이스 공급자와 서비스 제공자는 동일한 서비스 내에 존재할 수 있다. 서비스제공자는 표준화된 표현형태의 건강라이프로그 데이터를 받아서 처리 및 분석하며 다른 유관기관 또는 연계서비스와 데이터를 교환하거나 공유할 수 있다. 일반적으로 보안은 정보의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 등을 유지하는 것이며, 이러한 속성을 저해하는 행위를 보안위협이라고 할 수 있다[6]. 건강 라이프로그 서비스는 디바이스, 네트워크, 서버간의 보안이 이루어져야 하며, 건강라이프로그 단말부, 건강라이프로그 중계부, 건강라이프로그 서버, 건강라이프로그 분석부와 같은 라이프로

그 시스템 구성요소 뿐 아니라 네트워크나 서비스 영역까지 발생할 수 있다. 건강 라이프로그 단말과 서버의 경우, 악성코드 및 바이러스 감염, 사용자 정보를 탈취하는 백도어(Backdoor) 생성, 악의적인 펌웨어, 운영체제 보안의 취약성, 잘못된 시스템 보안 정책으로 인한 오류 등의 위협요소가 존재한다. 건강 라이프로그 네트워크의 경우, 데이터의 위변조나 가로채기, 비 인가된 접근, 프로토콜의 취약성을 이용한 공격, 서비스 거부, DDoS, 무결성 오류 등의 위협요소가 존재한다. 건강 라이프로그 응용프로그램 및 서비스의 경우, 서비스 거부, 패스워드 유출로 인한 피해, 악의적 사용자의 접근, 버퍼 오버플로우, 프라이버시 침해, 시스템 장애 등의 위협요소가 존재한다. 이와 같이 다양한 형태의 보안 위협요소로부터 데이터 유출, 프라이버시 침해, 서비스 안정성 파괴 등의 문제가 발생할 수 있다. 개인의 민감한 생체정보나 데이터가 암호화되지 않고 평문으로 전송되는 경우 유출의 심각한 문제가 발생하게 되며, 건강 라이프로그 정보를 전송하는 과정에서 데이터를 중간에 가로채어 위조 및 변조를 통해 인가된 사용자처럼 위장하여 프라이버시가 침해될 수 있다. 단말부의 경우 주기적으로 수집된 라이프로그 정보를 중계부나 서버에 주기적으로 전송해야하는 관계로 가용한 컴퓨터 자원을 소모시키고 정상적인 서비스가 불가능할 수 있도록 유도가 가능하다.

IV. 건강 라이프로그 서비스 보안 참조모델

본 장에서는 3장에서 제시된 보안 위협요소 분석에 따라 건강 라이프로그 서비스 보안 참조 모델을 제시하고자 한다. 건강 라이프로그 단말부는 인가 및 인증 모듈을 제공해야 하며, 건강 라이프 중계기로 안전한 데이터 교환 기능을 지원하기 위해 암호모듈을 구현해야한다. 건강 라이프로그 중계부는 인증 및 암호모듈 뿐 아니라 접근제어 모듈이 구현되어야 하며, 건강 라이프로그 중계부 내부에 방화벽을 구축해야한다. 건강 라이프로그 서버는 중계부와 마찬가지로 암호모듈, 인증모듈, 접근제어 모듈을 구현해야한다. 또한, 건강 라이프로그 데이터에 대한 감사모듈과 저작권 및 신뢰성을 위해 정보증명 모듈을 구현해야하며, 건강 라이프로그 서버 내부에 방화벽을 구축해야한다. 건강정보 분석부는 기본적인 암호모듈, 인증모듈, 접근제어 뿐 아니라 감사기록의 기능을 구현해야한다. 또한, 건강 라이프로그 분석부 내부에 방화벽을 구축해야한다. 건강 라이프로그 서비스는 서비스 간 연계를 위한 최소 요구 조건을 준수하는 것을 통해 다양한 형태로 서비스 될 수 있다. 따라서, 다양한 제공자의 건강 라이프로그 서비스 제공을 위해서 각 사용자를 식별하기 위한 개인 식별방법을 제공하여야 하며 트랜잭션이 수행될 때마다 감사로그가 기록되어야한다 건강 라이프로그 제공자 간 데이터 교환은 건강 라이프 데이터 이송을 포함하여 다른 건강서비스 제공자가 필요로 하는 데이터의 요청을 처리하기 위한 의료정보 표준 프로토콜을 지원해야하며, 사용자 데이터 교환 및 검색을 지원해야 한다. 마지막으로, 암호모듈, 인증모듈, 접근제어 모듈 구현을 통해 보안 요구사항을 만족해야한다.

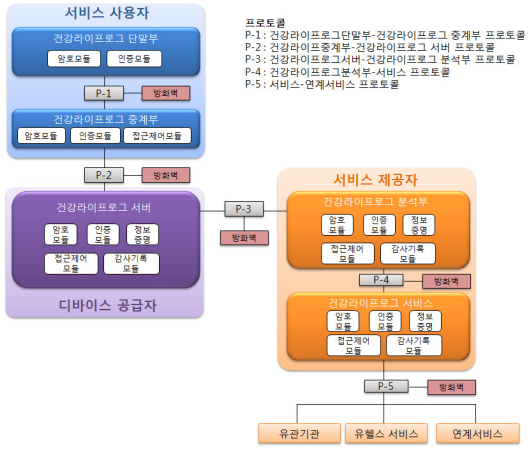

그림 3. 건강 라이프로그 서비스 보안 참조 모델
Fig. 3. Security reference model for health lifelog services

건강 라이프로그 서비스를 제공할 경우 다른 서비스 사이에 방화벽을 구축해야한다. 보안 참조모델에서 제공되어야 할 보안 기능에 대한 자세한 설명은 다음과 같다.

1. 인증(Authentication)

인증은 시스템에 접속하는 사용자가 등록 혹은 승인된 사용자인지를 확인하는 보안 절차를 의미한다. 건강 라이프로그 시스템은 건강 라이프로그를 접속하려는 모든 사용자와 객체에 대해서 인증해야한다. 다른 어플리케이션을 통해 건강 라이프로그 정보에 접근하려는 경우도 반드시 해당 어플리케이션에 대한 인증이 먼저 이루어져야 한다. 건강 라이프로그 시스템은 건강 라이프로

그 어플리케이션 사용자에게 인증 메커니즘을 제공해야 한다. 건강 라이프로그 시스템은 건강 라이프로그 사용자를 구별할 수 있도록 유일한 식별자를 소유해야 하며 사용자와 시스템간의 세션 접속이 이루어지기 전에 인증 절차를 완료해야 한다. 건강 라이프로그 어플리케이션 혹은 건강 라이프로그 시스템은 미리 정의된 보안 정책 혹은 개인정보 보호법에 따라 데이터의 접근을 통제해야 한다. 또한, 건강 라이프로그 시스템은 다른 외부 시스템과 신뢰적인 방법을 통하여 데이터를 교환하고 접근할 수 있도록 건강 라이프로그 시스템 접속을 통제해야 한다. 건강 라이프로그 시스템의 인증방법은 보안레벨에 따라 적절히 선택되어야 하며 하나 이상의 보안방법을 조합하여 사용할 수 있다. 또한, 보안 위협이 복잡해지고 다양해짐에 따라 인증 메커니즘 방법도 주기적으로 변경해야하며, 다양한 암호학적 방법과 일회용 패스워드 방식이 적용될 수 있다. 건강 라이프로그 정보에 대해 생성, 읽기, 수정, 전송, 요청의 유효성을 결정할 수 있다.

2. 인가(Authorization)

인가는 특정한 프로그램, 데이터 또는 시스템 서비스 등에 접근할 수 있는 권한을 부여하여 시스템 보안을 유지하는 방법을 말한다. 건강 라이프로그 시스템은 건강 라이프로그 사용자, 의료인, 시스템 관리자와 같은 개인들이 건강 라이프로그 정보의 전부 혹은 부분적인 접근할 수 있도록 기능을 제공해야 한다. 사용자는 미리 접근 제어 규칙을 정의함으로써 자신의 건강 라이프로그 정보 접근을 승인하거나 거부할 수 있으며, 건강 라이프로그 시스템 접속이 승인 완료된 경우 건강 라이프로그 시스템을 사용하려는 사용자 혹은 객체의 접근 제어 목록을 관리해야 한다. 건강 라이프로그 시스템에 접속하려는 사용자에 대한 분류 방법은 인지 불가능해야 한다. 건강 라이프로그 시스템은 건강 라이프로그 사용자를 위해 인가된 건강 라이프로그 사용자의 신분, 규칙, 콘텐츠, 보안 정책에 따라 서로 다른 서비스 레벨에 따라 인가해야 하며, 응급상황의 경우 사용자의 지시사항, 보안 정책, 개인정보보호법에 따라 건강 라이프로그 정보의 접근제어를 지원해야한다. 건강 라이프로그 사용자는 건강 라이프로그 정보에 포함시킬 데이터의 범위를 정해야 한다. 수정 불가능한 문서에 민감한 건강 라이프로그 정보가 포함될 경우 개인 프라이버시 문제를 발생하기 때문이다. 건강 라이프로그 사용자가 건강 라이프로그 정보 공유를 위해 어떤 정보를 공개하고 어떤 정보를 은폐할 것인지에 대한 선택할 수 있도록 기능을 제공해야 한다.

3. 접근제어(Access Control)

접근제어란 정보 보안 정책에 따라 사용자, 프로그램, 프로세서, 시스템 등을 허가된 주체만이 정보 시스템 자원에 접근할 수 있도록 제한하는 것이다. 건강 라이프로그 시스템은 비 인가된 건강 라이프로그 자원의 사용을 막기 위해서 건강 라이프로그 시스템 사용자, 건강 라이프로그 어플리케이션, 건강 라이프로그 제공자 등 건강 라이프로그 기능 및 시스템 구성요소 모두에 대한 접근 제어가 검증되고 실행되어야 한다.

4. 부인방지(Non-Repudiation)

부인방지는 메시지의 송수신이나 교환 후, 송수신 거래 사실을 사후에 증명함으로써 부인을 방지하는 보안 기술을 말한다. 건강 라이프로그 시스템은 건강 라이프로그 시스템에 의해 인증된 데이터 생성, 수신, 데이터 교환에 대한 부인을 하지 못하도록 해야 한다. 건강 라이프로그 시스템은 생성된 데이터 기록의 원본이 원본임을 부인할 수 없도록 보장해야 한다. 특별히, 건강 라이프로그 관련 메시지를 수신하거나 발신한 경우 이를 부인하지 못하도록 해야 한다. 부인방지는 디지털 서명 같은 방법이 의해 달성될 수 있으며, 디지털 영수증을 생성하기 위해 전송된 메시지를 활용할 수 있다. 부인봉쇄에 사용되는 날짜와 시간은 표준 시간 참조에 의해 기록되어야 한다. 건강 라이프로그 시스템은 보안 정책이나 개인정보 보호법에 의한 요구에 의해 수행한 행위를 구분하고 초기 구성요소, 수정, 데이터교환에 대한 타임스탬프를 유지해야 한다.

5. 안전한 데이터 교환(Secure Data Exchange)

건강 라이프로그 시스템은 서비스 제공자와 사용자 사이에 안전한 데이터 교환을 지원해야 하며 데이터 교환에 대한 무결성과 신뢰성을 보증해야 한다. 건강 라이프로그 데이터 교환은 적절한 보안성과 기밀성 등의 고려사항을 요구해야 하며 필요한 경우 데이터의 수신처/발신처에 대한 데이터 은폐를 할 수 있으며 상황에 따라 서로 다른 보안 정책들이 적용될 수 있다. 건강 라이프로그 시스템은 건강 라이프로그 데이터의 일치성과 호환성을 보장해야 한다. 건강 라이프로그 시스템은 비신뢰적

인 링크를 통해 데이터가 전송될 경우 암호화/복호화된 데이터를 전송해야 한다. 건강 라이프로그 시스템은 필요한 경우 안전한 데이터 라우팅과 데이터 익명화를 제공할 수 있다. 데이터 교환을 위해 암호화가 사용되는 경우 표준화된 암호화 방법을 사용하여 데이터를 암호화할 수 있어야 한다.

6. 정보 증명 (Information Attestation)

정보증명은 임의 정보에 접근할 수 있는 주체의 능력이나 주체의 자격을 검증하는데 사용되는 수단을 말한다. 건강 라이프로그 시스템은 수집 및 공개되는 건강 라이프로그 정보와 관련된 보증서명 유지를 포함하여 건강 라이프로그 정보에 대한 전자적 보증을 관리해야한다. 정보 보증의 목적은 건강 라이프로그에 대한 행위, 사건, 조건, 선택, 진단에 대한 책임을 할당하고 저작권을 보여주기 위함이다. 건강 라이프로그 정보의 각 요소는 저자를 명시해야 하고 타인에 의해 생성되고 서명될 수 없는 저작권으로 구별되어야 한다. 정보 증명 기능은 합법적이고 정당한 요구에 의해서 유지되어야 하고, 정보 증명 기능을 제공할 경우 건강 라이프로그 정보는 관련 의료인 혹은 법적 보증인에 의해 신뢰할 수 있어야 한다.

7. 비밀성과 신뢰성(Privacy and Confidentiality)

비밀성은 비합법적인 사용자에 대한 시스템 상의 데이터 혹은 시스템 간의 교환, 전송되는 데이터의 내용을 볼 수 없게 하는 기능이다. 신뢰성은 시스템에 요구되는 기능을 명백히 규정된 조건 하에서 명세한 시간 동안 제공하는 것이다. 건강 라이프로그 시스템은 보안 메커니즘 구현을 통해 적용 가능한 합법적이고 조직적인 개인정보보호 규칙의 집행이 가능해야 한다. 지역적/분산적 네트워크상에 존재하는 인증된 건강 라이프로그 정보를 가지고 건강 라이프로그 시스템에 접근할 수 있도록 개인의 비밀성과 신뢰성이 지켜져야 한다. 가능한 개인이 민감할 수 있는 정보가 드러나지 않도록 개인정보 규칙이 다양해야 하며 민감한 건강라이프 정보에 대한 보호가 이루어져야 한다. 건강 라이프로그 시스템은 건강 라이프로그 사용자의 의도, 데이터 요구의 사용 허가, 보안 정책과 개인정보보호법에 따라 응급상황과 같은 특별한 상황에서 은폐된 정보의 공개를 지원해야 하며 투명한 비밀성 정책 유지해야 한다. 건강 라이프로그 시스템은 건강 라이프로그 사용자가 건강 라이프로그 시스템의 비밀성 정책에 동의할 수 있는 기능을 지원해야 한다.

8. 서비스 가용성(Service Availability)

서비스 가용성은 서버와 네트워크, 프로그램 등의 시스템이 정상적으로 사용 가능한 정도를 의미한다. 건강 라이프로그 시스템에서 서비스 가용성이란 잠정적으로 서비스를 사용할 준비가 되어있는 날짜와 시간으로 표현된다. 건강 라이프로그 시스템의 가용성(데이터 접근에 대한 서비스의 날짜와 시간)과 적시성(데이터요구에 대한 반응시간)은 건강 라이프로그 사용자 혹은 건강 라이프로그와 서비스 제공자 사이의 단계별 서비스 동의를 명세화함으로 이루어질 수 있다. 건강 라이프로그 시스템은 보안 정책과 개인정보 보호법에 따라 인증된 건강 라이프로그 사용자에게 단계별 서비스 동의정보를 제공할 수 있는 기능을 지원해야한다. 건강 라이프로그 시스템은 단계별 서비스 동의에 명시된 대로 서비스 가용성 통계를 포함하여 건강 라이프로그 사용자에게 성능 통계를 제공해야한다.

9. 감사기록(Auditable Records)

감사기록은 시스템 사용자의 행위에 대한 증거가 되는 데이터를 시간 순으로 기록, 저장하는 것을 말한다. 건강 라이프로그 시스템은 육하원칙에 따라 행위의 기록을 지원해야한다. 라이프로그 정보의 생성, 수정, 읽기, 추출, 삭제에 대해 날짜와 시간을 표준시간 참조에 따라 이루어져야 하며, 감사기록기능은 개별적 라이프로그 기록에 대한 기록과 리포트를 생성할 수 있어야 한다.

지금까지 라이프로그 서비스를 제공함에 있어 보안 참조모델에서 제공되어야 할 기능에 대해서 자세히 살펴보았다. 건강 라이프로그 정보 보호 참조 모델에서는 제시된 모든 보안 기능의 구현을 원칙으로 하지만, 상황과 경우에 따라 융통성 있는 참조모델로 활용되어야 한다.

V. 결 론

최근 의료 환경이 의료기관 중심에서 소비자중심으로 이동하고 있으며, 개인이 스스로 자신의 건강과 관련된 라이프로그를 기록하고 관리할 수 있는 건강 라이프로그 서비스가 활성화되고 있다. 건강 라이프로그에는 각 개인의 사생활과 관련된 민감한 정보가 포함되어 있을 수

있으므로 개인정보 유출을 위해서는 보안이 필수적이다. 하지만, 대부분 라이프로그 서비스에서는 보안에 대한 고려가 미미한 상황이다. 본 논문에서는 건강 라이프로그 서비스에서 발생되는 보안위협 요소를 분석하였고, 분석된 결과를 바탕으로 건강 라이프로그 서비스에서 안전한 보안을 제공할 수 있는 보안 참조 모델을 제시하였다. 제안된 보안 참조 모델의 적용은 향후 건강 라이프로그 서비스를 제공함에 있어서 건강 라이프로그 정보에 대한 비밀성, 신뢰성, 무결성을 보장하고 보안성이 강화된 서비스를 제공 할 수 있다.

References

[1] https://secure-nikeplus.nike.com
[2] Kiyoharu Aizawa, Yuto Maruyama; He Li, Chamin Morikawa, "Food Balance Estimation by Using Personal Dietary Tendencies in a Multimedia Food Log, IEEE Transactions on Multimedia, Volume: 15, Issue: 8, pp. 2176 - 2185, 2013
[3] www.wareable.com/sony/smartband-2-review
[4] Myung-Kyu Yi, Hee-Joung Hwang, "A Low Power Lifelog Management Scheme Based on User Movement Behaviors in Wireless Networks", The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), Vol. 15, No. 2, pp.157-165, Apr. 30, 2015.
[5] Snehal Chennuru, Peng-Wen Chen, Jiang Zhu, Joy Ying Zhang "Mobile Lifelogger - Recording, Indexing, and Understanding a Mobile User's Life ", Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Volume 76, pp. 263-281, 2012
[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 (IIBC), Vol. 15, No. 6, pp.163-171, 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)