웰니스 서비스의 u-Healthcare 보안 연구동향 및 고찰

오현석 [1], 주재웅 [1], 강원민 [1], 이강만 [2], 정화영 [3], 박종혁 [1*]
[1] 서울과학기술대학교 컴퓨터공학과
[2] 국립강릉원주대학교 컴퓨터공학과
[3] 경희대학교 후마니타스 칼리지
[1]e-mail : {ohs4401, woong07, wkaqhdsk0, jhpark1}@seoultech.ac.kr
[2]e-mail : gangman@cs.gwnu.ac.kr
[3]e-mail : hyjeong@khu.ac.kr

Research Trends and Considerations for u-Healthcare Security in Wellness Services

Hyun Seok Oh[1], Jae Woong Joo[1], Won Min Kang[1], Gangman Yi[2], Hwa Young Jeong[3], Jong Hyuk Park[1*]
[1]Dept. of Computer Science and Engineering and Dept. of Interdisciplinary Bio IT Materials, SeoulTech, Korea
[2]Dept. of Computer Science and Engineering, Gangneung-Wonju National University, Korea
[3]Humanitas College of Kyung Hee University, Seoul, Korea

요 약

최근 Wellness 산업과 스마트 디바이스가 융합되면서 기존의 질병관리 체계보다 앞서 예방하는 건강관리 u-Healthcare 가 개발되고 있다. 하지만 u-Healthcare 에서 취급되는 개인정보 및 의료정보는 메시지 탈취/변조로 인해 공격자에게 악용되어 의료사고를 유발하고 환자의 생명까지 앗아갈 수 있으며 또한 프라이버시 침해로 인해 사용자의 신변을 보장 받을 수 없다. 본 논문에서는 웰니스 서비스의 u-Healthcare 보안의 고려사항과 연구동향에 대해 살펴보고 현재 u-Healthcare 분야에서 보안이 적용된 시스템에 대해 분석하고 취급되는 정보보호의 중요성에 대해 고찰한다.

1. 서론[1]

최근 스마트 디바이스 및 Wearable Device 와 Wellness 의 개념을 접목시킨 휴대가 용이한 건강관리 기기가 등장함에 따라 사용자의 생체신호 및 건강상태가 장소와 시간에 관계없이 일상생활에서 쉽게 확인할 수 있는 서비스가 개발되고 있다. 더불어 유비쿼터스 컴퓨팅 환경과 바이오 기술이 융합되어 u-Healthcare 서비스 분야의 연구가 활발히 진행 중이다. u-Healthcare 서비스 환경에서는 환자의 생체신호 및 건강정보를 수집하여 유·무선 네트워크를 통해 간단한 진료부터 원격진료 등의 건강관리 서비스를 제공한다. 하지만 u-Healthcare 서비스에서는 환자를 식별할 수 있는 정보와 환자의 병력까지 정보로써 활용하기 때문에 메시지의 탈취, 변조, 서비스 방해 공격 등의 공격이 가능하여 보안적인 문제점을 갖는다. u-Healthcare 에서 수집되는 수 많은 개인정보, 진료정보, 생체정보, 건강상태 등이 악의적으로 사용될 경우 사용자의 생명까지 위협하는 결과를 초래한다. 따라서 개인 프라이버시를 보장하고 안전한 정보 공유와 같은 보안기법 등이 필요하다 [1, 2].

*교신저자: 박종혁(서울과학기술대학교)

본 논문에서는 웰니스 서비스 중 최근 관심이 집중되고 있는 u-Healthcare 서비스의 보안 고려사항에 대해 논의하고 연구동향에 대해 분석 및 고찰한다.

2. 보안 고려사항

u-Healthcare 의 보안 환경에서는 인증, 무결성, 기밀성, 접근제어, 프라이버시 보호 등에 대해 고려해야 한다.

2.1 인증

u-Healthcare 에서의 시스템은 인가된 사용자만 시스템에 접근이 가능해야 한다. 인증을 통하여 관리자 및 의료종사자 신원을 확인 한다 [3].

2.2 무결성

개인 의료정보 위·변조에 대한 무결성이 보장되어야 한다. 사용자의 진료정보 및 생체정보가 공격자에게 의해 악용될 시 의료사고 및 부정확한 정보제공을 유발할 수 있다. 디지털 서명으로 무결성을 보장한다 [3].

2.3 기밀성

환자 정보에 대한 기밀성이 보장되어야 한다. 환자의 의료정보와 개인정보, 생체정보와 같은 개인정보는 병원 DB 및 u-Healthcare DB 에서 암호화를 통해

저장 · 관리해야 한다 [3].

2.4 접근제어

사용자의 정보에 접근제어를 통해 데이터 및 시스템에 접근제어를 해야 한다. 인가 되지 않은 관리자 및 의료종사자, 기타사용자에게 권한 및 역할을 부여하여 정보접근에 제한을 둔다 [4].

2.5 프라이버시 보호

u-Healthcare 에서 취급되는 개인정보, 진료정보, 생체정보, 건강상태 등은 외부로 유출되거나 공개되었을 경우 프라이버시 침해가 된다. 환자의 명예, 경제적인 피해를 대비하여 프라이버시 보호가 제공되어야 한다 [3, 4].

3. u-Healthcare 보안 연구동향 및 비교 분석

3.1 연구동향

본 절에서는 웰니스 서비스의 u-Healthcare 보안 연구동향에 대하여 논의한다.

송제민 외 3 명은 역할기반 접근제어 모델을 적용하여 개인의 프라이버시와 개인 정보보호를 제공하는 RBAC(Role-Based Access Control Model)에 기반한 개인 맞춤형 건강 정보 제공 healthcare 서비스 플랫폼을 제안했다. CCR(Continuity of Care Record)을 기반으로 한 데이터 저장과 메시지 송수신 방식으로 PHR(Personal Health Record) 정보 관리 및 교환 서비스 기능과 사용자 관점과 전문가 관점으로 나누어 자가진단 및 건강관리 서비스 기능, 구매정보 및 의료정보가 일정 수 이상 일치한 경우 개인 맞춤형 의료정보 판매 서비스 기능, 스마트 디바이스를 통한 약물정보 검색 및 제공 서비스를 설계하였다 [5].

윤은준 외 1 명은 병원 내 환자들 모두 RFID 태그를 스마트 밴드형태로 착용하고 있는 상태와 의료 종사자들이 사용하는 통신 채널은 안전한 채널임을 가정하고 RFID 기반의 환자 인증 프로토콜과 데이터베이스 보안 프로토콜을 통하여 보안성과 효율성을 제공하는 RFID 환자 인증 시스템을 제안하였다. 의료 DB 보안을 위해 2n 번의 해쉬/MAC 연산을 통하여 인증을 빠른 시간에 할 수 있는 특징을 갖는다 [6].

Nikooghadam 외 1 명은 AES(Advanced Encryption Standard)와 ECC(Elliptic Curve Cryptosystem) 암호 시스템을 사용하여 하이브리드 암호시스템을 적용한 모바일 에이전트를 제안하였다. 이는 의료정보의 보안요구사항을 고려하여 송수신 파일에 대한 기밀성과 인증을 제공한다. 또한 기존의 보안 스킴들이 MITM Attack 에 취약함을 증명하였다 [7].

3.2 비교 분석

본 절에서는 웰니스 서비스의 u-Healthcare 보안관련 기존 연구를 비교 분석한다. 2 장에서 논의된 보안 고려사항인 인증, 무결성, 기밀성, 접근제어, 프라이버시 보호를 분석요소로 한다.

<표 1> 연구동향 비교 분석

기존연구 / 분석요소	[5]	[6]	[7]
인증	╳	○	○
무결성	╳	○	╳
기밀성	○	○	○
접근제어	○	○	○
프라이버시 보호	○	○	○

(○: 강함, △: 보통, ╳: 약함)

u-Healthcare 보안 고려사항에서의 인증은 RFID 를 이용한 환자 인증 시스템[6]과 하이브리드 암호시스템을 적용한 모바일 에이전트[7]는 고려를 하였지만 RBAC 기반의 개인 맞춤형 건강정보관리 서비스 플랫폼[5]은 인증 프로토콜이나 시스템에 대해 고려하지 않는다. 무결성은 [5], [7]에서 고려되지 않았지만, [6]에서 제안되는 시스템에서는 자신의 DB 에 저장되어 있는 정보와 병원으로부터 수신한 정보가 일치 하지 않을 시 오류 메시지로 무결성을 검증한다.

4. 결론 및 고찰

본 논문에서는 웰니스 서비스의 u-Healthcare 보안 고려사항과 연구동향에 대해 논의하고 현재 u-Healthcare 분야에서 보안이 적용된 시스템들에 대해 분석하였다.

웰니스 서비스의 u-Healthcare 는 개인정보, 진료정보, 생체정보, 건강상태 등 민감한 의료정보를 다루는 서비스임에도 불구하고 메시지 탈취 및 위 · 변조와 같은 공격에 취약한 보안적 한계점이 존재한다. u-Healthcare 정보가 유출 될 시 금전적 피해를 포함하여 사용자의 생명까지도 위협받을 수 있기 때문에 u-Healthcare 에 대한 보안 취약점을 분석하여 사고를 미연에 방지하고 개인정보를 보호하는 연구가 필수적이다. 따라서 웰니스 서비스의 u-Healthcare 의 사용자와 서비스제공 관리자 간의 데이터 암호화 및 안전한 인증을 제공하는 정보공유 솔루션과 웰니스 서비스 환경에서의 개인 프라이버시 보장에 대한 법적 제도 마련이 필요하다. 향후 웰니스 서비스의 거듭되는 무선 네트워크 기술발전에 앞서 u-Healthcare 에 대한 보안 연구 또한 계속되어야 할 것으로 사료된다.

Acknowledgment

본 연구는 미래창조과학부 및 정보통신산업진흥원의 ICT 융합고급인력과정지원사업의 연구결과로 수행되었음 (NIPA-2014-H0401-14-1022)

참고문헌

[1] 오동은, 박요셉, 박광호, 김희철. “웨어러블 컴퓨팅과 웰니스 휴먼케어”, 한국컴퓨터정보학회지, 제 21 권, 2 호, pp. 11-15, 2013.

[2] 윤은준. “u-헬스케어 서비스에서의 정보보호 기술동향”, 한국통신학회지, 제 29 권, 10 호, p. 55-65, 2012.

[3] 강영진, 이훈재. “u-헬스케어 보안 위협 및 향후 대책”, 한국컴퓨터정보학회 하계학술대회 논문집, 제 20 권, 2 호, pp. 55-58, 2012.

[4] 송유진, 박광용. “의료데이터 공유 및 활용 서비스를 위한 보안/프라이버시 요구사항”, 정보보호학회지, 제 20 권, 3 호, pp. 90-96, 2010.

[5] 송제민, 김명식, 정경지, 신문선. “RBAC 에 기반한 개인 맞춤형건강 정보 제공 헬스케어 서비스 플랫폼”, 한국산학기술학회논문지, 제 15 권, 3 호, pp. 1740-1748, 2014.
[6] 윤은준, 유기영. “의료정보보호를 위한 RFID 를 이용한 환자 인증 시스템”, 한국통신학회논문지, 제 35 권, 6 호, pp. 962-969, 2010.
[7] Morteza Nikooghadam, Ali Zakerolhosseini. “Secure Communication of Medical Information Using Mobile Agents”, Journal of medical systems, Vol.36, No.6, pp. 3839-3850, 2012.