클라우드기반 u-헬스케어 시스템을 위한 보안 이슈 및 요구사항 분석

이영실* · 김태용** · 이훈재**

*동서대학교 일반대학원 유비쿼터스 IT학과

**동서대학교 컴퓨터정보공학부

Security issues and requirements for cloud-based u-Healthcare System

Young Sil Lee* · TaeYong Kim** · HoonJae Lee**

*Dept. of Ubiquitous IT, Dongseo University Graduate School

**Div. of Computer Information Engineering, Dongseo University

E-mail : youngsil.lee0113@gmail.com, tykimw2k, hjlee@dongseo.ac.kr

요 약

디지털 기기 간 융합과 무선 통신 기술의 발전, 생체신호 측정 센서의 소형화, 종이나 수기로 관리되던 의료관련 정보를 디지털화한 전자의무기록(EMR, Electronic Medical Record) 구축 및 전자건강기록(EHR, Electronic Health Record)의 도입 등으로 인해 '언제 어디서나' 자신의 건강 상태를 모니터링하고 개인 맞춤 건강관리 서비스를 받을 수 있는 Ubiquitous Healthcare (u-헬스케어) 시대가 도래하였다. 또한 클라우드 컴퓨팅(Cloud computing) 기술의 등장은 u-헬스케어 서비스의 발전을 더욱 가속화시키고 있는 요인 중 하나이다. 그러나 이러한 u-헬스케어 서비스 활용 과정에서 개인의 정보가 악의적으로 사용될 경우 정확하고 신뢰성 있는 헬스케어 서비스를 제공받지 못할 뿐만 아니라 단순 건강 검진 및 치료의 수준을 넘어 크게는 개인의 생명과 직결되는 심각한 문제를 초래한다. 이에 본 논문에서는 클라우드 컴퓨팅 환경에서의 u-헬스케어 서비스와 관련된 다양한 보안 이슈를 분석하고 이를 토대로 안전한 보안 의료정보 공유 시스템 구축을 위한 보안 요구사항에 대하여 서술한다. 더불어 향후 국내 u-헬스케어 산업 활성화를 위한 발전방향에 대하여 논하고자 한다.

ABSTRACT

Due to the convergence between digital devices and the development of wireless communication technology, bit-signal sensor miniaturization, building an Electronic Medical Record (EMR) which is a digital version of a paper chart that contains all of a patient' s medical history and the information of Electronic Health Record (EHR), Ubiquitous healthcare (u-Healthcare) that can monitor their health status and provide personal healthcare service anytime and anywhere. Also, the appearance of cloud computing technology is one of the factors that accelerate the development of u-healthcare service. However, if the individual information to be used maliciously during the u-healthcare service utilization, leads to serious problems directly related to the individual' s life because if it goes beyond the level of simple health screening and treatment, it may not provide accurate and reliable healthcare services. For this reason, we analyzed a variety of security issues related to u-healthcare service in cloud computing environment and described about directions of secure health information sharing system construction. In addition, we suggest the future developmental direction for th activation of u-healthcare industry.

키워드

u-Healthcare, Cloud Computing, Healthcare Security, Cloud Computing Security

Ⅰ. Introduction

오늘날 의료서비스 정책변화와 정보기술(IT)의 발전으로 인하여 의료 기관들은 새로운 시대적 환경변화를 겪고 있다. 즉, 소득수준과 교육의 향상, 인구의 노령화, 사회복지의 향상, 국민의 기본권리로서의 의료서비스 인식의 변화 등으로 의료서비스에 대한 질적 향상에 대한 요구가 증대되고 있다[1]. 이와 더불어 디지털 기기 간 융합과 무선 통신 기술의 발전, 생체신호 측정 센서의 소형화, 종이나 수기로 관리되던 의료관련정보를 디지털화한 전자의무기록(EMR, Electronic Medical Record) 구축 및 전자건강기록(EHR, Electronic Health Record)의 도입 등으로 인해 '언제 어디서나' 자신의 건강 상태를 모니터링하고 개인맞춤 건강관리 서비스를 받을 수 있는 Ubiquitous Healthcare (u-헬스케어) 시대가 도래하였다. 또한, 클라우드 컴퓨팅(Cloud Computing) 기술의 등장은 u-헬스케어 서비스의 발전을 더욱 가속화시키고 있는 요인 중 하나이다.

영국 BBC 보고서는 전세계 u-헬스케어 시장이 2009년 1,431억달러에서 2018년 4,987억달러로 3배 넘게 급성장할 것으로 전망했으며, 삼성경제연구소도 보고서를 통해 '향후 한국 헬스케어 산업이 글로벌 경쟁력을 갖춘 수출 산업으로 성장하고 고령화 등 신수요를 충족하기 위해서는 한국의 강점인 정보기술(IT) 및 의료서비스 역량과 제약·의료기기 산업을 접목한 「융복합형 헬스케어 산업」을 집중 육성해야 한다'고 강조한 바 있다[2].

그러나 이러한 u-헬스케어 서비스 활용 과정에서 개인의 정보가 악의적으로 사용될 경우 정확하고 신뢰성 있는 헬스케어 서비스를 제공받지 못할 뿐만 아니라 적절하지 못한 치료 등 단순 건강 검진 및 치료의 수준을 넘어 크게는 개인의 생명과 직결되는 심각한 문제를 초래한다.

이에 본 논문에서는 클라우드 컴퓨팅 환경에서의 u-헬스케어 시스템과 관련된 다양한 보안 이슈 및 요구사항을 분석하고 향후 발전 방향에 대하여 논하고자 한다.

Ⅱ. Security Issues and Requirements

2.1. Cloud Computing

이러한 클라우드 컴퓨팅은 서비스의 다양한 유형에 따라 보안 정책 및 서비스 관리 정책이 서로 상이하다. 정책을 설정함에 있어서도 표준화되어 있는 프로세스가 아직 완전히 정립되어 있지 않고, 이 때문에 클라우드 간의 협업 시스템 구축 시 또는 신뢰성 있는 클라우드 서비스 제공 시 서로 상이한 보안 및 서비스 정책으로 인한 호환성 및 관리 효율성 문제가 야기된다. 이를 해결하기 위한 보안 기능 요구사항의 정의가 시급한 실정이며, 현재 IEEE/ANSI 830-1998, NASA DID P200, DoD 498 등 국제적으로 인정받고 있는 다양한 단체들에서 각기 요구사항 명세 표준들을 제시하고 있으며, 이 중 IEEE 830이 가장 일반적으로 많이 활용되고 있다.

또한, 클라우드에 대한 보안의 인식을 높이고 지식을 공유하기 위해 2008년에 만들어진 단체인 CSA(Cloud Security Alliance)는 지난 2013년 2월에 발표한 "The Notorious Nine: Cloud Computing Top Threats in 2013" [3] 보고서를 통해 클라우드 컴퓨팅의 보안 위협에 대하여 정리하였으며 그 내용은 아래와 같다.

- Data Breaches (데이터 유출)
- Data Loss (데이터 소실)
- Account Hijacking/Service Hijacking (계정 탈취 / 서비스 탈취)
- Insecure APIs (안전하지 않은 API)
- Denial of Service (DoS;서비스 거부)
- Malicious Insiders (악의적인 내부 사용)
- Abuse of Cloud Services (클라우드 서비스의 남용)
- Insufficient Due Diligence (클라우드 서비스의 이해 부족)
- shared Technology Vulnerabilities (공유 기술의 취약점)

2.2. u-Healthcare System

u-헬스케어의 보안 이슈에 대하여 논하기에 앞서 먼저 헬스케어와 다양한 형태에 대하여 정의하고자 한다. 헬스케어란 의료진을 통한 질병의 예방 또는 치료 및 정신적·육체적 건강상태의 관리로 정의되어 있다. 즉, 건강의 관리는 질병을 극복하기 위하여 적절하게 조치하는 부분과 건강상태를 유지하기 위하여 적합한 방법을 사용하는 두 부분으로 나눠질 수 있다. 또한, IT 기술의 발전 추세에 따라 그 서비스의 형태를 e-Health, m-Health, Home-Health, Telemedicine 등으로 분류할 수 있으며, 이러한 모든 보건의료 서비스는 추후 u-Health로 포괄하는 형태로 발전할 것으로 기대된다[4].

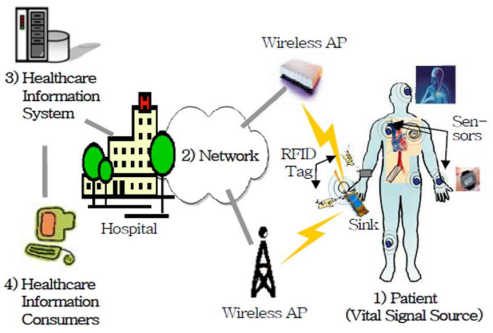

그림 1. u-헬스케어 융합서비스[5]

u-헬스케어는 다양한 기술들이 집약 및 융합된 서비스 기술로서 그림 1과 같이 생체 및 환경 정보를 센싱, 모니터링하기 위한 의료 센서나 기기, 센서 간 통신 및 데이터 송수신을 위한 유무선 네트워크, 생체 데이터 분석과 건강 피드백을 담당하는 의료 정보 서버 그리고 생성된 의료 정보를 소비하는 다양한 소비자 집단(i.e., 환자, 의료진 및 관련 종사자 등)으로 구성될 수 있다.

또한, 헬스케어 서비스의 형태로 가장 많이 알려진 m-Healthcare와 u-Healthcare에 대한 이해를 돕기 위하여 아래의 표 1에서 e-Healthcare networks와 u-Healthcare networks의 차이점을 나타내고 있다.

표 1. Difference between e-healthcare and u-healthcare networks[6].

e-Healthcare Networks	u-Healthcare Networks
Any time service	Any time/anywhere service
Mobile/Web interfaces	Mobile/peripheral device interfaces
On-line mode	On-line/Off-line mode
Geographically constrained	Geographically distributed
No location tacking	Location-sware solution
Single security agent	Collaborating security agents
Single domain security infrastructure	Multi-domain security infrastructure

u-헬스케어 서비스는 개인의 건강 및 의료 정보를 포함하며 개인적인 정보를 공유하고 다루고 있기 때문에 무선 네트워크 환경에서의 보안(Security) 및 프라이버시(Privacy) 측면에서 다양한 위협요소가 존재할 수 있다. 아래의 그림 2는 u-헬스케어 환경에서 발생할 수 있는 다양한 보안 취약점과 위협 요소들을 나타내고 있다.

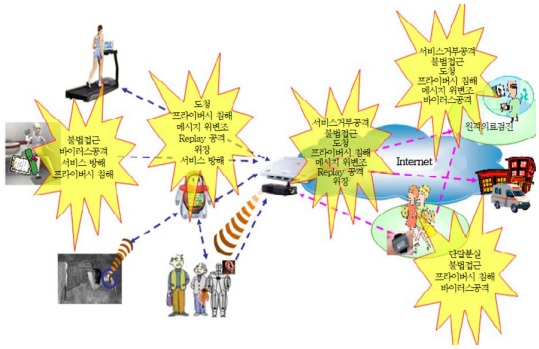

그림 2. u-헬스케어 환경의 보안 위협[5]

이를 통해 유·무선 네트워크 기반 서비스에서 발생 가능한 보안상의 취약점 및 공격이 u-헬스케어 환경에서 유사하게 전이되는 것을 알 수 있으며, 이를 보완하기 위한 안전성, 신뢰성 보장 및 데이터 보호를 위한 기술적 대안이 기본적으로 요구된다.

이와 더불어, 의료 서비스, 즉 정확한 진료를 받기 위해서는 생체 정보를 포함한 개인의 질병 내력, 가족력, 신체적 특징 등의 개인 의료 정보를 충분히 제공해야 하며, 이 정보는 환자가 이동함에 따라 중복된 검사와 의료 조치가 반복되는 것을 막기 위해 선택적으로 다른 의료 기관에 위임 및 제공되어야 한다. 따라서 의료 정보에 대한 프라이버시 보호적 차원에서의 개인 의료 정보권한 관리 및 위임, 활용에 관한 기술적, 법·제도적 지원책이 요구된다. 또한, 불법적인 의료 정보 열람과 이용을 막고 그 책임 소재를 판단하기 위해 보안 감사 체계가 보완 및 제공되어야 한다. 이는 최근 심각한 보안 취약점으로 거론되고 있는 내부자에 의한 정보 유출의 위험성을 막기 위함이다.

Ⅲ. Security Requirements for Cloud-based u-healthcare system

클라우드 기반 u-헬스케어 시스템에서는 일반적인 보안 요구사항으로 거론되는 의료 데이터의 무결성(Integrity)과 기밀성(confidentiality), 가용성(Availability)과 유용성(Utility), 인증(Authentication)뿐만 아니라, 정보 소유권(Ownership of information), 부인봉쇄(Non-repudiation), 환자 동의와 인가(Patient consent and authorization), 감사와 저장관리(Audit and archiving) 등 다양한 보안 요구사항들이 필수적으로 요구된다.

이와 더불어, 클라우드 기반 u-헬스케어 시스템은 기본적으로 병원과 클라우드 제공자에 의해 구축되며, 클라우드의 기본 형태로 분류하면 Public Cloud와 Private Cloud를 모두 이용하는 Hybrid형이라 할 수 있다. 대형 병원의 경우 자신만의 개인 클라우드 환경을 구축할 수 있으며, 진료 정보, 검진 자료, 병리 자료, 간호 차트 등과 같은 의료 정보는 병원 내 개인 클라우드(Private Cloud)와 공개 헬스케어 클라우드(Public Cloud) 내 각각 저장된다. 이러한 경우 병원간의 교차 접근을 위해 요청 병원과 소유 병원 사이의 안전한 통신로 보안(Communication channel security)이 매우 중요하다.

또한, u-헬스케어는 센서 등의 디바이스를 통해 생체 신호를 측정하고 이를 통해 사용자의 상태를 진단하는 등 헬스케어의 핵심 역할을 담당한다. 그러나 이러한 생체 신호 측정 센서 노드의 하드웨어 자원 제약으로 인해 전체 헬스케어 시

스템에 상당한 영향을 미칠 수 있다. 따라서 u-헬스케어 시스템 구축 시 이를 고려하여 효율적인 (Efficiency) 설계를 하여야 한다.

마지막으로, 응급상황을 고려한 유연성 (Flexibility)이 필요하다. 환자의 모니터링 데이터를 읽기위한 권한은 응급상황이 발생했을 때 허락된 리스트에 없는 이용 가능한 의사가 임시적으로 주어질 수 있다. 이를 위해 위임 정책을 제공하여 사용자의 위치정보에 따라 역할이 활성화될 수 있도록 유연한 설계가 필요하다.

Ⅳ. Conclusion

클라우드는 콘텐츠와 기기에 이동성을 더 높여주며 점점 더 우리 일상의 깊숙한 곳으로 파고들고 있으며, 개인의 삶과 기업의 활동에 큰 영향을 미치고 있다. 그러나 클라우드에서 시스템을 구축하고 해당 클라우드가 안전성을 보장한다고 해서 클라우드 기반 시스템의 안전성이 보장되는 것은 아니다. 클라우드로의 전이는 서버 중심의 시스템을 서비스 기반의 시스템으로 옮겨가는 것을 의미하고, 클라우드는 서비스 기반의 시스템에서 서비스가 존재할 수 있도록 하부를 제공해주는 것에 지나지 않는다[7].

이에 따라, 본 논문에서는 클라우드에서 u-헬스케어 서비스를 위한 다양한 보안 이슈와 보안 요구사항을 분석하였다. 이를 위해 최근 클라우드 컴퓨팅 환경에서의 보안 이슈를 분석함과 동시에 u-헬스케어 시스템의 보안 요구사항을 분석하였다. 또한, 이를 바탕으로 클라우드 기반의 u-헬스케어 시스템을 위한 보안 요구사항에 대하여 서술하였다.

분명, 클라우드로의 전이는 시스템의 가용성과 효율성 향상 등 다양한 이점을 가지게 되지만 새로운 보안 위협도 생겨나는 만큼 이를 위한 보안 대책이 필요하며, u-헬스케어 시스템은 소비자의 의료 정보를 다루며 이를 악용할 경우 단순 건강검진 및 치료의 수준을 넘어 크게는 개인의 생명과 직결되는 문제를 발생시킬 수 있는 만큼 더욱 신중한 접근이 필요하다 사료된다.

한편, 세계적으로 u-헬스케어 산업은 모바일, 빅데이터, 클라우드 등 다양한 기술을 접목하여 단순한 원격진료 뿐만 아니라 질병관리와 예방, 맞춤형 의료 서비스를 제공하는 신산업으로 진화하고 있으며, 국내보다 10년 이상 앞서 원격진료를 도입하고 u-헬스케어 서비스를 제공하며 지속적으로 성장하고 있다.

그러나 국내의 경우 지난 2013년 10월, u-헬스케어 산업 육성을 위해 '원격진료 허용' 관련 의료법 개정안을 입법 예고하고 진행 중이나 현재까지 정부와 의료계의 대립이 지속되고 있다. 또한 u-헬스케어에 대한 소비자의 의식이 해외와 비교하여 현저하게 낮은 수준이라 실질적으로 원격진료가 허용된다 하더라도 국내 u-헬스케어 시장 규모는 약 800만명에 불과할 것으로 추정된다[8]. 이에 따라 대부분의 국내 의료 IT업계는 해외 시장을 대상으로 사업을 진행하고 있다.

따라서 국내 u-헬스케어 산업 육성을 위해서는 u-헬스케어 기기 개발 및 정보통신기기와 시스템 개발도 중요하나, 그에 앞서 정부와 의료계, 산업계 간의 제도 확립 및 협력채널 구축과 동시에 u-헬스케어에 대한 소비자의 의식적인 변화가 선결되어야 할 것으로 사료된다.

Acknowledgement

이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행되었으며(과제번호:2013-071188) 또한, 부산광역시에서 지원하는 BB21 과제에서 지원받았음.

Reference

[1] 채련, "건강관리도 스마트하게—스마트 헬스케어 서비스," 한국선진화포럼, 2013.12.

[2] 김상현, "[2014 신년기획 기술강국 코리아] U헬스케어…스마트빌딩…기술융합으로 '1+1=3' 끌어내라," 인터넷한국일보, 2013.12.

[3] CSA, "The Notorious Nine: Cloud Computing Top Threats in 2013," Technical report, 2013.02.

[4] 진경수 외, "유헬스의 현재와 미래," 제이비콤, 2008.02.

[5] 송지은 외, "u-헬스케어 보안 이슈 및 기술 동향," 전자통신동향분석, 제22권 제1호, 2007.02.

[6] W.D. Yu, R. Gummadikayala, and S. Mudumbi, "A web-based wireless mobile system design of security and privacy framework for u-Healthcare," Proceeding of the 10th International Conference on e-health networking, applications and Services, Singapore, pp.96-101, 2008.

[7] 심상규, "클라우드 환경의 9가지 보안 이슈와 안전한 클라우드를 위한 노력," 펜타시큐리티시스템(주), 2013.04.

[8] 홍은기, "급성장하는 U헬스케어 산업 2014년 이것에 주목하라," 컴퓨터월드 News, 2014.01.