ISSN: 1226-7244 (Print)
ISSN: 2288-243X (Online)
논문번호 15-04-14

j.inst.Korean.electr.electron.eng.Vol.19,No.4,548~556,December 2015
http://dx.doi.org/10.7471/ikeee.2015.19.4.548

개인건강서비스를 위한 보안 요구사항

Security Requirements of Personal Health Service

김 상 곤*, 황 희 정**★

Sang-Kon Kim*, Hee-Joung Hwang**★

Abstract

When the variety of personal health services are provided in the ICBM(IoT, Cloud, Bigdata, and Mobile) environment, the security requirements of personal health service(PHS) including privacy issues is proposed in this paper. Because it is expected that the services related to personal health are provided in the cloud environment, the security requirements of a cloud environment is firstly investigated and then security threats including direct and indirect threats in a cloud environment are analyzed in terms of the security of PHS. In addition, the security requirements of PHS is developed based on the security requirements of electronic medical record(EMR) for medical service in this paper, then the validity of the proposed security requirements is shown by the relation between security requirements of cloud environment and PHS to indicate that a security requriement is supported by several security requirements of PHS.

요 약

본 논문에서는 다양한 형태의 개인건강서비스들이 ICBM(사물인터넷, 클라우드, 빅데이터, 및 모바일) 환경에서 제공될 때, 프라이버시 이슈를 포함하여 개인건강서비스에 대한 보안 요구사항이 제안된다. 개인건강과 연관된 서비스들은 클라우드 환경에서 제공될 것이 예상되므로, 우선적으로 클라우드 환경의 보안 요구사항에 대해 조사한 후, 클라우드 환경에서의 직접적인 위협과 간접적인 위협을 포함한 보안 위협을 개인건강서비스의 보안 관점에서 분석한다. 그리고 본 논문에서 의료서비스를 위한 전자의료기록(EMR)에 대한 보안 요구사항에 기반을 두고 개인건강서비스를 위한 보안 요구사항을 도출한 뒤, 클라우드 환경의 보안요구사항이 개인건강서비스의 보안요구사항에 의해 충족될 수 있음을 나타내는 관계를 보임으로서 제안된 개인건강서비스에 대한 보안 요구사항의 타당성을 제시한다.

Key words : Personal health service, security requirement, cloud environment, privacy issues, personal health record

* Dept. of Cyber Security, Ajou University,
e-mail : paulka@ ajou.ac.kr, 031-219-1603

**★ Dept. of Computer Engineering, Gachon University, e-mail ; hwanghi@gachon.ac.kr, 031-750-4758

※ Acknowledgment
This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.B0101-15-247, Development of open ICT healing platform using personal health data)
Manuscript received Nov. 30, 2015; revised Dec. 7, 2015; accepted Dec. 8. 2015

Ⅰ. 서론

세계적으로 인간의 수명은 연장되고 도시 중심의 생활과 함께 동반된 낮은 출생률로 인해, 노령인구의 상대적인 증가로 노령화 지수(ageing index)가 지속적으로 높아지고 있는 추세이다[1]. 이와 더불어 노령인구를 위한 건강 및 의료서비스에 대한 국가적 지출도 급속히 늘어나고 있어, 이와 같은 문제를 해결하기 위한 노력으로 정보통신기술(information communication technology, ICT)을 활용하여 ICBM 환경에서 건강관리 및 의료서비스를 “언제, 어디서나” 이용 가능하도록

만들기 위한 유헬스(u-health) 시스템 및 서비스가 도입되었고 개인의 질병관리와 더불어 건강관리의 중요성이 인식되었다.

유헬스 서비스의 일환으로 개인의 질병, 건강, 그리고 독거(independent living)를 효율적으로 점검하고 관리하기 위해 요구되는 다양한 종류의 개인건강기기들에 대한 국제표준을 ISO/IEEE 11073 개인건강기기(personal health device, PHD) working group(WG)에서 진행하고 있다[2]. 11073 PHD 표준은 11073-20601 optimized exchange protocol(OEP)을 기반으로 11073-104zz 개인건강기기들의 표준을 제정하였다[3,4]. 체중계[5], 체온계[6], 혈압계[7], 맥박계[7], 혈당계[8], 심전계[9], 독거 활동 허브[10] 등 개인의 다양한 건강관련 정보를 간헐적(episodic) 또는 주기적(periodic)으로 측정하여 개인건강관련 정보를 획득하고 이를 지정된 관리기기로 전송하여 특정한 형태의 개인건강기록(personal health record, PHR)으로 저장하고 관리한다. 이와 연관하여 240여개 회원사들로 구성된 컨티뉴아(Continua health alliance)는 다양한 개인건강기기와 관리기기의 상호 운용성(interoperability)을 지원하기 위해 11073 PHD 표준과 컨티뉴아의 추가적인 프로토콜 스택을 모두 지원하는지를 시험 및 인증하고 있다[11].

선진국들의 주도로 시작된 유헬스 서비스에 대한 요구를 기반으로, 상기의 국제표준 단체들의 활동과 더불어 개인의 건강관리를 중요하게 여기는 국제적인 시장의 변화 추세에 맞춰 다양한 형태의 개인건강서비스가 제공될 것으로 예상된다. 예를 들어, 스마트폰을 대표하는 회사들에서 스마트폰과 연동되며 개인건강기기가 탑재된 시계를 경쟁적으로 출시하고 있는 것은 향후 유헬스 서비스 시장의 성장 가능성이 높다는 것을 의미한다.

그림 1은 유헬스 서비스의 시스템 구성을 나타낸 것이다. 유헬스 시스템은 다양한 개인건강기기들과 관리기기로 구성된 11073 PHD 표준 기반의 개인건강기기 네트워크(PHD network)와 클라우드 환경에서 건강관련 서비스 제공자 네트워크(health service provider, HSP network)로 구성된다. 그리고 유헬스 서비스는 개인건강관련 서비스와 원격진료/원격의료(telemedicine)를 포함한 의료관련 서비스로 구분될 수 있으며, 본 논문은 개인건강서비스에 중점을 두고 있다.

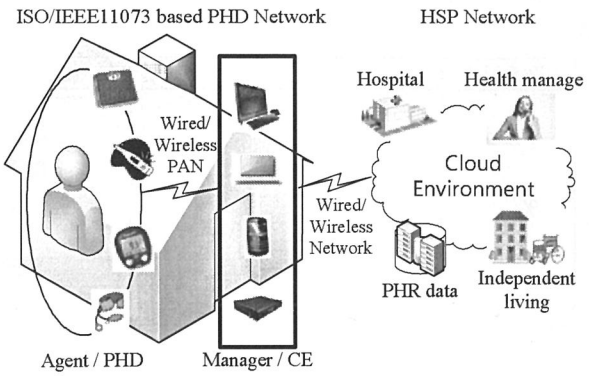

Fig. 1. Personal health service system in a cloud environment

그림 1. 클라우드 환경에서의 개인건강서비스 시스템

의료서비스의 전자의료기록(electronic medical record, EMR)은 원격 진료/의료를 포함한 의료서비스를 제공하는 의료기관 및 국가기관의 보안정책에 따라 체계적이고 안전하게 관리되는 반면 개인건강서비스를 위한 개인건강기록은 소비자들의 요구에 맞춰 출시될 다양한 형태의 개인건강서비스를 공급하는 제공자에 의해 자체적으로 관리되어야 하므로 체계적인 보안관리가 적용되기 어렵기 때문에 전자의료기록에 비해 보안적인 면에서 많은 문제점들을 드러낼 것으로 예상된다.

본 논문에서는 개인건강기기 네트워크에 속한 다수의 개인건강기기들로부터 생성된 개인건강기록을 활용한 다양한 개인건강서비스가 클라우드 컴퓨팅 기반의 클라우드 환경에서 제공될 때 발생할 수 있는 보안 요구사항을 조사하고 개인건강서비스 보안 관점에서 보안 위협을 분석한다. 그리고 개인건강서비스를 안전하게 제공하기 위한 보안 요구사항을 도출하고 검증한다.

본 논문은 다음과 같이 구성된다. 2장에서 클라우드 환경에서 정의된 요구사항을 분석하고 개인건강서비스와 연관된 보안 위협들을 도출한다. 3장에서 의료서비스를 위한 개인의료기록의 보안 요구사항을 토대로 개인건강서비스에 대한 보안 요구사항을 도출하고 클라우드 환경의 보안 요구사항과의 연관성을 확인하고 타당성을 검증한다. 본 논문의 결론은 4장에서 제시된다.

Ⅱ. 클라우드 환경의 보안 요구사항과 보안 위협

클라우드 컴퓨팅은 적용의 신속성, 비용의 효율성, 그리고 구현의 용이성을 갖추고 있어 빠르게 확산될 것으로 예상되었다. 그러나 확산 속도가 예상에 미치지 못하고 있는데 이는 보안에 대한 우려 때문인 것으로 파악되고 있다. 이에 국제표준단체에서 클라우드 컴퓨팅 보안에 대한 표준을 제정하고 있다.

Telecommunication standardization sector of the international telecommunication union (ITU-T)에서 앞서 클라우드 컴퓨팅에 대한 참조 모델 표준(ITU-T Y.3502, cloud computing reference architecture, CCRA)을 제정하여 클라우드 컴퓨팅에 대한 기본 개념과 원리에 대한 전반적인 프레임워크(framework)를 제공하였다[12].

또한, 클라우드 컴퓨팅을 위한 보안 프레임워크(ITU-T X.1601, security framework for cloud computing, SFCC)을 통해 클라우드 환경에 대한 보안 위협이 분석되었고, 이를 해결하기 위한 보안 능력(capability)에 대해 서술하였다[13].

본 장에서는 클라우드 환경에서의 보안 요구사항에 대해 분석한 뒤, SFCC에서 정의된 클라우드 환경에서의 직접적인 보안 위협(threats)과 간접적인 보안 위협(challenges)을 통합적으로 분석하여, 개인건강서비스 보안과 연관된 14개 보안 위협들을 도출한다.

1. 클라우드 환경의 보안 요구사항

클라우드 컴퓨팅은 가상화 기술(virtualization technology)을 이용하여 컴퓨팅, 네트워크, 그리고 저장장치를 공유하여 사용함으로써 사용자가 시간과 장소의 제약 없이 필요한 자원을 할당받아 사용하도록 편의성을 제공하는 동시에 전체적인 자원을 효율적으로 사용하고 관리하여 설비비용 및 운영비용을 절감하는 장점을 가지고 있다. 그러나 기존의 컴퓨터시스템 환경과 다른 가상화된 클라우드 환경에서 가능한 새로운 보안 취약점들(vulnerabilities)이 발생하고 있고, 기존의 보안 시스템으로는 적절한 대응이 어려워 클라우드 환경에서의 가상화된 서버에 대한 다섯 가지 보안 요구사항과[14] 가상화된 저장장치에 대한 네 가지 보안 요구사항이[15] 제안되었다. 상기의 보안 요구사항들을 통합적으로 분석하여 표 1과 같이 클라우드 환경에서의 서비스와 연관된 네 가지 보안 요구사항(security requirements)과 각각의 세부 요구사항(detailed requirements)을 정하였다

Table 1. Security requirements in a cloud environment
표 1. 클라우드 환경의 보안 요구사항

Security requirements	Detailed requirements
Confidentiality	Cryptographic technology
	Data encryption/decryption
	Key management
	Data transmission
Authentication & access control	Authentication management
	Account management
	Access control
	Authority control
	Session management
Integrity	Authentication code management
	Software integrity
	Data integrity
Availability	Accident monitoring
	Data backup
	Data recovery

가. 기밀성(confidentiality)

클라우드 환경의 가상화된 자원들은 인가되지 않은 사용자에 의한 접근이 가능하기 때문에, 데이터 유출에 대한 대책으로서 데이터에 대한 기밀성이 제공되어야 한다. 이를 위해 아래의 네 가지 세부 요구사항들이 지원되어야 한다.

- 암호기술(cryptographic technology)

암호화 알고리즘(algorithm)을 포함하여 인증된 암호기술이 사용되어야 공격으로부터 안전하게 데이터를 보호할 수 있다.

- 데이터 암호화/복호화(data encryption/decryption)

데이터가 안전하게 전송 및 저장되기 위해 시스템 환경을 고려하여 적절한 암호화/복호화 과정이 제공되어야 한다.

- 키 관리(key management)

기밀성을 강화하기 위해 키의 생성, 갱신, 및 폐기 등 적절한 키 관리가 필요하다.

- 데이터 전송 (data transmission)

통신과정에서 정보 또는 데이터의 획득 또는 유추를 목적으로 한 공격으로부터 보호하기 위해 안전한 데이터 전송이 필요하다.

나. 인증 및 접근 제어(authentication & access control)

클라우드 환경의 가상화된 자원들에 대한 불법적인 접근이 가능하므로 이를 방지하기 위해 인증 및 접근 제어가 제공되어야 한다. 이를 위해 아래의 네 가지 세부 요구사항들이 지원되어야 한다.

- 인증 관리(authentication management)

안전한 인증은 클라우드 환경에서 합법적인 사용자를 위한 필수 요소로 패스워드 또는 공개키 등의 방법을 이용하여 제공된다.

- 계정 관리(account management)

클라우드 서비스 제공자는 사용자 계정을 안전하게 생성하고 관리하여야 하며, 사용자의 탈퇴 시 사용자 계정의 폐기가 보장되어야 한다.

- 접근 제어(access control)

서비스 및 데이터에 대해 인증된 사용자의 접근은 보장되고 악의적인 접근은 감시 및 관리되어야 한다. 이를 위해 접근 제어관련 정책, 인증, 그리고 계정 관리 등이 필요하다.

- 권한 제어(authority control)

서비스의 관리 및 사용에 대한 권한을 계정별 보안 등급을 고려하여 부여하고 관리해야 한다.

- 세션 관리 (session management)

통신과정에서 사용자는 동시에 여러 개의 세션을 형성하여 시스템 부하를 증가시키고 보안 취약점을 드러낼 수 있으므로 세션의 생성부터 종료까지 적절한 관리가 요구된다.

다. 무결성(integrity)

클라우드 환경의 가상화된 자원들은 사용자들에 의해 공유되어 인가되지 않은 사용자에 의한 접근이 가능하기 때문에, 불법적인 수정을 방지하기 위해 무결성이 제공되어야 한다. 이를 위해 아래의 세 가지 세부 요구사항들이 지원되어야 한다.

- 인증 코드 관리(authentication code management)

수정 발생 여부를 확인하기 위해 생성하는 인증 코드에 대한 안전한 관리가 필요하다. 이것은 해시 함수(hash function)등을 이용한 다이제스트(digest) 생성 등 다양한 방법으로 제공된다.

- 소프트웨어 무결성(software integrity)

서비스와 연관된 소프트웨어 및 정보에 대한 무결성이 제공되어야 한다. 이를 위해 인가되지 않은 수정에 대한 감시와 더불어 정기적인 감시가 요구된다.

- 데이터 무결성(data integrity)

암호화, 전자 서명 등의 기술을 적용하여 데이터에 대한 인가되지 않은 수정을 방지하여 무결성을 보장해야 한다.

라. 가용성(availability)

클라우드 환경에서의 서비스는 끊임없이 지속되어야 하므로 사용자에 대한 가용성이 보장되어야 한다. 이를 위해 아래의 세 가지 세부 요구사항들이 지원되어야 한다.

- 사고 모니터링(accident monitoring)

보안 사고에 대한 체계적인 모니터링을 통해, 보안 사고에 대한 징후를 파악하고 사고 발생 시 필요한 대응 체계를 확립하여 신속하게 대응해야 한다.

- 데이터 백업(data backup)

사고 발생 시 적절히 대응하고 가용성을 제공하기 위해 정해진 정책과 절차에 따라 주기적으로 데이터를 백업해야 한다.

- 데이터 복구(data recovery)

사고 발생 시 적절히 대응하고 가용성을 제공하기 위해 정해진 정책과 절차에 따라 신속하게 데이터를 복구해야 한다.

2. ITU-T X.1601 기반의 보안 위협

SFCC는 클라우드 서비스 고객(cloud service customer, CSC), 클라우드 서비스 제공자(cloud service provider, CSP), 그리고 클라우드 서비스 파트너(cloud service partner, CSP)로 구분하여 클라우드 환경에서의 직접적인 보안 위협과 간접적인 보안 위협을 정의하는데 이를 통합적으로 분석하여, 표 2과 같이 21개의 보안 위협들 중 개인건강서비스와 연관된 14개의 보안 위협을 도출하였다.

데이터 손실과 유출(data loss and leakage)은 CSC에 대한 심각한 보안 위협으로 적절한 암호

Table2. Security threats and challenges of SFCC related to PHS(personal health service)

표 2. 개인건강서비스와 연관된 SFCC의 보안 위협

No	Threats and challenges of SFCC	PHS
1	Data loss and leakage	T
2	Insecure service access	T
3	Insider threat	
4	Unauthorized administration access	T
5	Ambiguity in responsibility	
6	Loss of trust	C
7	Loss of governance	C
8	Loss of privacy	C
9	Service unavailability	C
10	Cloud service provider lock-in	
11	Misappropriation of intellectual property	C
12	Loss of software integrity	C
13	Shared environment	C
14	Inconsistency and conflict of protection mechanisms	
15	Jurisdictional conflict	
16	Evolutionary risks	C
17	Bad migration and integration	C
18	Business discontinuity	C
19	Cloud service partner lock-in	
20	Supply chain vulnerability	
21	Software dependencies	C

관리가 요구된다. 불안전한 서비스 접근(insecure service access)은 클라우드 컴퓨팅의 분산된 환경에서 사용자(user) 또는 관리자(administrator)의 기밀(credentials)이 공격에 취약하므로 신뢰성 있는 접근 제어가 요구된다. CSP에 대한 공격이 후 CSC의 관리자 계정에 대해 비인가된 관리자 접근(unauthorized administration access)이 발생 가능하므로 적절한 권한 제어가 필요하다. 상기의 세 가지 보안 위협들은 직접적인 보안 위협들(threats)로 표 2의 PHS 열에 “T”로 구분하여 표기하였다.

CSC가 CSP의 보안 수준(level)을 획득하거나 공유하지 못할 경우, 신뢰의 손실(loss of trust)이 발생할 수 있으므로 적절한 보안 수준 제어의 제공이 요구된다. 그리고 관리의 손실(loss of governance)은 CSC의 데이터가 악의적인 공격에 대해 취약할 수 있으므로 CSC에 대한 심각한 보안 위협이 된다. 프라이버시 손실(loss of privacy)은 CSP가 CSC의 개인 정보를 처리할 때, 개인 정보의 유실 또는 CSC의 인가 없이 별도의 목적으로 개인정보를 처리할 수 있으므로 개인 정보에 대한 안전한 관리가 요구된다. 서비스 비가용성(service unavailability)은 동적으로 자원을 활용하는 클라우드 환경에서도 발생할 수 있으며 이를 위해 자원에 대한 적절한 유지 관리가 필요하다. CSC에 대한 지적재산권 남용(misappropriation of intellectual property)을 방지하기 위해, 엄격한 접근 및 권한 제어가 제공되어야 한다. CSC의 코드가 CSP에 의해 동작될 경우, 소프트웨어 무결성 손실(loss of software integrity)이 발생할 수 있으므로 소프트웨어에 대한 무결성이 보장되어야 한다. 가상화 기술을 이용하여 자원을 나누어 사용하는 공유된 환경(shared environment)에서 접근 및 권한 제어를 통해 할당된 자원을 안전하게 격리하고 관리해야 한다. 점진적 위험(evolutionary risks)은 시스템 설계 단계에 존재할 수 있으므로 동적으로 차츰 발전하는 시스템에 대한 동적인 보안 평가가 지속적으로 요구된다. 부적절한 이동 및 통합(bad migration and integration)을 방지하기 위해, 인터페이스의 호환성 및 일관된 보안 정책이 지속적으로 적용되어야 한다. 비즈니스 중단(business discontinuity)을 방지하기 위해 서비스 가용성이 보장되어야 한다. 보안 취약점이 감지되었을 때, 다른 소프트웨어와의 연계된 동작으로 인해 즉각적으로 업데이트할 수 없게 되는 소프트웨어 종속(software dependencies)이 발생할 수 있으므로 보안 수준 및 서비스 가용성에 대한 적절한 관리가 요구된다. 상기의 열한 가지 보안 위협들은 간접적인 보안 위협들(challenges)로 표 2의 PHS 열에 “C”로 구분하여 표기하였다.

III 개인건강서비스을 위한 보안 요구사항

클라우드 환경에서의 개인건강서비스는 2장에서 분석된 것과 같이, 가상화된 자원을 이용하는 클라우드 컴퓨팅에 대한 보안 요구사항과 보안 위협을 기반으로 개인건강서비스와 연관된 보안

요구사항을 추가적으로 고려해야 한다.

국내의 경우, 국가기관의 주도로 다양한 헬스케어 시스템 및 서비스 개발 사업이 진행되었고 보안과 연관되어 의료기관 중심의 의료서비스를 위한 개인건강정보 보호에 대한 기술적 보안사항이 단체표준으로 제정되었다[16]. 단체표준의 개인건강정보는 개인의료기록에 대한 것으로, 본 논문의 주요 관점인 개인건강기록 중심의 개인건강서비스에 중심을 두고 있지 않다. 즉, 국가기관이나 의료기관과 같이 적절한 보안정책을 적용하기 어려운 개인건강서비스에 대한 보안 요구사항에 대한 정의가 요구된다.

이에 본 장에서 단체표준의 내용을 분석하여 개인건강서비스에 필요한 보안요구사항을 도출하고 클라우드 환경의 보안 요구사항 사이의 연관관계를 파악하여 그 타당성을 제시한다.

1. 개인건강서비스의 보안 요구사항

단체표준에서 개인건강정보의 기술적 보안 요구사항은 네 가지(수집, 저장 및 관리 단계, 폐기 단계, 교류 단계, 그리고 침해사고 예방 및 대응)로 나누어 필수항목과 권고항목을 별도로 정하고 있다. 각각에 대해 분석한 후 개인건강서비스의 보안 요구사항으로 도출된 27개의 항목에 대한 개략적인 설명은 다음과 같다.

가. 수집, 저장 및 관리 단계

개인건강기록은 의료기관의 내부 및 외부의 측정단말을 포함하여 개인의 측정단말로부터 수집되고, 다양한 응용 서비스에 의해 저장 및 관리될 것이다. 이를 위해 다음과 같은 보안 요구사항들이 요구된다.

(1) 자산의 분류(asset classification)
- 필수 항목

정보자산을 업무특성 및 중요도에 따라 분류하고, 보안 수준에 대해 정의해야 한다.

(2) 권한 관리(authority management)
- 필수 항목

개인건강기록에 대한 접근 권한을 차별화하고 관리가 이뤄져야 한다.

(3) 계정 관리(account management)
- 필수 항목

접근권한 부여를 위해 유일한 식별을 위한 계정 관리가 이뤄져야 한다.

(4) 인증 관리(authentication management)
- 필수 항목

접근권한 부여를 위해 각각의 계정에 대한 인증 관리가 필요하다.

(5) 담당자 관리(administrator management)
- 필수 항목

담당자의 자격이 변경된 경우, 접근 권한 변경 또는 말소가 이뤄져야 한다.

(6) 패스워드 관리(password management)
-필수 항목

개인건강기록 취급자가 취약한 패스워드를 사용하지 않도록 패스워드 관리 지침을 마련하고 적용해야 한다.

(7) 보안 시스템(security system)
- 필수 항목

침입 탐지, 차단 및 방지를 위한 보안관련 시스템을 설치하고 운영 및 관리해야 한다.

(8) 접근 제어(access control)
- 필수 항목

개인건강기록은 별도의 접근 제어가 필요하며, 권한 관리도 연계하여 적용해야 한다.

(9) 저장장치 관리(storage management)
- 권고 항목

가상화된 저장장치에 분산 또는 중복 저장된 개인건강기록에 대한 관리가 요구된다.

(10) 소프트웨어 관리(software management)
- 권고 항목

허용된 응용프로그램을 이용해야만 개인건강기록에 접근할 수 있도록 제어하고, 접근 기록(log)을 저장하여 사후 추적이 가능하도록 해야 한다.

(11) 암호 통신(encrypted communication)
- 필수 항목

개인건강기록이 전송될 때, SSL(Secure Socket Layer), IPsec 등의 기술을 적용하여 통신구간 암호화를 적용해야 한다.

(12) 데이터 암호화(data encryption)
- 필수 항목

개인건강기록을 포함하여 중요한 데이터 및 개인정보들은 암호화하여 저장하고 관리해야 한다.

(13) 로그 관리(log management)
- 필수 항목

개인건강기록에 대한 접근 및 처리에 대한 로그 데이터를 기록하고 관리해야 한다.

(14) 로그 감시(log monitor)

- 권고 항목

문제점 파악을 위해 로그 데이터를 주기적으로 확인하고 감시해야 한다.

(15) 로그 데이터 백업(log backup)

- 필수 항목

로그 데이터는 정기적으로 백업하고 일정기간 동안 저장하고 관리해야 한다.

(16) 출력 정보 최소화(minimization of output information)

- 필수 항목

출력 용도를 특화하고 용도별 출력양식을 별도로 지정하여 접근권한에 따라 출력되는 정보를 최소화해야 한다.

(17) 출력 관리(output management)

- 권고 항목

개인건강기록의 출력 시, 출력과 관련된 정보를 기록하고 관리해야 한다.

나. 폐기 단계

클라우드 환경에서 개인건강기록은 가상화된 저장장치를 이용하여, 시간 및 장소의 제약 없이 효율적으로 저장되고 관리된다는 장점이 있으나, 원본과 사본의 파악이 힘들어 폐기를 위한 다음과 같은 요구사항들이 필요하다.

(1) 폐기 절차(deletion procedure)

- 필수 항목

개인건강기록에 대한 불법적인 복구가 불가능하도록 폐기 절차를 수립하고 적절하게 관리해야 한다.

(2) 보증된 폐기(assured deletion)

- 권고 항목

개인건강기록이 폐기될 경우, 가상화된 저장장치에 사본이 존재하지 않도록 완전히 폐기되었음이 보장되어야 한다.

다. 교류 단계

개인건강기록은 다양한 개인건강서비스를 위해 정보교류가 빈번하게 이뤄질 것이며 이를 위한 보안 요구사항은 다음과 같다.

(1) 서비스 수준 협약(service level agreement)

- 필수 항목

개인건강서비스를 위해 참여한 제공자 사이의 역할의 정의, 인증 절차 등의 합의와 문서화가 이뤄져야 한다.

(2) 보안 기술(security technology)

- 필수 항목

건강서비스 제공자 사이의 서비스 수준 협약에 따라 정보교류 시, 권한관리, 접근제어, 전송 보안 등 적절한 보안기술이 적용되어 안전한 교류를 보장해야 한다.

(3) 트랜잭션 감시(transaction monitor)

- 권고 항목

개인건강기록에 대한 교류가 발생한 경우, 트랜잭션에 대해 높은 수준의 보안 강도로 감시하고 필요한 경우, 로그를 저장하고 관리해야 한다.

라. 침해사고 예방 및 대응

개인건강서비스에 대한 가용성 제공을 위해 개인건강기록에 대한 침해 사고 예방과 대응이 필요하며 이를 위한 보안 요구사항은 다음과 같다.

(1) 사고 보고(accident report)

- 필수 항목

침해 규모를 단계별로 정의하고, 사고 발생 규모에 따른 적절한 보고 체계를 수립하고 대응해야 한다.

(2) 사고 대응(accident countermeasure)

- 필수 항목

사고 발생 시 피해를 최소화하기 위한 대응체계를 구축하고 적용해야 한다.

(3) 사고 감시(accident monitor)

- 필수 항목

보안 시스템을 활용하여 불법적인 조회 또는 접근이 발생하는지를 지속적으로 감시해야 한다.

(4) 취약점 진단(vulnerability diagnosis)

- 필수 항목

침해방지를 위해 시스템의 취약점에 대해 주기적인 진단을 수행해야 한다.

(5) 갱신 관리(update management)

- 필수 항목

침해사고를 방지하기 위해 보안관련 시스템 및 소프트웨어를 설치하고 주기적으로 갱신하여 최신 상태를 유지해야 한다.

Table 3. Relation between security requirements of cloud environment and PHS

표 3. 클라우드 환경의 보안 요구사항과 개인건강서비스의 보안 요구사항 사이의 관계

security requirements	
cloud	PHS
cryptographic technology	service level agreement security technology
data encrypt/decrypt	storage management data encryption
key management	authentication management storage management data encryption
data transmission	encrypted communication data encryption
authentication management	authentication management administrator management password management
account management	account management administrator management password management
access control	asset classification authority management access control Min. of output information
authority control	asset classification authority management administrator management Min. of output information output management
session management	encrypted communication transaction monitor
authentication code management	access control storage management deletion procedure assured deletion
software integrity	access control software management
data integrity	access control storage management deletion procedure assured deletion
accident monitoring	security system log monitor accident report accident monitor vulnerability diagnosis update management
data backup	storage management log management log backup
data recovery	storage management accident countermeasure

2. 개인건강서비스의 보안 요구사항과 클라우드 환경의 보안 요구사항의 연관성

본 논문에서 제안된 개인건강서비스의 보안 요구사항이 타당함을 검증하기 위해, 2.1절에서 서술된 클라우드 환경의 보안 요구사항과 제안된 개인건강서비스의 보안 요구사항 사이의 관계를 제시하고 이를 기반으로 제안된 개인건강서비스의 보안 요구사항이 클라우드 환경의 보안 요구사항을 모두 지원 가능함을 검증한다. 표 3은 클라우드 환경의 보안 요구사항과 개인건강서비스의 보안 요구사항 사이의 관계를 나타낸다.

표 3에 나타난 것과 같이, 클라우드 환경의 보안 요구사항은 2개 이상의 개인건강서비스의 보안 요구사항들과 연관되어 있으며, 개인건강서비스의 보안 요구사항들을 조합하여 보안관점에서 안전한 개인건강서비스가 제공될 수 있다. 따라서 본 논문에서 제안된 개인건강서비스의 보안 요구사항은 클라우드 환경에서 제공되는 개인건강기록 중심의 다양한 개인건강서비스들을 안전하게 관리하는데 적합하다.

Ⅳ 결론

본 논문은 소비자 중심의 다양한 개인건강서비스로 인해, 보안적인 측면에서 개인의료기록에 비해 훨씬 취약할 것으로 예상되는 개인건강기록 중심의 개인건강서비스 보안에 대해 연구하여, 클라우드 컴퓨팅 환경에서의 보안 위협으로부터 개인건강서비스 및 개인건강기록을 안전하게 보호하기 위한 것이다. 이를 위해, 우선적으로 클라우드 환경에서의 보안 요구사항과 보안 위협에 대해 개인건강서비스의 보안 관점에서 분석하였다. 그리고 의료서비스를 위한 개인의 전자의료정보의 보안 요구사항을 분석하여 개인건강서비스에 대한 보안 요구사항을 도출하여 제안하고 그 타당성을 검증하였다. 본 논문에서 제안된 개인건강서비스 보안 요구사항을 참고하여 다양한 개인건강서비스들이 개발되고 제공될 경우, 개인의 건강기록 및 사생활 정보가 안전하게 보호될 것으로 기대한다.

References

[1] Population Ageing: “1950-2050”, UN, http://www.un.org
[2] Health Informatics-Personal Health Device Communication, ISO/IEEE 11073. Available: http://standards.ieee.org
[3] Health Informatics-Personal Health Device Communication Part 20601: Application Profile-Optimized Exchange Protocol. ISO/IEEE Std. 11073-20601-2008
[4] Health Informatics-Personal Health Device Communication Part 20601: Application Profile-Optimized Exchange Protocol Amendment 1. ISO/IEEE Std. 11073-20601a-2010
[5] Health Informatics-Personal Health Device Communication Part 10415: Device Specialization - Weighing Scale. ISO/IEEE Std. 11073-10415-2010
[6] Health Informatics-Personal Health Device Communication Part 10408: Device Specialization - Thermometer. ISO/IEEE Std. 11073-10408-2010
[7] Health Informatics-Personal Health Device Communication Part 10407: Device Specialization - Blood Pressure Monitor. ISO/IEEE Std. 11073-10407-2010
[8] Health Informatics-Personal Health Device Communication Part 10417: Device Specialization - Glucose Meter. ISO/IEEE Std. 11073-10417-2010
[9] Health Informatics-Personal Health Device Communication Part 10406: Device Specialization - Basic Electrocardiograph. ISO/IEEE Std. 11073-10406-2011
[10] Health Informatics-Personal Health Device Communication Part 10471: Device Specialization - Independent Living Activity Hub. ISO/IEEE Std. 11073-10471-2008
[11] Continua Health Alliance. Available: http://www.continuaalliance.org
[12] “Information technology-Cloud computing-Reference architecture,” Recommendation ITU-T Y.3502, 2014
[13] “Security framework for cloud computing,” Recommendation ITU-T X.1601, 2014
[14] Chanwoo Lee, Sangkon Kim, Youngmin Yeo, Jongsub Moon, “Proposal of Security Requirements based on Layers and Roles for the Standardization of Cloud Computing Security Technology,” *Journal of Security Engineering*, Vol.10, No. 4, pp. 473-488, 2013
[15] Youngmin Yeo, Chanwoo Lee, Jongsub Moon, “Proposal of Security Requirements for the Cloud Storage Virtualization System,” *Journal of The Korea Institute of Information Security & Cryptology*, Vol.23, No.6, pp.1247-1257, 2013
[16] “Technical Privacy and Security Requirement for Personal Health Record,”, TTA, TTAK.KO - 10.0304, 2008

BIOGRAPHY

Sang-Kon Kim (Member)

2008 : PhD degree in Electrical and Computer Engineering, Seoul National University.
2008~2015 : Lecturer of Electronics and Information Engineering, Korea University.
2015~ : Assistant Professor of Dept. of Cyber Security, Ajou University

Hee-Joung Hwang (Member)

2000 : MS degree in Computer Science and Engineering, Inha University.
2008 : PhD degree in Computer Science and Engineering, Incheon University.
2000~ : Associate Professor of Dept. of Computer Engineering, Gachon University.