정 보 보 호 학 회 지
제24권 제6호, 2014. 12

클라우드 환경에서의 사이버물리시스템 관점에서 본 헬스 케어 보안 관련 이슈들

이 혜 림*, 조 재 연**, 윤 지 원***

요 약

사이버 물리 시스템(Cyber physical system, CPS)은 사물인터넷(IoT)과 달리 네트워크로 이루어진 물리적 장치들 간의 제어 및 통제를 포함하는 관리 시스템이다. 사이버물리시스템의 대표적인 사례인 헬스 케어 시스템은 시스템 내에서 다뤄지는 의료정보라는 데이터의 특별한 성격으로 인하여 데이터의 저장에서 관리까지 여러 가지 보안 위협들이 존재한다. 본 논문에서는 사이버 물리 시스템으로서의 헬스 케어 시스템이 클라우드 환경으로 이루어졌을 때 어떤 위협들이 존재하며 이러한 위협들이 어떻게 분류될 수 있는지, 또한 위협을 방지하기 위해 국내외 어떤 기술 및 표준화 노력들이 있었는지 알아보고자 한다.

Ⅰ. 서 론

IT기술의 발전은 정보혁명이라는 이름하에 인터넷의 발전과 함께 여러 전자제품들의 고도화에 힘입어 사회 전반으로 확대되고 있다. 이러한 기술적 변화는 우리의 삶의 스타일과 형태까지도 바꾸고 있으며 정치·사회·문화의 영역에까지 닿고 있다. 본 논문에서는 특히 이 정보혁명에 의해서 가장 많은 변화를 보이고 있는 헬스 케어 분야에 대한 내용을 기술한다. 본 논문의 제목은 크게 세 가지 단어들의 조합으로 만들어졌다. 즉 “클라우드 컴퓨터”, “Cyber Physical System (CPS)”, “Healthcare”는 2014년 현재 산업계와 학계 이외에도 정치와 사회 다방면에서 부각되고 있는 단어들이다. 우선 CPS의 개념은 좀 더 명확히 정의하면 사물인터넷(Internet of Things, IoT)의 개념과 차이가 있으나, 단순하게 유사한 개념이라고 이해하고 넘어가도 큰 무리는 없다. 클라우드 컴퓨터라는 단어는 최근 정보통신기술 사회의 큰 충격을 안겨준 BigData와 관련이 있다는 점에서 의미가 있어 위와 같은 제목으로 본 논문을 작성하고자 한다. 먼저 본 논문은 특정 기술에 대한 논문은 아니라는 점을 밝히고 싶다. 대신 사이버물리시스템 관점에서 헬스 케어 분야가 과거에 어떤 연구와 투자가 이루어졌으며 현재 기술 발전 및 보안 현황, 미래의 발전 방향에 대한 동향 및 자신들의 의견을 기술한 리뷰 논문과 유사하다고 볼 수 있다. 특히, 혹자들은 몇 년 전부터 해외에서 조금씩 이슈화되고 있는 사이버 물리 시스템 (CPS)이 2015년부터 IoT와 BigData의 뒤를 이어 국내의 새로운 연구 주제가 될 것이라고 믿고 있다. 그러므로 이 논문을 읽는 독자들은 헬스 케어 시스템이라는 영역으로 새롭게 시작된 사이버물리 시스템에 대한 보안 이슈를 접하고 이에 대한 차후 연구 방향 및 발전 방향을 고려하는 데 도움이 되길 바란다.

이 논문은 제 2장에서 간단한 배경지식을 다룬다. 클라우드 컴퓨터와 사이버물리시스템 그리고 헬스 케어 시스템에 대한 간단한 설명이 본 장에서 이루어진다. 제 3장에서는 사이버 물리 시스템 관점으로 본 헬스 케어 시스템의 여러 보안 문제를 언급한다. 이 장에서는 과거에 발생한 보안침해사례들을 언급하고 각 사례들을 분류표에 기반하여 나눈다. 또한 현재 국내외 헬스 케어 보안과 관련한 표준화동향도 포함하고 있으며 앞으로 헬스 케어 시스템 보안을 위해서 어떤 연구와 노력들이 필요한지에 대한 언급으로 해당 장을 마친다. 결론을 맺

* 고려대학교 정보보호대학원 석사과정생 (dream8933@naver.com)
** 고려대학교 정보보호대학원 석사과정생 (sjjy811@korea.ac.kr)
*** 고려대학교 정보보호대학원 교수 (jiwon_yoon@korea.ac.kr, 교신저자)

기 전에 토론을 위한 장을 따로 두었다. 이 장에서 저자들은 헬스 케어 시스템을 단순한 의료행위를 넘어 생명공학분야로의 확대해석의 필요성을 언급하고자 한다.

Ⅱ. Background (배경지식)

2.1. 클라우드 컴퓨터 (Cloud computer)

2006년 9월 구글 전 CEO 에릭 슈미츠와 크리스토프 비시글리아 직원의 사내 회의에서 클라우드 컴퓨팅(Cloud Computing) 개념이 제안되었다. 이름에서 알 수 있듯이 가상의 구름을 만들어서 이용하자는 개념이다. 클라우드 컴퓨팅은 새로운 기술이라기보다 기존에 존재하는 분산컴퓨팅, 유틸리티 컴퓨팅, 웹서비스, 서버 및 스토리지의 가상화 기술, 공개 소프트웨어 등과 같은 기술들을 통합하여 하나의 거대한 가상 구름과 같은 컴퓨팅 환경을 구축하는 것을 말한다. 즉 물리적으로 분리되어 존재하는 컴퓨팅 자원을 가상화 기술을 이용하여 하나의 거대한 자원으로 만들어서 제공하는 기술이다.

클라우드 컴퓨팅이 IT산업에서 각광받는 이유는 무엇보다도 IT자원을 서로 공유하고 유휴자원을 효율적으로 활용하여 시스템이나 제품 생산에 있어서의 비용절감이라는 큰 이점을 얻을 수 있다는 점일 것이다. 하지만 이러한 비용절감 뿐만 아니라, 다른 영역에서도 그 유용성을 찾을 수 있다. 예를 들어, 컴퓨터의 효율적인 사용을 통한 전원사용률 감소, 이를 통해 얻게 되는 에너지 절약을 들 수 있으며, 불필요한 장비 사용을 방지함으로 데이터 센터 공간을 줄일 수 있다.

2.2. Cyber Physical System

전자 및 정보통신기술들이 발전함에 따라 전자기기들은 여러 가지 주목할 만한 변화를 얻게 되었다. 그 첫 번째 변화는 연산 및 통신 속도의 향상이다. 과거에 시간이 오래 걸려서 연산이 어려웠던 많은 문제들이 CPU의 연산속도 향상으로 그 문제들이 해결되었으며 향상된 연산 속도의 향상은 다중 CPU 및 GPU (Graphical Processing Unit) 시스템의 도입으로 가속화되었다. 또한 컴퓨터 내부 연산장치의 고속화와 함께 통신 속도도 함께 향상되었다. 단말기뿐만 아니라 ISP가 관리하는 라우터(Router)의 회선 증가를 통해서 병목현상이 감소되었으며 통신 장비의 입출력 채널의 알고리즘 개선을 통해 속도 향상이 이루어지고 있다. 또 다른 변화는 장비의 소형화다. 각 물리적 장비의 집적화를 통하여 소형화를 이룰 수 있었다. 이러한 장비의 물리적 소형화는 공간적 활용도를 높임과 동시에 기업에서 가장 중요시하는 저전력(low power) 이점을 얻을 수 있다.

이러한 변화들로 물리적 환경에서 별도로 존재하던 많은 물리적 장비들이 우리의 주변에 장착이 되기 시작했다. 이와 함께 사물인터넷(Internet of Things)이라는 기술과 접목되어 물리적 장치들로부터 유입되는 대량의 정보 수집이 가능해졌고 이를 분석하기 위한 빅데이타 분석(BigData Analysis)기술이 핵심 기술로 대두되었다. 하지만 이제 빅데이타 분석기술과 사물인터넷을 뛰어넘는 개념이 도래했는데, 그것이 바로 사이버물리시스템(Cyber Physical System, CPS)이다. 비록 전문가들에게도 IoT와 CPS에 대한 구분이 여전히 모호해 보이며 CPS에 대한 명쾌한 정의가 아직 만들어지지 않았지만 CPS는 IoT와 달리 소형화 및 고성능화된 장비들을 통제하고 관리하는 관점까지 포함하는 개념이다. 즉 IoT 는 장비들의 소형화를 통한 탑재화에 초점을 두었고 임베디드 시스템(Embedded system)이 인터넷처럼 퍼질 수 있다는 점이 IoT의 핵심이며 CPS는 IoT에 의한 단순한 물리적 변화뿐만 아니라 통제 및 관리를 포함하여 정보적인 측면까지 고려하는 시스템이라는 점에서 그 차이점을 찾을 수 있다. 이것은 CPS는 IoT 개념에 BigData 분석 기술이 추가되어 관리 및 제어가 포함된 개념이라고 재해석 가능하다. 분명히 이러한 주장에는 이견이 있겠지만, 본 논문에서 IoT는 CPS로의 과도기적 개념이라고 말할 수 있다.

2.3. Healthcare

사물인터넷 및 사이버물리시스템의 확대는 그 어느 분야보다도 헬스 케어 분야에서 가장 활발하게 이루어지고 있다. 헬스 케어에 대한 이러한 변화는 초기에 물리적으로 여러 장소에 다양한 종류로 분산으로 관리되던 환자의 의료정보들을 한 곳에 모으는 일종의 데이터 버이스화 작업에서 시작되었다. 이러한 통합데이터베이스 작업은 기존의 의료산업이 제공하지 못하던 많은 이점을 제공했다. 예를 들어 환자정보의 검색속도의 향상이라는 단순한 이점뿐만 아니라, 의료보험 관리체계 향

상, 환자들과 질병에 대한 지속적 관리 및 체계적 분석이 가능해졌다. 그런데 이러한 데이터베이스화는 두 가지 관점에서 여전히 그 한계가 존재한다. 첫째는 의사나 의료산업관계자들 관점이고 다른 하나는 환자들의 관점이다. 즉, 단순한 데이터베이스를 넘어서는 기술향상의 요구가 두 가지 다른 방향에서 만들어졌기에 기술들 역시 두 가지 다른 방향으로 발전하고 있다고 말할 수 있다. 우선, 의사나 의료산업관계자들의 관점을 놓고 보면 아래와 같은 현상들이 중요한 점으로 부각되었다.

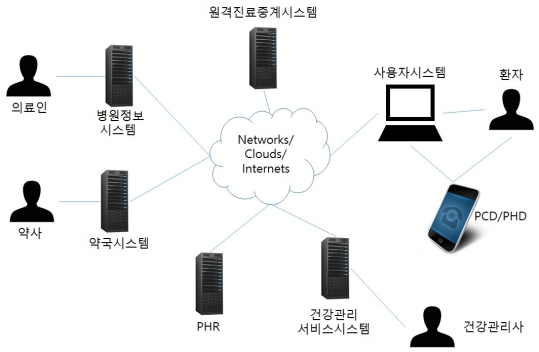
- 다른 의료기관들 간의 환자정보 및 의료기술 데이터 통합화를 통한 정보 공유 및 협력방안
- 여러 고성능 장비들의 계측 값의 정확한 연산 및 사용을 통한 진료시스템의 정확도 향상
- 양질의 의료서비스 창출 및 제공
- 생체 계측 데이터와 같은 대용량 데이터에 대한 효율적 관리를 위한 정책 및 기술 필요
- 원격진로를 통한 보건의료의 확대

이와 함께 환자와 같은 고객을 위한 방향으로도 아래와 같이 동시에 발전하고 있다.

- 본인의 건강기록을 환자의 요청시 언제든지 어디서나 확인 가능케 함
- 환자가 자신의 건강상태를 측정하고 활용할 수 있는 서비스 제공
- 원격진로를 이용 의료서비스 사용의 편이성 향상

이와 같이 두 집단의 요청이 현재 헬스 케어 산업의 방향을 만들어냈다고 볼 수 있다. 이러한 요구들을 만족시키는데 가장 효율적으로 작동하는 기술이 바로 헬스 케어 관련 지능형 전산화 기술들이며 이것은 우리에게 이제는 익숙한 Cloud computing, BigData, IoT, CPS를 통해서 가능해졌다.

[그림 1]은 국가기술 표준원에서 헬스 케어 시스템의 하나인 스마트의료정보에 대한 관계도이다 [7]. 이 그림에서 볼 수 있듯이, 의료인(의사, 약사)은 고객인 환자들과 네트워크 환경으로 연결되어 있다. 이 네트워크는 인터넷이 될 수 도 있고, 클라우드 환경이 될 수도 있다. 이렇게 의료인들은 각자의 병원정보시스템이나 약국시스템을 통해 그 네트워크에 연결이 되며 그 네트워크에



출처: 표준기반 R&D 로드맵 스마트의료정보, 국가기술표준원, 한국표준협회, 2014

〔그림 1〕 스마트의료정보 유헬스 서비스 액터 인터렉션 관계도

환자가 접속함으로서 원격진로와 같은 헬스 케어 시스템의 서비스를 받을 수 있다. 그런데 이 그림을 좀 더 자세히 살펴보면 몇 가지 중요한 사항들을 찾을 수 있다.

- 의료인: 단순한 원격진료라면 이것은 의사가 의료인의 주체가 될 것이다. 하지만 CPS환경에서는 의료인의 주체는 사람만이 아니며, 주체는 환자의 입원부터 퇴원, 그리고 그 이후 외래진료과정에서의 모든 센서와 의료장비로부터 얻어진 계측값들이 될 수 있다. 즉, CPS상의 헬스 케어 시스템은 단순히 의료인의 진료를 넘어서 센서와 의료장비를 통한 대용량의 데이터를 클라우드에 저장 및 관리하고 이를 처리·분석하는 기술까지 탑재하여야 한다.
- PHR: Personal Health Record의 약자로서 소비자(환자)의 개인건강 기록을 저장하고, 본인의 건강 기록을 조회할 수 있도록 지원하는 서비스 시스템이다. [그림 1]에서는 PHR 시스템이 네트워크 외부에 존재하는 것으로 그려졌으나, 이 서비스 역시 Cloud 환경에서 저장·관리가 가능하다.
- PCD / PHD: Patient Care Device와 Personal Healthcare Device의 약자로서 소비자가 자신의 건강상태를 측정하기 위해서 활용하는 장치이다. 이 시스템은 최종 사용자인 환자에게 정제된 정보를 제공함과 동시에 환자로부터 직접 얻는 피드백을 받아서 클라우드 환경으로 재전송할 수 있는 시스템이다.
- 건강관리사: 병원과 약국과 달리 진료보다는 고객의 외래진료나 보건자체를 책임지고 도와주는 시스템으로서 이들 역시 사람이 주체가 될 수도 있고 건강

관리 시스템이 여러 가지 센서들을 이용해서 환자들의 상태를 실시간으로 측정하여 대용량 정보를 건강관리 서비스를 통해서 클라우드에 제공 가능하며 클라우드나 건강관리서비스 시스템에서 직접 환자의 건강상태에 대한 정보를 추출할 수 있게 된다.

Ⅲ. Healthcare Security in Cyber Physical Systems

[그림 1]에서 볼 수 있듯이, 헬스 케어 시스템은 네트워크나 클라우드 환경에서 여러 가지 시스템들이 통합된 환경이며 이러한 환경을 제어하고 관리할 수 있는 시스템이 바로 헬스 케어상의 사이버물리시스템(CPS)이다. 지금까지는 의료진, 약사, 건강관리사, 환자들의 편의성과 효율성만을 위하는 스마트의료정보시스템인 CPS 관리 시스템 개발에만 초점을 맞추었다. 하지만 오로지 효율성에만 초점을 맞추어 개발을 하다 보니, 상대적으로 헬스 케어와 관련된 CPS의 보안성에 대한 관심은 적었다. 헬스 케어는 개인의 의료 정보를 다루기 때문에 CPS의 다른 어떤 분야들보다도 보안성에 대한 기술적 연구와 정책수립이 절실히 필요하다. 예를 들어, 의료진의 컴퓨터가 해킹을 당하면 의료진과 연결된 병원정보 시스템이 해커에게 노출이 되며, 환자들의 병명, 주민번호와 같이 여러 치명적인 개인정보가 허가받지 않은 외부인에게 노출될 수 있다. 일례로, 2014년 10월 국내에서 의료용 공인인증서가 유출되는 사고가 있었다. 이 사고는 국내에서 처음으로 공식적으로 확인된 해킹에 의한 의료정보 유출사건이었으며, 국내 환자들의 진료기록, 처방목록, MRI 촬영화면 등의 의료정보와 의약업체 판매 현황까지 홍콩에 위치한 서버에 수집되었다는 점에서 그 위험성이 매우 높았다. 또한 다수의 의료기관 내의 PC가 악성코드에 감염된 것으로 파악되었고, 하나의 서버가 약 2000대의 PC를 동시에 제어가 능하기 때문에 대규모의 정보유출의 위험성이 밝혀졌다.

헬스 케어 시스템 보안과 관련된 많은 국내외 연구는 관리적 측면[1,3]에서의 연구와 기술적 측면[4]에서의 연구로 나뉘어져 왔다. 국내에서 IoT 관련 정보보호 로드맵과 스마트 헬스 케어에 대한 관리적 측면의 정책 문서들이 최근 발행되고 있다[7,8]. 특히 기술적인 측면에서의 연구는 무결성, 기밀성, 가용성, 익명성, 무연결성 등에 기반하여 이루어졌다. 이에 따라 Privacy-Preserving Approaches(PPA)가 많이 연구되었으며 공개키 암호, 비밀키 암호와 Attribute based encryption(특징 기반 암호), Homomorphic encryption(동형암호) 등의 암호 기술들과 함께 비암호 기술들도 연구되어 왔다.

이에 앞서 [그림 1]에서 보이는 헬스 케어 시스템에서 어떤 보안위협이 있을 수 있는지를 알아볼 필요가 있다. 어떤 위협이 헬스 케어 시스템에 존재할 수 있는지를 알아보기 위해서는 크게 두 가지 관점에서 분석이 필요하다. 첫째는 공격당할 수 있는 희생 대상을 중심으로 조사하는 것이다. 즉, 희생대상을 중심으로 볼 때 크게 환자, 의료용PC나 스마트폰, 그리고 의료DB 이렇게 세 가지로 구분시킬 수 있다. 또 다른 관점은 위협의 목적에 따른 분류이다. 가장 대표적인 헬스 케어 시스템에서의 보안 위협은 정보 유출이다. 해커가 환자의 정보를 환자가 갖고 있는 센서들로부터 직접 얻을 수도 있고 또는 환자가 의료서비스와 접하게 되는 컴퓨터 환경을 직접 공격하여 정보를 유출할 수 있다. 물론 해커가 직접 의사의 컴퓨터나 병원 내 시스템을 공격하여 소기의 목적인 중요 정보를 유출할 수 있다. 또 다른 보안위협의 목적은 정보유출이 아닌 의료시스템의 오작동을 유도하는 것이다. 이렇게 여러가지 요인에 기반해 공격유형을 구분하여야 방어 전략에 대해서도 좀 더 치밀하며 긴밀하게 대처할 수 있다. [그림 2]는 이러한 방식에 따른 헬스 케어 시스템을 분류한 분류표이며 우리는 기존에 발생했었던 보안침해사례들을 위 분류표에 따라서 6가지 시나리오로 구분한다.

〔그림 2〕 헬스 케어 시스템의 보안위협에 대한 분류

3.1. Healthcare Security 의 과거

최근에 의료정보화 과정을 거치면서 국내외로 여러 가지의 중요 보안침해사고가 발생했다.

예를 들어, 2014년 10월에 해킹에 의한 국내의 의료정보유출 사고가 발생했다. 특히, 이 사건은 국내에서 공식적으로 확인된 해킹에 의한 의료정보 유출사건이라는 점에서 중요성을 갖는다. 이 침해사고로 인해, 진료기록, 처방목록, MRI 촬영화면 등의 의료정보와 의약업체 판매현황을 포함하는 국내 병원환자들의 의료정보가 홍콩에 위치한 서버에 수집되었으며, 다수의 의료기관내의 PC가 악성코드에 감염된 것으로 파악되며 해당 서버가 최대 2000대의 PC를 동시에 제어할 수 있기 때문에 대규모의 정보 유출 위험성이 존재하는 헬스 케어 시스템의 보안 사고였다. 이외에도 Healthcare 보안과 관련하여 최근에 발생된 여러 가지의 침해사고 사례들이 국내외에 발생하였으며, 이들을 [표 1]에 간략하게 정리하였다.

3.2. Healthcare Security 의 현재

현재 헬스 케어 시스템 보안과 관련하여 어떤 준비와 투자가 이루어지고 있는지를 알기 위해서 보안 표준화 동향을 알아보았다. 현재, 표준화 동향을 보자면, 크게 키관리, 접근제어, 헬스 케어 기기간 통신 규약, 기기내 통신규약 및 데이터 형식 및 저장에 걸쳐 넓게 개인정보 및 기밀성을 만족시키는 방향으로 여러 노력들이 이루어지고 있다. [표 2]는 이러한 헬스 케어 시스템과 관련된 표준문서들의 간단한 기술과 이에 해당하는 표준화문서 번호들이다.

3.3. Healthcare Security의 미래

Healthcare 시스템들의 미래는 현재진행중인 클라우드 컴퓨터이다. 그런 의미에서 Healthcare security역시 클라우드 컴퓨팅 보안이라고 말할 수 있다. 특히, Cyber physical system과 사물인터넷(IoT)으로 인해서 폭증하는 의생명 데이터들을 더 이상 기업이나, 공공기관, 병원 및 개인이 개별적으로 저장 및 관리하는 것은 어려워지는 환경이 도래했다. 이런 의미에서 클라우드 컴퓨팅 환경은 너무나도 자명한 미래의 모습이다. 그런데 여기서 중요한 부분은, 클라우드 컴퓨팅 환경이 가능해지려면 보안이라는 이슈가 해결되어야 한다는 점이다. 이런 점에서 대량의 데이터들을 어떻게 저장, 관리하느냐가 관건이며 여러 가지 관리 기법들의 다각적인 연구와

〔표 1〕 국내외 Healthcare 시스템들의 보안 침해 사고들, 〔그림 2〕의 S: 위협 시나리오 ($S \in \{1,2,3,4,5,6\}$)

Event	Date	Reason	Description	S
보스턴 BIDMC병원 데이터 유출 - 1	2011.07.	악성코드 감염	2021명의 환자기록(이름, 성별, 생년월일, 의료기록번호, 방사선 치료 날짜)이 인터넷으로 유출	3/5
보스턴 BIDMC병원 데이터 유출 - 2	2012.07.	전문의 Laptop 도난	Laptop내 데이터 암호화 부재와 도난으로 인해 3900명의 환자 기록 탈취	5
미국 Froedtert 병원 환자 개인정보 유출	2013.02.	바이러스 감염	43,000명의 환자 중 일부의 사회보장번호가 유출	5
The Surgeons of Lake Country 해킹 및 데이터 인질극	2012.06	해커 침입 후 Data Ransom	일리노이 주 의료기관 시스템에 해커 진입 후 데이터를 암호화한 후 패스워드에 대한 대가 요구	6
국내 의료뉴스 웹사이트를 통한 악성코드 유포	2013.08	악성코드 유포	의료용 인증서, 개인용 인증서, 의료정보 기록에 접근토록 하는 EMR인증서 유출	5
대형병원 임상실험센터웹사이트	2014.04	해킹 및 악성코드 유포	국내 대형병원의 임상실험센터의 웹사이트가 해킹되어 악성코드 유포지로 악용됨	5
인공 심장박동기/인공심장 해킹 취약성	2008.05	해킹에 의한 인공심장 오작동	인공심박동기/인공심장을 해킹하여 기기 오작동 가능하다는 연구논문이 발표	2
인슐린펌프 무선기능 취약성	2011	무선기능 취약성 공격	인슐린 펌프의 무선 기능 취약성을 통해 인슐린 펌프의 오작동 유도	2
생화학 자동분석장치 소프트웨어	2013.01	생화학 자동 분석장치에 연결된 DB해킹	COBAS ITEGRA 400 plus 분석기에서 사용하는 오라클의 데이터베이스의 취약점을 이용하여 원격으로 잘못된 정보를 DB에 저장가능	4
네트워크 접속형 의료기기, 모바일기기	2013.06	악성코드 감염	낡은 의료기기의 취약성에 대한 대처가 미비하여 모니터링 시스템 내 악성코드 감염됨.	5

〔표 2〕 국내외 헬스 케어 관련 표준화 동향

Contents	IDs
헬스 케어 PKI 관련 표준화 (digital certificate, 인증서 종류 및 암호화 관련)	ISO 17909-1:2013 ISO 17909-2:2008 ISO 17909-3:2008 ISO 17909-4:2014
권한 관리 및 접근제어 관련 표준화	ISO 22600-1:2014 ISO 22600-2:2014
의료영상장비의 표준화 (데이터 표현과 통신을 위한 표준 기술) - DICOM[1)]	ISO 12052-2006
독립된 시스템간의 정보처리 상호 운용성 및 호환성을 제공하기 위한 의료정보통신기술의 표준화 (CEN/TC 251)	ISO/TS14265:2011 ISO/TS14441:2013 (WG3가 보안 부분담당)
환자의 특정 정보를 사용하는 헬스 케어 시스템 내 데이터 구조, 저장, 보안, 기밀성, 기능성, 정보교환 등에 대한 표준화	E1239-04,E1340-05, E1384-07,E1633-08a,E1714-07,E1869-04 등 다수 (ASTM Committee E31에 의해 주도)
HL7메시지가 라우터 중계를 통한 보안위협을 분류하고 보안 서비스 요구사항 기술	HL7

투자가 필요하다.

예를 들어 클라우드 컴퓨팅 환경에서 헬스 케어 시스템이 운영 중이라면 아래와 같은 클라우드 컴퓨팅 환경에서의 보안에 대한 조건[1-3]을 만족할 필요가 있다.

① 인증 및 접근제어에 있어서 물리적인 접근통제뿐만 아니라, 식별 및 관리에 보안 필요
② 연산 자원의 공유를 통한 보안이슈가 필요
③ 가상화를 통해서 개체들로부터 받아들여지는 위협에 대한 준비가 필요
④ 분산컴퓨팅 시스템으로부터 일어날 수 있는 시스템 충돌 및 데이터 손상 등의 위협 대처 필요
⑤ 인터넷을 통한 모바일 접근에 대한 보안 문제 대처가 필요하다. 예를 들어, 스마트폰을 통한 정보 유출 및 개인정보 손상 이슈에 대한 대비가 필요
⑥ 언제든지 시스템을 빠르고 쉽게 교체 가능해야 함.
⑦ 대용량의 데이터들을 효율적으로 관리하면서 이들에 대한 Privacy preserving 성질을 만족하는 보안기술이 필요

1) DICOM (Digital Imaging and Communication in Medicine)은 의료영상 장비의 표준화를 위해 미국 방사선의학회(ACR)와 미국전기공업회(NEMA)가 1993년 첫 데모버전을 보임.

Ⅳ. 토 론

제 3장까지 우리는 헬스 케어 시스템을 중점으로 다루면서 의료정보에 초점을 맞추었다. 하지만, 사실 헬스 케어 시스템은 의료정보뿐만 아니라, 생물학 정보[6] 시스템까지도 포함할 수 있다. 게놈 프로젝트(Genome project)라는 생명정보학의 발전과 유전학 및 분재생물학 그리고 의료영상기술[5]의 발전은 의생명 데이터들의 폭발적 증가를 갖고 왔다. 생물학 발전의 일례로 한 사람의 DNA 서열을 모두 알아내고 그 서열을 통해서 그 사람의 잠재적 병명이나 유전적 결함 등을 알아내는 것이 가능해졌으며 분석 속도 또한 과거 1년이 넘게 걸리던 기술들이 이제는 단 몇 시간 안에 가능해졌다. 이러한 기술적 향상은 대학이나 연구소에서의 제한된 영역를 벗어나 이제는 산업시장으로 그 범위를 넓히고 있으며 자연스레 클라우드 컴퓨팅 환경으로 발은 넓히고 있다. 이 정보들은 본 논문에서 언급하던 환자정보들만큼이나 중요한 정보들을 갖고 있기때문에 생명정보학이 헬스 케어 시스템에 포함된다면 이는 우리가 중요하게 바라보고 접근해야 할 대상임이 분명하다. 또한 이러한 데이터들이 학문영역을 넘어서 자본시장으로 넘어감에 따라서 일종의 서비스 산업으로의 재탄생이 가능해졌다. 의생명 산업 역시 머지않아 사이버물리시스템으로 해석이 가능해질 것이며 우리는 이에 따라 보안 위협들을 하나씩 따져볼 필요가 있다.

Ⅴ. 결 론

본 논문에서 클라우드 환경에서 관리되고 있는 헬스 케어 시스템들을 사이버 물리 시스템 (Cyber Physical System, CPS)이라는 관점에서 바라보고 어떠한 보안위협이 있어왔고 그러한 위협은 어떻게 분류가 가능하며 어떤 기술들과 표준화가 이루어지고 있는지를 살펴보았다. 특히 사이버 물리 시스템에서 헬스 케어 시스템은 단순히 데이터를 안전하게 저장하는 것 뿐 아니라 안전하게 통제하고 제어하는 단계에서의 안전까지 고려하고 있었다. 앞으로도 헬스 케어 시스템이 사람의 생명과 직결되는 시스템인 만큼 또 의료정보라는 예민한 데이터를 다루는 시스템인 만큼 보안의 전체적인 그림부터 세

부적인 사항까지 고려되어져야 한다는 주장과 함께 이 논문을 마무리한다.

참 고 문 헌

[1] R. Colomo-Palacios, E. Fernandes, M. Sabbagh, and A. de Amescua Seco, “Human and intellectual capital management in the cloud: software vendor perspective”, The journal of Universal Computer Science, vol. 18, no. 11, pp. 1544-1557, 2012

[2] H. Takabi, J. B. D. Joshi, and G. J. Ahn, “Security and privacy challenges in cloud computing environments”, IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, 2010.

[3] K. Haufe, S. Dzombeta, and K. Brandis, “Proposal for a security management in cloud computing for health care”, The Scientific World Journal, vol. 2014, Article ID 146970, 7 pages, 2014.

[4] A. Abbas and S. U. Khan, “A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds”, IEEE journal of Biomedical and health informatics, vol. 18, no. 4, July, 2014.

[5] G. C. Kagadis, C. Kloukinas, K. Moore, J. Philbin, P. Papadimitroulas, C. Alexakos, P. G. Nagy, D. Visvikis and W. R. Hendee, “Cloud computing in medical imaging”, Medical Physics, vol. 40, no. 070901, 2013.

[6] E. S. Dove, Y. Joly A. Tasse, “Genomic cloud computing: legal and ethical points to consider”, European Journal of Human Genetics, pp. 1-8, 2014.

[7] 국가기술표준원 and 한국표준협회, “표준기반 R&D 로드맵 스마트의료 정보”, 2014

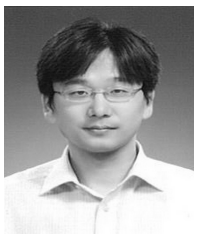
[8] 미래창조부, “사물인터넷 (IoT) 정보보호 로드맵”, 2014. 10. 31

〈저 자 소 개〉

이 혜 림 (Hye Lim Lee)
정회원

2012년 8월 : 고려대학교 정보수학과 졸업
2013년 3월~현재 : 고려대학교 정보보호학과 석사과정
관심분야 : 정보보호, 응용통계, 보안관제 시스템 구축

조 재 연 (Jaeyeon Cho)
2011년 2월 : 고려대학교 수학과 졸업
2014년 3월~현재 : 고려대학교 정보보호대학원 석사과정
관심분야 : 정보보호, 금융공학, 응용통계



윤 지 원 (Ji Won Yoon)
종신회원

2003년 2월 : 성균관대학교 정보공학과 졸업
2005년 5월 : 영국 에든버러 대학교 정보대학 석사
2008년 11월 : 영국 캠브리지대학교 전자공학과 박사
2008년 3월~2009년 5월 : 영국 옥스퍼드 대학교 로봇연구소 연구원
2009년 7월~2011년 5월 : 아일랜드 더블린대학교 통계학과 연구원
2011년 7월~2012년 8월 : IBM 연구소 정규직 연구원
2012년 9월~현재 : 고려대학교 정보보호대학원/사이버국방학과 조교수
관심분야 : 통계신호처리, 정보보호