IoMT 기술과 의료정보 보안

우성희 · 이효정*

한국교통대학교

IoMT Technology and Medical Information Security

SungHee Woo · Hyojeong Lee*

Korea National University

E-mail : shwoo@ut.ac.kr / leehj@ut.ac.kr

요 약

사물 인터넷 (IoT)은 모든 시장과 산업을 연결시켜 다양한 서비스와 서비스 제공 업체를 위한 새로운 비즈니스 모델을 가능하게 한다. 의료 사물 인터넷 (IoMT)은 의료 발전을 가속화 할뿐만 아니라 보다 인간적인 접근 방식으로 치료를 가능하게 한다. 또한 데이터를 통해 치료 방법과 정밀 의료의 질을 개선 및 적시에 진료를 받을 수 있도록 하며 간소화된 워크플로우를 통해 의료기관의 운영 생산성을 향상시킨다. 하지만 의료분야는 사람의 건강과 생명에 직접적인 영향을 주기 때문에 무엇보다 보안성 확보가 이슈가 되고 있으며 이를 악용하려는 해커들에게 표적이 되고 있다. 따라서 본 연구에서는 의료분야의 IoMT 기술과 보안의 위협요소 및 대응방안을 분석한다.

ABSTRACT

The Internet of Things (IoT) connects all markets and industries, enabling new business models for a variety of services and service providers. The Internet of Medical Things (IoMT) not only accelerates medical advances, but also enables treatment with a more human approach. In addition, it improves treatment methods and quality of precision medical care through data, enables timely treatment, and improves operational productivity of medical institutions through a simplified workflow. However, since the medical field directly affects human health and life, securing security has become an issue above all else, and is a target for hackers trying to exploit it. Therefore, in this study, IoMT technology and security threats and countermeasures in the medical field are analyzed.

키워드

IoMT, IoT, Medical Information Security

Ⅰ. 서 론

사물인터넷 기술은 여러 분야의 산업과 융합되어 새로운 시장을 창출하고 있다. 특히, 의료분야의 경우 IoT 기술뿐만 아니라 빅데이터, AI기술까지 다양한 신기술이 결합하여 새로운 의료 서비스를 만들고 있다. 전세계 의료분야의 IoT 시장은 2021년까지 1,367억 달러로 예상되며, 신체의 여러 부분에 연결되고 모니터링 되는 의료기기가 약 370만 개로 추정된다[1].

의료사물인터넷(IoMT:Internet of Medical Things)이란 개인의 생활습관, 질병 이력, 의료이용정보, 유전체 정보 등을 디지털 데이터로 만들어 화 정보, 기기, 시스템이 하나로 연결되는 기술로, X-ray, MRI 스캐너 등 고정식 의료기계, 맥박 조정기와 같은 체내 이식기기, 웨어러블 워치와 같이 착용 가능한 기기 등의 IoMT 기기들이 있다. 이러한 IoMT의 도입은 환자, 의료 제공자, 환자 가족, 보험사 등을 긴밀히 연결하여 신속하고 편리한 환경에서 건강관리를 하도록 한다. 현재 IoMT는 머

* corresponding author

신러닝 기술의 발전과 네트워크 의료기기 및 스마트 폰의 증가로 시장의 성장은 가속화 될 것이다. 또한, 클라우드 컴퓨팅 및 빅데이터와 결합한 IoMT는 의료 데이터 분석을 통한 예방 솔루션을 제안하는 새로운 서비스를 만들어 내고 있다. 하지만 의료분야는 사람의 건강과 생명에 직접적인 관계가 있어 보안성 확보가 우선되어야 하며 이를 악용하려는 해커들의 표적이 되고 있다. 본 연구에서는 의료분야의 IoMT 기술과 보안의 위협요소 및 대응방안을 분석한다.

II. IoMT 기술

사물인터넷의 발전은 자동차, 건설, 환경 등 여러 산업과 융합하여 새로운 시장을 개척하고 있으며 이중 의료에 적용되는 사례가 증가하고 있다. 질병에 기초한 의료 서비스 분야(실시간 모니터링, 홈케어, 만성질환관리등)에 적용된 기술[2]을 보면 다음과 같다.

표 1. IoMT 기술

IOMT 기술	내 용
Open APS(Artificia l Pancreas System)	인공지능 췌장 시스템을 이용하여 야간시간에서 아침식사 사이에 혈당을 유지하도록 인슐린 펌프를 조절하여 제 1형 당뇨병을 조절
CGM(Continuous glucose monitoring) System.	최초의 이식형 당뇨 조절 시스템으로 환자의 팔의 피부에 CGM센서를 이식해 최대 90일 동안 환자의 혈당 수치를 충전식 송신기에 전송하고 이 정보를 블루투스 방식으로 환자 스마트실시간 폰에 설치된 앱으로 실시간으로 전송
의료기록 자동 저장 장치	다발성 골수종 환자들의 생활 패턴 데이터를 조사하기 위해 개발
앱을 이용한 약물 사용 기록 저장	만성폐쇄질환 환자들을 위한 연구중인것으로 맞춤형 센서를 통해 수동으로 기록을 입력하고 전송하여 환자와 의사들에게 플랫폼으로서 정보 제공
삼킬 수 있는 센서	삼킬수 있는 센서로 항정신성 약물이나 고혈압약과 같은 꾸준한 복용이 중요한 경우 사용
스마트 컨택트 렌즈	구글의 스마트 렌즈 기술중 하나인 비 외과적인 내장형 컨텍트 렌즈 기술을 인가 받음. 환자의 안구 눈물을 이용하여 혈당을 측정하고 정보를 모바일 기기로 전송하는 시스템
혈응고 검사	블루투스를 이용한 혈액 응고 속도를 빠르게 측정할수 있게 하는 첫 번째 기기로 항응고 질환을 앓고 있는 환자들이 스스로 뇌졸중이나 출혈에 대비 할수 있도록 함
스마트와치를 이용한 우울증 치료	우울증을 앓고 있는 환자들의 30일간의 치료에 이용
류마티스 관절염 환자들의 삶의 질 측정	류마티스 관절염을 앓고 있는 환자들에게 3개월간 일반적인 증상과 함께 다른 삶의 질에 대해서도 측정하여 추적
파킨슨의 경과 모니터링	모바일 기기, 센서, 머신러닝 기술을 이용하여 실시간으로 24시간 내내 의사들과 연구자들에게 질병의 증상 정보를 제공

III. IoMT 보안 위협요소와 대응방안

3.1 보안 위협요소

의료기관 내부의 각종 의료 서비스에 활용되는 의료기기, 의료기기를 연동시키는 게이트웨이, 유·무선 네트워크, 의료정보시스템(EMR, EHR 등에서 의료기기에서 보내 온 정보를 모니터링하는 부분만으로 제한)등 많은 곳에 보안 위협 요소들이 존재하지만 의료기기 하드웨어 영역과 OS 영역을 중심으로 위협요소[3][4][5][6]들을 살펴보면 다음과 같다.

표 2. 의료기기 하드웨어 영역

보안 위협	내 용
의료기기 분실 및 도난	물리적으로 의료기기를 분실하거나 도난당함으로 인해 의료기기 내 저장되어 있는 데이터 유출의 위험 존재
디버그 포트를 이용한 펌웨어 획득	의료기기 개발시 사용된 디버그에 포트를 제거하지 않은 의료기기에서 디버그 포트를 활용하여 펌웨어 등을 획득하는 공격으로 공격자가 내부 소스코드 및 구조를 파악할 수 있으며, 이를 기반으로 알려지지 않은 취약점을 확인하거나 특정 부분을 변조하여 의료기기에 다시 주입공격
부채널 공격	의료기기에서 전송되는 정보를 암호 알고리즘이 작동할 때 전기 소모량, 전자기 신호량 등을 분석해 암호키 등을 유추하는 공격기법
USB를 통한 악성코드 감염	USB 포트를 통한 악성코드 유포 또는 정보 유출
센서 스푸핑	인증체계를 적용하지 않은 센서에 스푸핑 공격 등으로 데이터 감지를 방해함으로써 의료기기 오작동 유발

표 3. 의료기기 사용 OS 영역

보안 위협	내 용
3rd party 소프트웨어 취약점	의료기기에 펌웨어 또는 운영체제 및 어플리케이션 소프트웨어, 운영체제, 라이브러리, 데이타베이스, 모듈 등 공개용 및 상용 소프트웨어에 자체에 포함된 취약점으로 인한 기기 오동작 및 정보 노출
부적절한 소프트웨어 패치	최신 버전의 소프트웨어 보안 패치가 되디 않거나 안전한 경로를 통하지 않은 패치로 악성코드 감염, 패치 전 적절한 안전성 테스트를 수행하지 않아서 발생하는 의료기기 오작동 등
악성코드 감염(랜섬웨어)	Anti-virus 시스템이나 백신 설치 어려움과 같은 의료기기 구조적 문제로 발생하는 위협으로 실행파일 검증 부족 등을 통한 악성코드 감염

표 4. 의료기기 관리 및 제어 영역

보안 위협	내 용
설정 및 측정 값(calibration values) 조작	악의적 공격자가 안전성 제어 또는 측정 기능의 값을 '덮어쓰기' 공격으로 변경하여 해당 기능을 상실하거나 안전성 한도 값을 초과하여 환자의 생명과 건강에 치명적인 위해를 가함
내부자 공격	악의적 의도를 가진 관리자 기기 설정 변경 또는 비정상적인 활동
취약한 인증	안전한 인증체계를 적용하지 않아 권한 없는 사람이나 기기가 의료기기에 접근하여 권한을 탈취

3.2 대응방안

의료기기는 사람의 생명과 연결되기에 다양한 관점의 보안과 철저한 보안이 필요하며 사물인터넷 공격에 대응하기 위해서는 다음 그림 1과 같은 보안 요구사항[4][5][6]을 준수할 필요가 있다. 보안 요구사항 중에서도 해커에 진입을 막기 위해 네트워크의 엑세스 관리가 요구되며 해커가 침투하더라도 내부자료를 가져가지 못하도록 망 분리를 하고 IoMT 장치에서 수집 및 저장된 데이터를 제한하고 암호화하여 저장한다.

Ⅳ. 결 론

4차 산업혁명 시대, 스마트폰 등과 연결된 스마트 조명, 스마트홈 구축에 용이한 인공지능 스피커 등 사물인터넷 기술이 미래 산업으로 주목받고 있다. 특히 미래 산업 분야에 사물인터넷 기술을 적용하는 사례가 증가하고 있으며 이에 의료분야에서도 의료사물인터넷을 도입하고 있다. 의료사물인터넷은 개인의 생활습관, 질병 이력, 의료이용정보, 유전체 정보 등을 데이터화 하여 정보, 기기, 시스템이 하나로 연결되는 기술로 인간이 더 건강한 삶을 살도록 도움을 줄 수 있으나 개인 의료정보의 보안 문제는 해결해야 할 과제로 남아있다. 철저한 보안과 기본 권리 보호를 바탕으로 기술을 사용할 수 있어야 할 것이다.

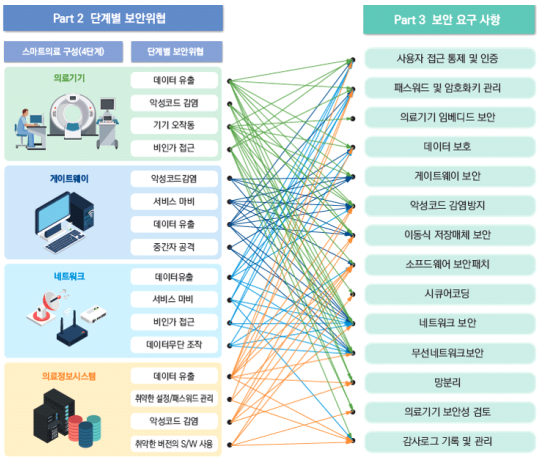

그림 1. 보안 요구사항[6]

Acknowledgement

이 논문은 2021년 한국교통대학교 지원을 받아 수행한 연구임.

References

[1]보건산업 4차 산업혁명 시리즈: 글로벌 의료사물인터넷(Internet of Medical Things, IoMT), KHIDI Brief Vol.250.

[2] 보건의료 R&D 동향, "헬스케어에 활용되는 10가지 IoT 기술", 한국보건 산업진흥원, 2017.5.

[3] IoT 기술, 의료 분야에도 도입 활발 'IoMT', http://www.kidd.co.kr/news/209693

[4] Comprehensive Guide to IoMT Cybersecurity -Risks, Safeguards, and What We Protect : https://www.alpinesecurity.com/blog/comprehensive-guide-to-iomt-cybersecurity

[5] Obstacles on the Path to Comprehensive IoMT Security(https://www.cybermdx.com/blog/obstacles-on-the-path-to-comprehensive-iomt-security)

[6] IoT보안 얼라이언스, 스마트의료 사이버보안 가이드, KISA, 2018.5.