JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 27 No. 7, pp. 57-64, July 2022
https://doi.org/10.9708/jksci.2022.27.07.057

A study on the Establishment of a Digital Healthcare Next-Generation Information Protection System

Ki-Hwan Kim*, Sung-Soo Choi**, Il-Hwan Kim***, Yong-Tae Shin****

*Senior Researcher, ETRI, Daejeon, Korea
**Professor, Dept. of Computer Science, Inha Technical College, Incheon, Korea
***Chief Researcher, Wonju Medical Device Techno Valley, Wonju, Korea
****Professor, Dept. of Computer Science, Soongsil University, Seoul, Korea

[Abstract]

In this paper, the definition and overview of digital health care that has emerged recently, core technology, and We would like to propose a plan to establish a next-generation information protection system that can protect digital healthcare devices and data from cyber attacks. Various vulnerabilities exist for digital healthcare devices and data, and cyber attacks are possible for those vulnerabilities. Through an attack on digital health care devices and information and communication networks, it can directly adversely affect human life and health, Since digital healthcare data contains sensitive and personal information, it is essential to safely protect it from cyber attacks. In the case of this proposal, for continuous safe management of data and cyber attacks on equipment and communication networks for digital health devices, It is expected to be able to respond more effectively and continuously through the establishment of the next-generation information protection system.

▸ **Key words**: Digital healthcare, Cyber attack, Security, Health Devices, Next generation, Information Protection, ISMS-P

[요 약]

본 논문에서는 최근 대두되고 있는 디지털 헬스케어의 정의와 개요, 핵심기술, 그리고 디지털 헬스케어 기기 및 데이터를 사이버공격으로부터 보호할 수 있는 디지털 헬스케어 차세대 정보보안모델 수립 방안을 제안하고자 한다. 디지털 헬스케어기기와 데이터를 대상으로 다양한 취약점이 존재하고 있으며, 그 취약점에 대하여 사이버공격이 가능하다. 디지털 헬스케어 기기 및 정보통신망에 대한 공격을 통하여 직접적으로 사람의 생명 및 건강에 악영향을 끼칠 수 있으며, 디지털 헬스케어 데이터는 의료, 민감정보와 개인정보를 포함하고 있으므로, 필수적으로 사이버공격으로부터 안전하게 보호를 해야 한다. 본 제안의 경우 디지털헬스기기에 대한 장비 및 통신망에 대한 사이버공격과 데이터에 대한 지속적인 안전한 관리를 위해서는 차세대 정보보호체계 수립을 통하여 보다 효과적이며, 지속적으로 대응할 수 있을 것으로 전망된다.

▸ **주제어**: 디지털 헬스케어, 사이버공격, 정보보안, 헬스기기, 차세대 정보보호, ISMS-P 인증

• First Author: Ki-Hwan Kim, Corresponding Author: Yong-Tae Shin
*Ki-Hwan Kim (itconsult@hanmail.net), ETRI
**Sung-Soo Choi (sungsoo71@ai-net.kr), Dept. of Computer Science, Inha Technical College
***Il-Hwan Kim (http@wmit.or.kr), Wonju Medical Device Techno Valley
****Yong-Tae Shin (shin@ssu.ac.kr), Dept. of Computer Science, Soongsil University
• Received: 2022. 06. 07, Revised: 2022. 06. 27, Accepted: 2022. 06. 29.
• This paper was presented at the 64th Summer Conference of the Korean Society of Computer and Information Technology in 2021.This is an extension of the thesis ("Research on Digital Healthcare and Information Security")

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

디지털 헬스케어는 모바일 헬스케어, 원격의료, 보건의료분석학, 디지털보건의료시스템 네 가지 분야로 구분할 수 있으며, 특히, 코로나19 영향으로 비대면 모바일 헬스케어, 원격의료, 디지털보건의료시스템 분야에 대한 정보보호가 중요해지고 있다.

디지털 헬스케어는 장소의 제한이 없이 사용자가 스마트 기기를 이용하여 의료 서비스를 받을 수 있도록 하는 연구 및 웨어러블 디바이스에 기반한 헬스케어 시스템에 대한 여러 연구가 진행되었다[1].

디지털 헬스케어는 원격진료, 스마트헬스, 모바일 헬스를 포괄하는 광의의 개념으로, 유헬스(U-Health)와 비교하여 산업의 주도권이 의료영역(의료기관, 환자)에서 일반 소비영역(일반제조기업 및 소비자)까지 확대된 형태를 보인다. 고령화에 따른 예방과 일상관리의 중요성이 증대되고 있으며, 건강 수명 연장을 위한 개인 맞춤형 헬스케어 수요가 증대되고 있다[2].

디지털 헬스케어 산업의 계수별 파급효과를 살펴보면, 첫째, 생산 측면에서 보면 디지털 헬스케어 산업의 생산유발계수는 전체산업 평균보다 크게 나타났다. 이는 본 산업이 전체산업에 미치는 생산 파급효과가 크다는 것을 나타낸다. 둘째, 부가가치 측면에서 살펴보면 부가가치유발계수가 전체산업 평균보다 크게 나타났다[3].

ICT(Information and Communications Technology) 기술과 헬스케어 산업의 융합을 통해 정보통신기술(ICT)과 융합한 의료기기 시장이 매년 성장하고 있다.

세계 디지털 헬스케어 산업 시장은 2013년~2017년간의 연평균성장률과 2017년~2020년간의 연평균 성장률을 반영하여 향후 시장 전망을 하면, 2019년에는 1,940억 달러 규모로 성장할 것으로 전망된다[4].

디지털 헬스케어는 환자의 혈압, 심전도 등 생체정보를 실시간으로 측정하여 진단과 치료를 돕는 기술이다. 우리 사회는 사망률의 감소와 저출산으로 인하여 인구 고령화가 심화되고 이로 인한 의료서비스의 실질적 수요가 증가되고 있어 ICT 기반의 의료기술을 도입하여 질병의 예방 및 관리에 대한 디지털 헬스케어 서비스의 수요가 증가하는 추세이다.

이에 따라 의료와 ICT 기술의 융합 기술인 디지털 헬스케어 서비스가 실현되고 있고 디지털 헬스케어의 진화된 모델을 통하여 공간적, 시간적 제약이 없어지고 원격진료와 같은 환자의 생활 공간 속에서 IT기술이 포함된 의료센서 및 헬스케어기기를 통해 수집된 의료 정보와 생체 정보를 기반으로 언제 어디서나 의료 서비스를 받을 수 있게 되었다. 다만, 디지털 헬스케어로 관리가 가능한 생체정보가 혈당, 맥박, 혈압 등 기본적인 생체정보에 머무르고 있으며 빅데이터나 인공지능(AI)을 활용한 의료 서비스 기술도 걸음마 단계이다. 반면, 선진국에서는 스마트렌즈로 실시간으로 간편하게 혈당을 측정하는 기술(구글 노바티스), AI로 암 등 환자에게 최적의 치료법을 제시하는 기술(IBM), 만성질환자의 규칙적인 복약 관리를 돕는 기술(메드마인더) 등 디지털 헬스케어 기술을 고도화하고 있다[5].

그러나, 대부분의 디지털 헬스케어 의료정보는 병력정보, 신상정보와 같은 다수의 개인정보를 포함하고 있어, 프라이버시를 침해할 수 있는 민감한 정보를 포함하고 있어 유출될 경우 심각한 피해를 초래할 수 있다. 이에 의료데이터의 공유 및 활용 과정에서 발생하는 개인정보 및 민감정보를 보호해야 하고 이를 위해 기술적, 관리적 차세대 정보보호 관리체계 요구사항이 필요하다.

본 논문에서는 디지털 헬스케어를 실현하기 위해 디지털 헬스케어를 통해 수집, 활용되는 의료 데이터 공유 및 안전한 활용 서비스를 위한 차세대 정보보호체계 수립 방안에 대해 검토하고자 한다.

본 논문의 구성은 2장에서 관련 연구를 소개하고, 3장에서 차세대 정보보안 모델을 설명한다. 마지막으로 4장에서는 전반적인 결론을 요약한다.

II. Preliminaries

1. Related works

1.1 Technology Trends in Digital Healthcare

디지털 헬스케어는 넓은 의미로 건강 관리를 의미하고 디지털 기술이 포함된 디지털 헬스케어와 전통적인 의료영역으로 나누어진다. 의료에서 디지털 시술을 이용한 응용 범위는 더욱더 넓어질 전망으로 Fig. 1은 디지털 헬스케어의 범위를 보여주고 있다[6].

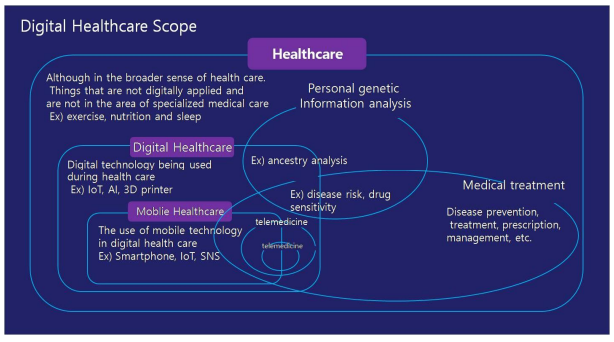


Fig. 1. Digital Healthcare Scope

디지털 헬스케어는 ICT기술과 융합을 통해 다양한 비대면 형태로 발전 가능하다. 그 예로 우울증 등 정신건강의 치료, 인지 재활 치료 등 디지털 치료를 가능하게 하는 비대면 인공지능 솔루션 기술, 5G 기반의 원격 환자 모니터링과 인공지능 기반의 비대면 진단 기술, 비대면 진단과 치료의 효과를 극대화하기 위한 다기관 의료지능 협진 및 비대면 선별 진단을 위한 의료지능 에이전트 기술, 디지털 트윈 기술 기반의 비대면 진료, 공공의료-대형병원-지역병원 사이의 협업이 가능한 의료지능 허브 네트워크 기술 등으로 발전 가능하다[7].

디지털 헬스케어는 인공지능, 빅데이터, 클라우드, 사물인터넷, 웨어러블, 원격의료 등 ICT와 융합된 디지털 기술을 통한 건강관리 및 의료서비스를 의미한다고 볼 수 있다. 기존 치료 중심에서 예측 가능한 예방으로 의료 패러다임이 바뀌면서 주목받고 있는 디지털 헬스케어는 의료 질과 서비스 향상은 물론 의료비 절감의 상당한 효과가 있다고 평가받고 있다.

개인의 의료기관 진료정보와 함께 유전체 정보 및 건강정보 등 다양한 데이터가 통합. 수집되는 빅데이터는 인공지능을 통해 분석·도출되는 정밀 의료서비스를 제공하는 근간이 될 전망이다. 또한 디지털 헬스케어와 함께 정밀 의료서비스를 제공하기 위해서는 더 많은 정보를 수집하고 활용할 수 있는 의료 클라우드 서비스 도입이 요구된다.

미국의 경우 마이크로소프트, 아마존, 구글 등이 정보보안 및 프라이버시 보호를 위한 법 규정 HIPAA(Health insurance portability and Accountability Act)와 BAA(Business Associate Agreement)의 준수를 약속한 이후 관련 시장이 빠르게 성장하고 있다.

일본의 경우 의료 클라우드 서비스는 대기업들이 시장을 주도하고 있으며 후지쓰의 경우 2013년 의료기관 대상으로 재택의료, 개호지원서비스 '왕진선생'을 시작하였고 NEC는 데이터센터를 활용해 종합 병원을 대상으로 지역 진료소 전자의무기록과 의료영상을 공유할 수 있는 클라우드 서비스를 제공하고 있다.

한국도 클라우드가 의료데이터 공유와 활용 문제를 해결할 대안으로 제시되고 있지만, 대형 병원 간의 데이터 표준 도입이 전제되어야 한다는 의견이 있고 이를 해결하기 위한 논의를 하고 있는 시점이다.

의료데이터를 공유하는 포터빌리티를 형성하기 위해서는 데이터 표준이 도입되어야 하며 병원들이 국제적 표준에 따라 데이터를 공개했을 때, 현실적인 의료데이터를 공유가 이루어질 전망이다.

정부도 Fig. 2와 같이 2021년 2월 마이 헬스웨이 플랫폼 사업을 발표하고 보건의료 분야 데이터 표준 API 구축하기 위하여 민간의료기관 데이터 전환, 디지털 헬스케어 데이터 수집, 심평원, 질병청의 공공 데이터 연계를 위한 표준화 작업을 시작했다[8].

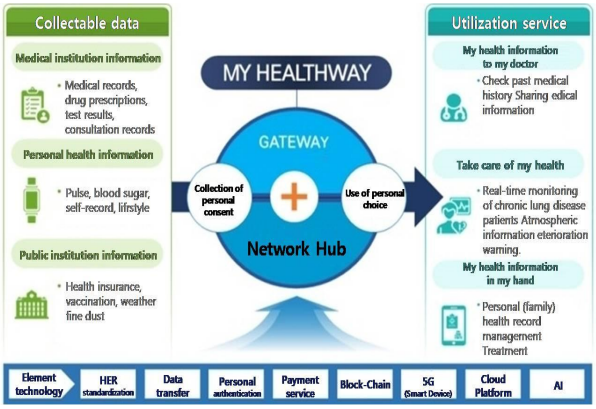


Fig. 2. My healthway platform

1.2 Technology trends in foreign digital healthcare

Fig. 3의 애플(Apple)사의 디지털 헬스키드 플랫폼에서 애플은 애플워치로 건강 정보를 수집하고 스마트폰으로 정보를 통합, 수집된 방대한 데이터를 클라우드로 저장하고 인공지능으로 이를 분석하여 개인 맞춤 의료, 예측의료, 참여의료가 가능하도록 디지털 헬스케어 서비스를 제공하고 있다[9].

Fig. 3. Apple's health kit platform

헬스키트를 중심으로 사용자(환자)와 각사의 헬스케어 기기와 앱이 있고 반대편으로 병원과 전자의무기록(EMR) 기업이 있어 환자들이 시간, 장소에 영향을 받지 않고 디지털 헬스케어 기기와 앱으로 데이터를 측정하면 이 의료데이터를 아이폰의 헬스키트 플랫폼에 통합적으로 저장 및 관리되면서, 전자의무기록을 거쳐 병원에 전달된다.

헬스키트를 중심으로 의료 생태계의 주요 주체인 환자와 헬스케어 기기, 스마트폰, 전자의무기록, 병원을 통합하는 데이터의 흐름이 완성된다.

구글사의 경우 2022년 3월 '구글 체크업' 행사 발표를 통해 핏빗(Fitbit)에 새로운 기능 도입, AI 혁신 의료기술 개발, 구글 검색엔진에 병원 예약 플랫폼 추가, 유튜브(Youtube) 건강 오보 제재 방안을 발표했다.

글로벌 이커머스 기업 아마존(Amazon)은 처방 약을 배송하는 온라인 약국을 시작으로 환자부터 기업, 병원까지 그 서비스 대상을 광범위하게 포함하고 있다. 특히 미국 전역에 있는 아마존 배송망과 창고를 활용한 디지털 헬스케어 인프라 구축이 용이하다는 장점을 가지고 있으며, 2020년 8월 웨어러블 기기 헤일로(Halo)를 통해 사용자의 음성으로 신체적, 정신적 이상을 감지하고 스마트폰 카메라로 체지방을 계산할 수 있는 인공지능 기반 스마트 밴드를 출시하였다[10].

1.3 Key core technologies for digital healthcare

디지털 헬스케어의 주요 핵심기술은 Table 1 과 같이 비침습 무구속, 무자각 건강정보 측정 기술, 맞춤형 진단 및 현장진단 기술, 개방형 건강관리 플랫폼 기술, 맞춤형 건강관리 서비스 기술로 구분이 가능하다[11].

Table 1. Key core technologies for digital healthcare

Core Technology
Non-invasive,non-constraint, non-aware health information measurement technology
Customized diagnosis and on-site diagnosis technology
Open Healthcare PlatformTechnology
Customizedremote health management service technology

비침습 무구속 무자각 건강정보 측정기술은 비침습 자가건강진단기술, 무구속 생체신호측정기술, 무자각 생활정보 패턴 측정기술, 인체 이식형 생체신호 측정기술로 세부기술로 나눌 수 있으며 맞춤형 진단 및 현장진단 기술은 유진정보 기반 맞춤형 진단기술, 현장진단 바이오칩, 센서기술로 세부내용으로 나눌 수 있다.

개방형 건강관리 플랫폼 기술은 개인 건강 레코드 구축, 공유, 활용 기술과 건강 빅데이터 분석기술, 모바일 건강관리 서비스 플랫폼 기술로 나누어지며 맞춤형 건강관리 서비스 기술은 원격 건강 모니터링 기술, 맞춤형 원격진료 기술, 맞춤형 원격치료 기술로 세부내용이 나누어진다.

디지털 헬스케어의 중요한 기술 중 하나인 Fig. 4 스마트 센서는 개인용 또는 가정용 의료기기에 통신기능을 추가한 초기 단계의 단순 측정센서에서 사용성과 편리함이 중심이 되는 웨어러블 센서, 일대 다수의 복잡 분석 기술로 발전하고 있다.

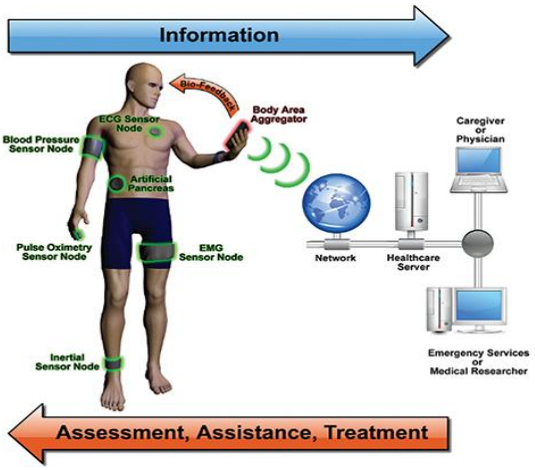


Fig. 4. Network interaction with smart sensors

오늘날 빠르게 개선되고 있는 5G 무선통신 기술과 고급 센서를 사용하여 많은 기업에서 디지털 헬스케어를 위한 솔루션을 제안하고 있다.

초연결시대가 도래함에 따라, 클라우드 및 커넥티드 기기의 발전은 다양한 IoT(Internet of Things)기기들이 개발될 수 있는 토대가 되고 있다. IoT 기기들은 대부분 임베디드 기기로서 가전제품부터, 항공 우주, 자동차, 의료 및 산업용 시장까지 폭넓게 적용된다[12].

또한, 데이터 분석 기술의 발전과 데이터 수집 채널이 다양하게 확대됨으로써 단순한 센서 값으로부터 여러 복합적인 정보를 추론해 내는 분석 기법이 핵심 기술로 떠오르고 있다. 빅데이터와 IoT는 환자의 상태를 감지, 예측 추론하는 기술로 디지털 헬스케어의 핵심기술중 하나이다.

IoT에 빅데이터 기술이 접목하여 디지털 헬스케어 서비스에 대한 사용자의 평가와 의도를 예측할 수 있어 보다 효과적인 서비스의 수용 의도를 파악하는 도구로 활용되며 SNS는 헬스케어 서비스의 커뮤니케이션 과정에서 일방향의 정보제공이나 알림과는 다르게 이용자의 행동에 영향을 미칠 수 있는 방법과 관계 설정이 가능하여 좀 더 나은 효과적인 방법으로 서비스 사용 요구 파악이 가능하다.

1.4 MEDBIZ Healthcare Platform

MEDBIZ 헬스케어 플랫폼은 Fig. 5 와 같이 기존 IoT 플랫폼과 의료정보 클라우드 및 빅데이터 플랫폼을 통합하는 시스템이다. 해당 시스템은 헬스케어 IoT 디바이스 연동, 외부 의료 데이터 연계, 일반 공공 데이터 연계, 건강심사평가원 빅데이터 연계를 지원한다. 헬스케어 데이

터를 수집·저장하고 관리하며 데이터의 분석을 통해 통합 서비스 제공을 목적으로 한다[13].

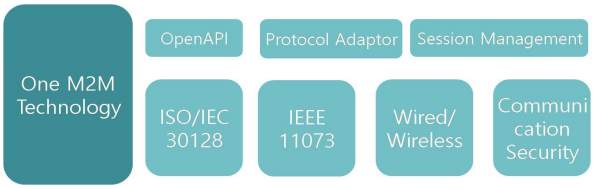


Fig. 5. MEDBIZ Healthcare Platform System Core Technology

1.5 Digital healthcare and security vulnerabilities

디지털 헬스케어 기기·서비스는 소프트웨어 및 네트워크 연결성이 강화되면서 Table 2 와 같이 네트워크 프로토콜 기반의 보안사고가 증가하고 있다. 해당 사례는 사이버보안 취약점뿐만 아니라 소프트웨어 코드가 조작될 경우 비인가 사용자가 해당 의료 기기를 조정할 수 있음을 보여주고 있다. 또, 의료기기 내부에 하드 코딩된 암호에 대한 취약점을 이용하여 인공 호흡기와 약물 주입 펌프 등의 수술 장비를 원격으로 조작할 수 있음을 뜻하기도 한다[14].

Table 2. Cases of security incidents and vulnerabilities in digital healthcare devices and services

Year	M	Security incident case
2020	1	FCD announces that some GE Healthcare medical devices may be remotely controlled and pose a risk to patients
	3	FDA Announces SweynTooth Cybersecurity Vulnerability May Affect Certain Medical Devices
2019	3	U.S. Department of Homeland Security Announces Medtronic's Implantable Defibrillator Could Be Attacked by Sensitive Information Collected Using Unsafe Protocols
	6	FDA Announces Medtronic Insulin Pumps Can Be Controlled Through Another Device Wirelessly Connected

디지털 헬스케어 관련 보안 위협은 인증 및 허가 유형, 암호 유형, 데이터 보안 및 안전한 통신 유형, 안전한 기기 및 물리적 보호 유형으로 분류할 수 있다.

인증 및 허가의 유형은 인증 우회, 비 인가된 기기연결, 과도한 권한부여, 연속된 인증시도, 응급상황 대응 제한, 동시 접속에 따른 정책 일관성 오류, 인증정보 노출 및 유추, 취약한 비밀번호, 인증결과 변조의 보안 위협으로 세분화할 수 있다. 암호의 유형은 취약한 암호화, 취약한 암호 알고리즘 보안위협으로 세분화할 수 있다.

데이터 보안 및 안전한 통신 유형은 입력값 검증 부재, 신뢰할 수 없는 데이터 송수신, 데이터 노출 및 변조, 사용자 세션 탈취 보안 위협으로 세분화할 수 있다.

안전한 기기 관리 및 물리적 보호 유형은 안전하지 않은 업데이트, 업데이트 실패, 무결성 오류, 서비스 거부, 악성 행위, 잔여 정보 악용, 중요 설정 임의 변경, 오류 대응, 안전하지 않은 개발, 취약한 운영체제, 취약한 서드파티 모듈 및 라이브러리 사용, 시스템 로그에 민감한 정보기록, 디버깅을 통한 중요정보 노출, 비인가 된 물리적 접근 보안 위협으로 세분화할 수 있다.

디지털 헬스케어 데이터 역시 보안 위협에 따른 환자 개인정보 유출의 위협이 발생할 수 있다.

의료정보의 프라이버시에 대한 위협요소 중에는 비공개되는 의료데이터 저장소에 저장.관리되는 의료정보를 무단으로 거래하고 유출시키는 것이다. 이러한 사례 중에 환자의 병력과 이름, 주소, 전화번호, 연령 등의 정보들이 전국의 약국과 건강 전문 업체로 판매되는 사례가 발생되고 있다. 예를 들면, 자궁암, 정신 분열증, 아토피성 피부염, 당뇨병 등의 병력을 가진 환자의 개인의료정보 리스트가 전국의 약국과 건강식품 판매 회사에 거래되는 일이 발생되고 있다[15].

III. The Proposed Scheme

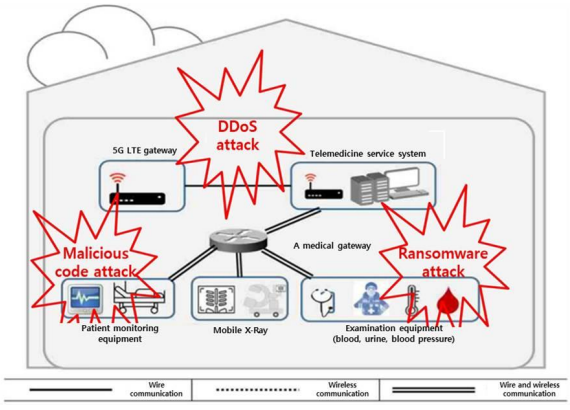


Fig. 6. Digital healthcare cyberattack Technology

디지털 헬스케어 기기·서비스에서 Fig. 6 과 같이 다양한 취약점에 대하여 사이버공격이 가능하다. 즉, 통신 구간에서 DDoS 공격을 통하여 해당 서비스를 정지하거나, 운영을 중단하게 할 수 있고, 악성코드 공격을 통하여 의료 민감정보 및 개인정보를 유출하거나 주요 의료기기를 원격조정 하여 인명을 다치게 할 수도 있는 것이다[16].

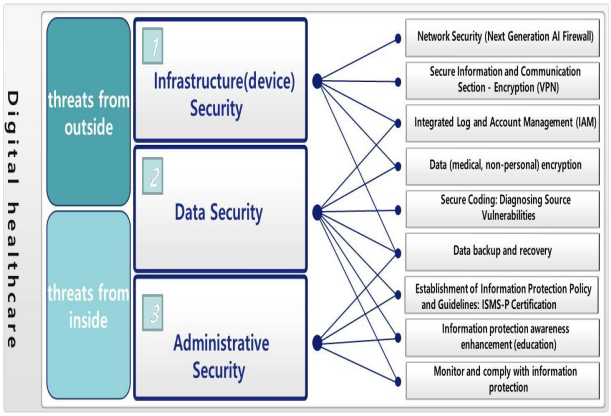


Fig. 7. Digital healthcare next-generation information security model

디지털 헬스케어 보안 위협에 대하여 Fig. 7과 같이 분야별 차세대 정보보안모델 수립 및 적용이 필요하다.

즉, 인프라 보안, 데이터 보안, 관리적 보안 분야에 대한 면밀한 이해와 적용이 필요하다. 첫째, 인프라 보안에 대하여 상세하게 알아보자. 보안운영체제 기반 기술에 대한 보안요구사항, 하드웨어 보안 모듈 적용, 무결성 측정 및 검증 기술, 시스템에 대한 접근제어, 감시로그 시스템, 암호화, 사용자 인증 기술 등으로 요약할 수 있으며 이를 더욱 세분화하면 인증 및 허가, 암호, 데이터 보안, 안전한 통신, 안전한 기기관리, 물리적 보호 유형으로 나눌 수 있다. 인증 및 허가는 디지털 헬스케어 기기 운영 및 관리 기능 접근 시 사용자 인증이 필요한 사용자 인증과 디지털 헬스케어 기기에 대한 기기인증을 통해 비 인가된 접근을 통제해야 하는 기기인증, 디지털 헬스케어 기기에 대한 비인가된 접근을 제한해야 하고 비밀번호, 암호키 등 중요 데이터에 비인가 된 접근을 제한하는 접근통제, 비밀번호는 하드코딩 되지 않고 안전한 저장 방법을 제공할 것, 기기 사용 초기에 인증정보를 잘 설정하도록 요구하거나 초기 인증정보를 변경하도록 요구하는 안전한 비밀번호 메커니즘 보안항목 요구사항으로 세분화 된다.

암호 유형은 디지털 헬스케어 기기에 적용되는 암호 알고리즘은 안전성이 검증된 알고리즘을 사용해야 하는 안전한 암호 알고리즘 사용항목, 암호키의 생명주기를 고려하여 안전하게 관리와 함께 암호 연산 목적에 따라 별도의 암호키를 사용하는 안전한 암호키 관리, 난수 생성 시 난수성이 검증된 알고리즘을 이용해야 하는 안전한 난수 생성 보안항목 요구사항으로 세분화 된다.

통신상의 안전성은 사용자 중심의 헬스케어 서비스가 제공될 경우 사용자의 프라이버시 정보에 대해서는 개체간의 안전한 상호 인증을 기반으로 전송 데이터의 기밀성과 무결성을 보장해야 한다[17].

안전한 통신 유형은 디지털 헬스케어 기기에 동일 사용자가 다중 접속이 되지 않도록 제한해야 하며 세션 연결 후 일정 시간 후 세션을 잠그거나 종료시켜야 하는 세션 관리, 통신 대상 기기 또는 서버와 통신방식을 고려하여 안전한 통신을 제공해야 하는 보안통신 보안항목 요구사항으로 세분화 된다.

물리적 보호 유형은 디지털 헬스케어 기기의 불필요한 인터페이스는 물리적으로 접근을 제한하여야 하고 기기에 대한 비인가 된 물리적 접근을 탐지하고 대응기능을 제공하여야 하는 인터페이스에 대한 물리적 보호 보안항목 요구사항으로 세분화 된다.

둘째, 데이터 보안을 위하여 디지털헬스 기기의 운영체제 및 프로그램의 지속적인 취약점진단 및 조치가 필요하다. 즉, 디지털 헬스케어 프로그램 개발시 소스코드 취약점이 존재하지 않도록 개발초기부터 시큐어코딩을 필수적으로 적용을 해야 되며, 중요 데이터 및 개인정보는 안전한 알고리즘(128bit이상 보안강도)으로 암호화하여, 저장을 해야 된다.

셋째, 전체적인 인프라, 데이터, 서비스에 대한 지속적인 정보보호를 위해서는 정보보호정책 및 지침 수립을 통한 관리적 보안이 필요하다.

즉, ISMS-P(Personal information & Information Security Management System) 인증을 통하여 디지털 헬스케어 서비스에 대한 안전성 및 신뢰성을 향상시키기 위한 절차와 과정을 체계적으로 수립, 문서화하고 지속적으로 관리·운영을 통하여 정보보호 목표인 정보의 기밀성, 무결성, 가용성을 실현하기 위한 일련의 과정 및 활동을 해야 한다[18].

현재 국내 스마트의료 보안을 정보통신망법(제13520호)에 따라 상급 종합병원 43개 정보보호관리체계(ISMS) 인증 의무화가 시행되고 있다. 따라서 지정 병원들은 정보보호관리체계 인증을 위한 보안강화를 위해 최선을 다하고 있다[19].

이상과 같이 디지털 헬스케어에 대하여 안전한 서비스를 위해서는 계층별 차세대 정보보호체계 수립을 해야 한다. 서비스는 물론 기기 부문에서도 초기 개발과 시스템 구축 시 안전하고 안정적인 사용을 위하여 정보보호 부문을 필수 단계로 적용하여야 하며, 각 부문별 통신, 시스템, SW 부문에서 인공지능 머신러닝 기법을 적용한 차세대 방화벽 설치, 서버보안, 단말기보안 등의 정보보호솔루션 구축뿐만 아니라, 최신 ICT 서비스 환경변화에 따른 위협분석 후 그에 따른 대응방안을 적용하여 디지털 헬스케어 차세대 정보보호체계수립이 필요한 것이다.

IV. Conclusions

코로나19의 영향으로 비대면 진료서비스 등의 디지털 헬스케어 서비스가 확대가 되어가고 있다. 특히, ICT인프라 및 기술을 사용하고 있어서, 항시 사이버공격의 대상이 되어가고 있다. 이에 현재의 대응방안은 방화벽(FireWall)을 통한 단순 네트워크 보안만 되고 있는 문제점이 있다.

본 연구는 디지털 헬스케어의 개요 및 핵심기술에 대한 이해와 인공지능, 빅데이터, 클라우드, 사물인터넷, 원격의료 등 ICT와 융합된 디지털 기술을 통한 건강관리 및 의료서비스가 확대되고 있는 시점에서, 디지털 헬스케어 기기 및 데이터를 대상으로 예상되는 DDoS 공격, 랜섬웨어 공격, 악성 이메일 공격, 기기 제어권 침해 등의 사이버공격으로 예상되는 의료, 개인정보 유출, 서비스 정지, 인명피해를 사전에 방지하기 위하여, 차세대 인공지능 애플리케이션형 정보보호 솔루션 구축과 지속적인 관리 및 운영을 위한 차세대 정보보호체계 수립을 제안하였다.

본 연구의 학문적 및 실무적 시사점을 제시하면 다음과 같다.

첫째, 디지털 헬스케어 서비스에 사용되는 인프라에 대한 정보보안이다. 디지털 헬스케어서비스에 필수적으로 사용되는 첫 번째, 기기가 스마트폰, 노트북, 컴퓨터...등 의 기기이다. 이러한 기기를 운영하기 위한 윈도우, 리눅스, 안드로이드와 같은 운영체제는 기술적으로 취약점을 가지고 있으며, 기기 간에 통신을 위한 인터넷 등의 통신망도 취약점을 가지고 있다는 것을 파악하였으며, 이에 대응방안으로 네트워크 보안을 위하여 인공지능 머신러닝 기법을 적용한 차세대 방화벽의 설치와 안전한 암호화 통신적용 및 기기인증 및 접속관리를 위하여 계정관리와 통합로그시스템의 적용을 제시하였다.

둘째, 디지털 헬스케어에 사용되는 데이터에 대한 정보보안이다. 디지털 헬스케어에 사용되는 의료정보, 민감정보, 개인정보와 같이 유출시 많은 피해가 예상되는 데이터이므로, 데이터 저장 및 전송 시 암호화 적용, 프로그램 개발시 소스취약점 진단 및 조치, 데이터 훼손 및 유실에 대비한 백업과 복구를 제시하였다.

셋째, 디지털 헬스케어 서비스를 위한 기기, 데이터, 통신망 등의 ICT 인프라에 대하여 취약점분석 및 제거를 통하여 안전한 환경을 지속적으로 유지하려면, ISMS-P, ISO27001 인증과 같은 인증제도를 도입하여 정보보호체계 수립, 정보보호 구현 및 운영, 모니터링 및 검토, 정보보호체계 유지 및 개선을 통하여 일시적이 아닌 지속적인 차세대 정보보호관리체계 수립이 필요하다고 제시하였다.

다만, 본 연구의 한계점은 차세대 정보보호체계 수립을 위하여 인공지능 머신러닝 기법을 적용한 차세대방화벽구축, 데이터암호화, 정보보호관리체계 운영에 대하여 효과측정에 대한 객관적인 지표의 제시와 전체 정보보호 상황을 통합관리하는 방안에 대한 연구가 부족하다고 판단된다.

향후 연구는 디지털 헬스케어 차세대 정보보호체계 수립 이후 정보보호 대응효과에 대한 객관적인 지표와 효율적인 정보보호 통합관리를 위한 정보보호 통합관리방안에 대하여 연구가 필요할 것으로 판단된다.

REFERENCES

[1] T. K Lee, "Digital Healthcare Research Trend based on Social Media Data",The Journal of the Korea Contents Association, Volume 20, No3, pp.515-526, Mar 2020

[2] E. Lee, S. K. Kim. “Digital Healthcare Innovation Trends and Policy Implications, Science & Technology Policy“, Vol48, pp.1-31. 2018

[3] J. M. Ahn, "Comparative Analysis of the Economic Ripple Effect of the Digital Healthcare Industry and the Telemedicine Industry",The e-Business Studies, Vol.22, No.5, pp. 15-25, Oct. 2021.

[4] H.S. Yang "IT Risk & Security Study on the Methods of Security and Quality Evaluation of smart Healthcare System", Korea Digital Policy Society Vol. 15 No. 11 pp.251-259, Nov.2017

[5] MinistryofFood and Drug Safety,"New concept medical device outlook analysis report", JinhanM&B, pp.1-126, Feb. 2017.

[6] D. H. Noh, J.Y. Bae, and, I.K Shin,"The Technology Trands of Digital Healthcare", Journal of Electrical Society, Vol 072,pp.225-226, Jul. 2021.

[7] S. H. Kim, D.Y. Jung,"ICT convergence-based non-face-to-face healthcare technology trend", Journal of the Korean Telecommunications Society, Vol37 No.9, pp.77-84, Aug. 2020

[8] 4th Industrial Revolution Committee, "My Health Way (My Data in the Medical Field)Introduction", pp4, 2021.

[9] Y. S. Choi, "Digital Healthcare (the future of healthcare)", Cloudnine, pp.1-735, 2020.

[10] M. J. Park, "The future of the healthcare industry?American bigtechcompany",https://www.dttoday.com/news/articleView.html?idxno=88997, Sep. 2021.

[11] S. G. Lee, “Global digital healthcare technology trends and challenges”, http://www.iitp.kr , Dec. 2017.

[12] J. Y. Ko, S. G. Lee, and, J.W Kim, "Technologies Analysis based on IoT Security Requirements and Secure Operating System",Journal of the Korean Contents Association, Vol.18, No.4, pp. 164-177, Apr. 2018.

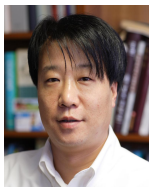
[13] MEDBIZ Project, http://board.wmit.or.kr/bbs/board.php , 2021
[14] KISA,“ Digital healthcare Security Model ”, Dec. 2020
[15] Y. J. Song, K. Y. Park, "Security/Privacy Requirements for Medical Data Sharing and Utilization Services",Journal of Information Security(KIISC), Vol20, No 3,pp. 90-96, Jun. 2010.
[16] K. H. Kim, I. H. Kim, and Y. T. Shin,"Research on digital health care and information security", Proceedings of KSCI Conference 2021, Vol. 29, No. 2, 219-220, July. 2021.
[17] D. H. Seo, J. M Baek and Y. H Moon,"Prevent Illegal Access Control for Secure Healthcare System", Journal of Electrical Society, Vol.59, no.3, pp.657-663, 2010.
[18] H. K. Gong, H. J. Geon, and S. H. Lee,"Research Trends in Economic Effects of Information Security Certification: Focused on the ISMS (Information Security Management System)",Journal of the Korea Institute of Information Security and Cryptology v.26 no.3 , pp.821-835, 2016.
[19] D. W. Kim, K. H. Han, "Recent Research Trends for Response to Security Threats in Smart Medical Environment"Journalofthe KoreanTelecommunications Society,Vol 35,No.2, pp.95-99, Jan. 2018.

Authors

Ki-Hwan Kim graduated from Soongsil University, Department of Information Security, Master's degree and complted Ph.D. in Computer Engineering. He is currently working as a Senior Researcher at Korea Electronics and Telecommunications Research Institute (ETRI) He is also am expert member of Korea Hacking Security Association. He also works as ISMS-P, ISO27001,27017&8 Certification Auditor, and obtains AI, IoT information security research and information security certification. He has Interest in institutional research.

Sung-Soo Choi received Ph.D. degrees in IT Policy Management from Soongsil University, Korea. Dr. Choi is currently working as an adjunct professor in the Inha Technical College, Incheon.

Il-Hwan Kim KIM received B.S. degree of Electronics at Korea Transportation University. Currently he is a Chief Researcher at Wonju Medical Device Techno Valley He also worked at Information Security Planning Department at Korea Regional Information Development Institute.



Yong-Tae Shin received Ph.D. degrees in Computer Science from University of Iowa He is currently working as a Professor of Department of Computer Science, Soongsil University. He is also a Director of Soongsil University Spartan SW Education Center.