The Journal of the Convergence on Culture Technology (JCCT)
Vol. 9, No. 4, pp.699-706, July 31, 2023. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2023.9.4.699

JCCT 2023-7-85

사물인터넷과 융합한 헬스케어 시스템에서의 보안 이슈 및 취약점 분석

Analyses of Security Issues and Vulnerability for Healthcare System For Under Internet of Things

김정태*

Jung Tae Kim*

요 약 최근 들어 다양한 기술의 융복합화로 인하여, 제4차 산업혁명이 이루어지고 있다. 그 대표적인 기술이 사물인터넷을 이용한 헬스케어 시스템 분야이다. 기존의 헬스케어 시스템을 기반으로, 모바일 환경하에서 각각의 장치. 센서, 프로토콜 등을 통해, 환자의 진료 상태 및 기록을 관리할 수 있는 응용 분야로 발전되고 있다. 특히 사물인터넷에서 응용되는 시스템의 경우, 디바이스들의 제한된 자원인 메모리 용량 부족, 컴퓨팅 연산 능력의 저하, 저전력 기술 등의 특징을 가지고 있다. 데이터 보호를 위하여, 이러한 특징 때문에, 기존의 암호화 알고리즘을 사용할 수 없게 된다. 따라서, 본 논문에서는 사물인터넷에서 발생할 수 있는 보안 이슈를 해결하기 위한 고려 사항 및 헬스 시스템의 구조를 분석하고자 한다. 현실적으로 각종 센서, 장치들이 기존의 기법을 통하여, 보안을 구현하기에는 안전하지 못하다. 보안의 위협 및 공격 요소를 살펴보고, 이를 해결할 수 있는 방법을 분석하고자 한다.

주요어 : 헬스케어 시스템, 사물인터넷, 취약성, 보안, 센서 노드, 취약점

Abstract Recently, the 4 generation industry revolution is developed with advanced and combined with a variety of new technologies. Conventional healthcare system is applied with IoT application. It provides many advantages with mobility and swift data transfers to patient and doctor. In despite of these kinds of advantages, it occurred security issues between basic devices and protocols in their applications. Especially, internet of things have restricted and limited resources such as small memory capacity, low capability of computing power, etc. Therefore, we can not utilize conventional mechanism. In this paper, we analyzed attacks and vulnerability in terms of security issues. To analyze security structure, features, demands and requirements, we solve the methods to be reduced security issues.

Key words : Healthcare system, Internet of things, Vulnerability, Security, Sensor node

Ⅰ. 서 론

2000년대 접어들어, 정보통신 및 반도체의 소형화 기술로 인하여, 비약적인 기술 발전을 통하여, 모든 통신 및 네트워크들이 초연결성을 가지도록, 융복합화 기술을 통하여 제4차 산업혁명으로 진행되고 있는 실정이다. 이러한 개방형 환경하에서 유무선 통신망에서 정보보호를 위한 다양한 기술적인 메카니즘이 융합 및 복합

*정회원, 목원대학교 전기전자공학과 교수 (단독저자)
접수일: 2023년 6월 25일, 수정완료일: 2023년 7월 5일
게재확정일: 2023년 7월 10일

Received: June 25, 2023 / Revised: July 5, 2023
Accepted: July 10, 2023
*Corresponding Author: jtkim3050@mokwon.ac.kr
Dept. of Department of Electrical and Electronic Engineering, Mokwon Univ. Korea

화를 통하여 구현되고 있다. 일반적으로, 개방형의 망 구조에서는 다양한 종류의 망들이 연결되기 때문에, 각각의 망 구조에 적합한 암호화 기법 및 기술이 적용되고 있다. 결과적으로, 유선과 무선 통신망이 결합하여 연결됨으로 인해, 기존의 망 구조에서 적용되고 있는 암호 알고리즘의 구현 및 정보보호 시스템 구축 관련 기술들은, 현재의 응용 시스템 구조에서는 많은 문제점을 내포하고 있다. 이러한 문제들은 사물인터넷 망에서 초연결성을 위해 사용되고 있는 각종 센서들의 제한된 자원인 저용량의 메모리, 낮은 컴퓨팅 파워, 저전력 등의 특징을 가진다. 그러므로, 기존의 전통적인 보안 기법을 구현하기 위해, 제한된 자원으로 암호 시스템을 구현하면 많은 문제점을 야기 시킬 수 있다. 특히, 사물인터넷 망은 단일 센서 노드들의 연결이라기 보다는, 서로 다른 센서들의 초연결로 구성되어 있어, 각각의 센서들의 보안 취약점으로 인하여, 최적화된 보안 구조를 가져야 한다. 기존의 인터넷 망들은, 유선망을 기본 백본망으로 설치되어 있으며, 고도화 기술에 따라 유무선 통신망이 융복합화 하여 연결되고 있다. 따라서, 기존의 유선망에서 사용하던 헬스케어 시스템의 서비스 형태가, 무선망의 발전으로 인하여 환자의 개인 정보를 모바일 기술을 통하여, 더욱더 쉽게 접근할 수 있다. 특히, 최근 들어 무선 센서 통신망의 기술적인 발전으로 인하여, 모바일 센서 노드들은 특히 개인화되고, 스마트폰과 같은 중계기를 이용하여 게이트웨이 형태로 구성되어, 외부의 인터넷 망을 통하여 헬스케어 시스템에 접근하는 구조의 플랫폼으로 발전되고 있다. 사물인터넷 망을 활용함으로써, 개선된 기술, 효율성 및 이동성 등의 장점을 가지게 된다. 그러나 이러한 장점에도 불구하고, 네트워크를 구성하는 기본적인 장치 및 노드들 간의 프로토콜 및 플랫폼 등에서 보안 취약점이 발생하게 된다.

II. IoT 관련 연구

IoT 환경하에서, 헬스케어 시스템을 연동할 경우, 다양한 장점을 가지게 된다. 병원의 다양한 시설을 위한 보안 및 유지보수, 최적화된 질병의 관리, 복잡화된 여러 의료 서비스 분야에서 최적의 조건을 유지하게 만든다. 이러한 최적의 의료 정보들은, IoT에 기반한 장치와 의료 장비들을 통하여 채집된 의료 정보의 무결성을 지원한다. 이러한 기술을 통하여 의료진과 환자들 모두 더 나은 진찰 환경을 조성하고 병원의 시설 편의와 개인적인 의료 서비스를 향상시킨다. 이러한 서비스는 메디컬 장비들을 언제, 어디서나, 인터넷을 통하여 실시간으로 접속 가능하다. 이러한 스마트 환경하에서의 헬스케어 시스템들은 기존의 환경에 비해, 유지보수가 쉬우며, 임베디드 형태의 센서 장치들을 사용하여 모니터링을 할 수 있다. 특히 의사, 간호사 등의 직접적인 방문을 통하지 않고도 환자의 건강 상태를 모니터하고 지원할 수 있게끔 해준다. Khaled H. Almotairi은 헬스 도메인과 보안 문제를 연계한 사물인터넷의 응용 시스템에 대해서 비교 분석하였다 [1]. Fatma Alshohoumi은 IoT 구조의 보안 및 프라이버시 이슈에 대한 문제점을 분석하였다 [2]. Jindong Zhao은 블록체인과 프러이버시 컴퓨팅 기술에 기반한 헬스케어 시스템을 위한 웨어버러블 메디컬 센서에 대해서 기술하였다 [3]. Mouza Bani Shemaili 등은 IoT 응용 시스템의 구현을 위한 암호 알고리즘으로, 경량 구조의 하이브리드 암호화 알고리즘을 제안했다. 그는 암호화 강도를 높이기 위하여, 다양한 구조의 시프트레지스를 사용하여 비선형성 구조를 결합하여, 안정성을 높이고 그 복잡도를 분석하였다 [4]. Antonio F 등은 IoT에서의 보안과 프라이버시를 위하여, 공개키 기반의 분산 접근제어 기술을 제안하였다. 특히 이러한 보안 문제점을 해결하기 위해서, 초경량화 보안 프로토콜, 암호 알고리즘의 설계, 하드웨어, 임베디드 소프트웨어의 설계 기술에 대해 분석하였다 [5]. 개방형 네트워크 망에서의 주된 보안의 문제점의 하나는 통합 보안 메카니즘이 요구되며 다음과 같은 특징을 가지고 있다.

- 개방 네트워크에서 무선 네트워크의 형태는 다양성을 가진다.
- 각각의 네트워크에서는 독자 방식에 맞는 보안 메카니즘으로 구성되고 있다.
- 고성능과 고비도의 보안을 위해서는 최적의 보안 프로토콜 및 독창적인 보안 메카니즘이 요구된다.
- 다가올 미래에는 다양한 응용 시스템에 적합한 융합 보안 메카니즘과 이를 위한 여러 가지의 프로토콜의 융합이 보편화될 것이다. 따라서, 본 논문에서는 이러한 사물인터넷 환경하에서 헬스케어 시스템을 구축하기 위한, 보안 이슈 및 취약점을 분석하는데 목적을 두고 있다.

III. IoT 보안의 기술적 요구사항 분석

보안을 강화하기 위한 가장 쉽고 효과적인 방법의 하나는, 보안 절차를 검토하고, 요구되는 보안 사항을 최적의 조건으로 맞추는 것이다. 이러한 보안 절차는 기업과 조직의 내부의 자산을 외부의 위협으로부터 효과적으로 보호 및 방어할 수 있는 프로토콜을 설계하는 것이 최적의 조건이다. 보안을 위해 요구되는 사항으로는 하드웨어 측면에서는 물리적인 보안 조치와 방화벽을 예로 들 수가 있고, 소프트웨어 측면에서는 바이러스 백신, 시큐어 운영체계 등 다양한 기법이 존재한다. 특히, 보안 절차의 경우에는, 회사에서 데이터 및 시스템에 대한 직원들의 접근 제어와 관련된 정책 및 절차 구현이 포함된다. 특히, 기업의 정보 보안 체계를 관리하고, 설계 방법을 개선하고 평가해야 한다. 기업은 기존의 보안 정책이나 보안을 위한 여러 가지의 방법이 효과가 없거나, 효율적이지 않은 전략을 채택하는 경우가 가끔 있다. 예를 들어, 효율성을 높이기 위해 워크플로우와 시스템을 재설계할 수 있다. 여러 사람이 동일한 단계를 사용하여, 동일한 업무를 수행하는 경우, 해당 단계를 최적화하는 방법을 찾을 수 있다.

많은 사람이 다른 단계로 동일한 업무를 수행하는 경우, 적절한 프로세스가 없을 수 있다. 최적화를 이루기 전에 일관된 프로세스를 설정하는 것이 중요하며, 이해 관계자가 책임을 지고 작업이 진행되도록 프로젝트 관리 기법을 준용해야 한다. 보안 정책 및 절차를 위해, 회사의 보안 조치가 업계 표준에 따라 운영되고 있는지 확인하고, 보안 절차를 검토하여 비효율성을 식별하고 개선할 수 있는 변경 사항을 적용해야 한다. 일반적으로 사물인터넷이 발전함에 따라, 기존의 헬스케어 시스템과 융합을 하여 시스템을 구축하고 있는데, 또 다른 과제에 직면해 있다. 무단 감시 및 접근으로 인한 환자의 사생활 침해 문제가 주요한 대상이다. 유비쿼터스 센서노드에서는 종단간의 노드에서 데이터를 수집하여, 환자의 위치를 추적할 수 있고, 헬스의 정보를 모니터링 할 수 있다. 따라서, 개인의 의료 프라이버시 침해에 대한 우려가 나타나고 있으며, 의료계에서는 HIPPA를 통한 개인의료정보 이용에 대한 가이드라인을 규정하고 있다 [6]. 헬스케어 시스템의 보안 및 개인 프라이버시 문제는 새로운 기술로 해결할 수 있다. 따라서 본 논문에서는 환자의 생체 신호의 센싱, 센싱 데이터의 수집, 데이터의 분석 및 진단, 환자의 위치 추적을 포함하는 유비쿼터스 환경하에서의 헬스케어 시스템에 대한 보안 및 취약점을 분석하고자 한다. 환자에 대한 정보의 접근 및 환자 추적을 위해 RFID를 채택하고, PKI와 스마트 카드를 이용한 인증 및 접근제어 권한을 부여하는 방식이 사용된다 [7]. 1996년 미국 의회에서 제정한 HIPAA(Health Insurance Portability and Accountability Act)는 미국 의료 산업에서 제정된 법률이다. 이는 의료 품질의 향상을 위해서, HIPAA는 가입된 모든 조직 및 기구에서 엄격하게 준수해야 하는 기본적인 지침을 제공한다. 개인정보보호 규정은 환자의 이름, 주소, 전화번호와 같이 개인의 신분을 드러내는 건강 정보의 일부인 보호 대상 건강 정보의 사용 및 유출을 통제할 수 있는 기술을 제공한다. 유무선 통신 기술, 컴퓨팅 기술, 인터넷 기술의 발전으로 인하여, 헬스케어 시스템을 IoT 기반으로 대체하여, 작업의 효율성 증가, 저장 비용의 감소, 의료 정보 오류의 감소, 데이터의 가공 및 공유 등을 통하여, 환자와 의료 관계자에게 많은 편의성을 제공하고, 삶의 질을 개선시키고 방법으로 전개되고 있다. 그러나, 헬스케어 시스템에서의, 개인정보, 프라이버시 문제 및 각각 시스템 상에서의 네트워크, 센서, 프로토콜 등의 취약점으로 인해 많은 문제가 발생하게 된다. IoT의 보안 위협 요소로는 물리적인 위협 요소로는 센서, 장치, 프로토콜, 디바이스 등의 하드웨어 시스템과, 기기 혹은 센서의 오동작 및 악성 코드에 의한 갑작스런 시스템의 다운 등의 소프트웨어 문제로 인하여, 사람의 생명 및 자산을 위협하고 있다.

따라서, IoT 시스템에서 야기될 수 있는 이러한 문제점을 감소시키기 위한 보안기술이 필수 불가결하다. 따라서, 본 논문에서는 헬스 시스템에서의 디바이스, 네트워크, 서비스 영역에서 요구되는 보안 측면에서의 기술 및 요구 사항을 정의하고, 그 대책에 대해서 분석한다.

3.1. 디바이스 및 소자 관련 기술

IoT 장치, 센서 등의 제한된 메모리, 프로세서의 저성능, 저전력을 위한 암호 알고리즘을 SoC(System on Chip) 형태의 구현이 가능하고, 저용량의 시큐어 운영체계의 개발이 요구되어 진다. 또한 센서 노드 및 장치에 대한 보안성 강화를 위하여, 외부의 제 3자 및 비승

인자에 대한 접근 제한 및 데이터의 위변조를 방지하는 기술을 포함해야 한다 [8].

1) 저사양의 소자의 해킹 문제

제4차 산업혁명을 주도하고 있는 사물인터넷은 각종 소자, 디바이스 및 센서들의 다양화와, 저사양의 하드웨어로 인하여 심각한 보안 사고의 취험에 노출되어 있다. 현재의 주요 보안 대상 분야는, 메모리의 크기, CPU의 컴퓨팅 능력, 전력 소모 등의 제한된 제원으로, 현재의 표준화된 암호화, 인증, 프로토콜을 구현하에는 취약점을 가진다. 따라서, 이를 문제를 해결하기 위한 대안으로 초경량화 모듈의 암호 엔진 및 새로운 구조의 알고리즘에 대한 연구가 진행되고 있다.

2) 디바이스, 소자, 장치, 기기 등의 취약점 증가

센서, 소자, 디바이스 등 부품의 종류가 다양화되고, 한정된 자원으로 인하여, 기존의 표준 알고리즘을 적용하기에는 많은 문제가 발생한다. 따라서, 기존의 암호화 시스템에 대한 보안 업데이트 및 패치의 적용이 어려워진다. 따라서, 장치 간의 통신이 이루어질 경우, 정보의 유출을 탐지하기 위하여, 침임 탐지용 모니터링 기술 및 관제 기술 등의 새로운 융합기술이 요구된다. 현재의 원천 기술로는 제한된 기술로 융복합적으로 구현해도 보안의 취약성은 감소가 되지 않고, 새로운 이슈들을 야기시킨다. 찌지에 선은 그의 논문에서 헬스 정보를 저장하기 위하여 블록체인에 기반한 기법을 제안하였다 [9].

3.2. 네트워크 보안 기술

상호 이기종의 기기들이 사물인터넷 통신을 기반으로 서로 간에 초연결성 구조의 네트워크로 일반적으로 구성된다. 다량의 기기들이 연결되어, 실시간의 이상 징후를 탐지 대응할 수 있는 신개념의 인공지능 기반의 탐지 기술 등이 필요하다. 현실적인 기술로는 다양한 매개체의 네트워크 간의 통신에서의 상호 비밀성 및 인증을 강화하기 위한 중간 매개 역할을 하는 게이트웨이(Gateway) 기반의 기술 개발이 반드시 요구된다.

1) 무선 센서 네트워크의 보안 취약성 증가

우리 주변 환경에서 보편적인 기술로 사용되고 있는 통신인 와이파이, 지그비, 블루투스 등의 네트워크 구조는 기존의 망과 연동함으로 비밀성과 인증성에는 저준위의 비도를 사용한다. 따라서, 고준위의 비도를 가진 알고리즘을 강화하기 위한 상호 인증 등의 고비도의 보안 레벨을 유지하기 어렵다. 외부에서 네트워크에 대한 트래픽 공격이 급증함에 따라, 가상화 클라우드 서비스를 통한, 좀비 컴퓨터의 확산으로 인하여, 각각의 센서, 디바이스, 장치 등에 악성코드를 감염시켜, 트래픽에 대한 폭발적인 공격으로 인하여, 네트워크의 다운 및 불안전 서비스를 가속화 한다.

2) 네트워크 장비의 보안성 강화 증가

많은 수의 이기종 간의 상호 연동 프로토콜에 대한 운영 기준을 정립하고, 저사양의 기기를 사용하는 통신망에 적용하기 위하여, 초경량의 고비도로 강화된 보안 알고리즘의 개발이 반드시 필요하다.

3.3. 플랫폼 및 서비스 관련

IoT 서비스 환경하에서, 최적화의 인증 기법 개발, 신개념의 프라이버시 보호 및 능동형 구조의 보안 솔루션의 개발이 필요하다. 이러한 요구 사항을 위하여, 많은 연구자들이 새로운 규격 및 사양의 강인한 구조의 프로토콜 및 각종 표준안을 작성하기 위한 연구를 진행하고 있다. 특히, 현재 응용 분야로써 스마트 홈 네트워크 및 헬스케어 시스템에 대한 연구를 집중적으로 하고 있다. 특히, 기존의 알고리즘을 응용하는 시스템에 최적화하기 위한 보안과 프라이버시에 대한 기술적인 문제가 선행되어야 한다. 특히, 스마트 헬스케어 시스템 및 의료 분야에서는 인간의 생명을 다루는 기기들이 몸에 내장되고 있어, 고가용성과 실시간성이 보장되어야 하고, 여러 종류의 접근 제어 기술이 선행적으로 개발되어야 한다 [10].

1) 인증 및 신뢰성 관리

기존 개방형 플랫폼의 경우, 각각의 기기들이 서로 다른 매개체를 이용하여 통신을 한다. 데이터를 주고받을 때, 오작동 등으로 인한 오류가 발생하고, 취약점이 또한 발생할 수 있다. 또한 각각의 에지단의 소자, 센서 및 디바이스가 수집한 데이터들을 중앙 집중 관리를 함으로 인하여, 사용자의 신원 정보 및 중요 정보가 유출될 위험이 한층 더 증가하게 된다.

2) 개인 정보 수집, 처리 및 관리

각각의 기기, 센서, 디바이스, 소자에 대한 정보 수집, 정보 처리가 선행된다. 수집된 정보에 대한 정보의 추적 방지 기술 및 개인 식별을 위한 정보의 취득을 위한 필터링 기술이 반드시 요구된다.

표 1. IoT의 핵심 기술
Table 1. Major Technology of IoT

IoT 핵심 기술	내용
암호 및 인증 기술	- 초경량/저전력, 키해킹 대응, 키은닉 및 키관리
프라이버시 기술	- 개인식별 추적제어, 프라이버시 레벨 제어 - 위험도기반의 빅데이터, 비식별화
네트워크 보안 기술	- 침해방지, 통신보안, 보안관제 및 보안관리 - 보안 게이트웨이
디바이스 보안 기술	- 저전력/고속 하드웨어 보안 모듈 - 디바이스 보안 및 시큐어운영체제, 기기간 원격 인증 접속제어

<표1>은 IoT의 응용분야에서 해결해야 할 보안의 핵심 요소를 나타낸다. 이러한 보안 프레임 설계는 다양한 보안 프레임 구조를 가지고, 암호화 및 각각의 메카니즘들 간의 융합으로 인하여 각각의 보안 정책에 의해 그 구성이 요구되어 진다. 이를 위해서는 전체 프레임워크 및 장치 수명 주기, 사용 용이성, 배치 용이성을 고려하여 시스템 관점을 고려하여 설계하여야 한다.

Ⅳ. 헬스 시스템의 설계

4.1. 시스템의 구조

기존의 인터넷 망으로 연결된 헬스 시스템은 이기종의 기기들에 센서들이 연결되어 있으며, IoT 기반의 헬스케어 시스템의 그 구성도는 (그림1)과 같다. 환자에 부착된 각종 센서들의 정보를 통신이 가능하게 하기 의한 매개체로, BAN(Body Area Network)와 스마트 폰을 이용하여 외부의 데이터를 접속 가능하게 한다.

외부 단말 기기인 모바일 폰과 인터넷 망을 통하여 내부의 병원 망과 연결하기 위한 게이트웨이를 설치하고, 헬스케어 시스템 내의 백본 서비스 망으로 구성되어 있다. 모바일 단말기는 대체로, 웨어러블 기기, ECG, 센서, RFID 태그 등으로 구성되어 있다. 게이트웨이(Gateway) 솔루션은 외부의 단말기와 각종 인프라를 IoT에 연결할 수 있는 핵심 기술을 제공한다. 일반적으로, 게이트웨이의 주요 기능으로는 네트워킹, 임베디드 제어, 응용 소프트웨어를 내장하고, 프로토콜을 통합하는 기능을 제공해야 한다.

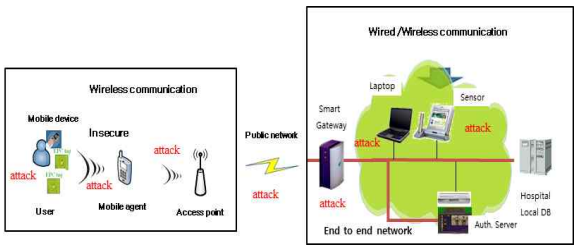

그림 1. IoT 기반의 헬스케어 시스템의 망 구조
Figure 1. Topology Architecture of Healthcare System Based on IoT

IoT 플랫폼 혹은 헬스 시스템의 기본적인 구성 요소로는 병원 내에서의 기기, 환자의 몸에 부착된 센서, 질병을 모니터링하는 휴대 전자기기 등으로 이루어져 있다. 특히, 진동 짜오는 그의 논문에서, 병원동 내에서의 환자의 의무 기록을 블록체인을 응용하여 프라이버시를 보호하는 기술을 제안하였다 [11].

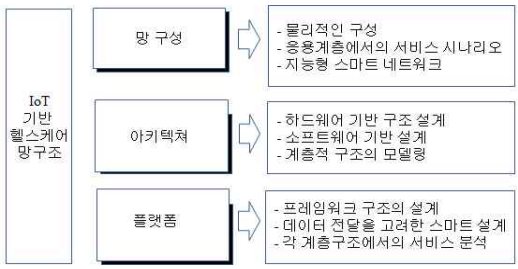

그림 2. IoT 기반의 헬스케어 시스템의 주요 구성도
Figure 2. Major Configuration of Healthcare System Based on IoT

(그림 2)에서 보는 바와 같이, 사물인터넷 기반의 MSN(Medical Sensor Network) 구조는 3개의 응응 부분으로 구성되고, 그 주요 특징은 다음과 같다. 주요 구성 요소는 보안 측면에서 보면, 외부 혹은 병원 내부 환자의 개인 정보와 통신 중에 발생하는 모든 데이터에 대한 데이터 보안 문제가 아주 중요한 이슈로 대두되고 있다. 일반적으로, MSN 네트워크에서의 개인 정보들은 MCN 내의 게이트웨이로 센서 정보들이 통합되어, 의사 등 의료인들의 단말기로 정보가 전송되는데, 이때 센서 노드에서의 취약점으로 인해 해킹의 위험에 노출

되어 있다. (그림 3)은 IoT 기반의 주요 계층 구조를 나타내고, 각 계층의 서비스를 설명하고, 이를 위한 기술을 나타낸다.

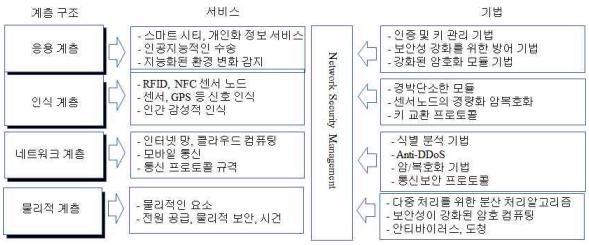

그림 3. IoT 기반의 헬스케어 시스템에서의 계층 구조
Figure 3. Hierarchical structure in Healthcare system based on IoT

4.2. 보안을 고려한 구조의 설계

환자의 개인 정보 및 프라이버시를 보호하고, 외부 및 제3자의 악의적인 공격으로부터, 자산을 보호하기 위해서는 모든 네트워크에서의 통신은 암호화가 필수적이며, 데이터의 무결성이 보장되어야 한다. 특히, 통신의 객체들은 안전한 키 교환을 통하여 상호 인증이 요구되며, 개선된 보안 메카니즘을 사용하여 구현되며 각각의 정보 전달 체계는 다음과 같다.

1) MSN에서의 센서 노드의 데이터 전송

에지 단에서 센서의 안전한 통신을 위한 보안 설정을 하고, 센서에서의 개별 정보는 제조사 혹은 메디컬 센터에서 직접 설정하여 구성되어야 한다.

2) MSN 게이트웨이의 정보 전송

외부의 인터넷 망을 통한 정보들이 헬스 시스템의 게이트웨이로의 접속을 통하여 시스템 내의 각종 단말기와 연결되기 때문에, 게이트웨이를 구현하기 위해서는 강력한 보안 알고리즘을 게이트웨이내에서 하드웨어 및 소프트웨어로 구성한다. 이때, 인터넷 접속을 통하여 접속되며, 표준 키 전송 프로토콜을 사용하여 안전한 채널을 구성해야 한다.

3) MSN 게이트웨이에서의 정보가 모바일 단말기로의 데이터 전송

센서 노드에서의 제한된 자원으로 인하여, 저용량의 하드웨어 및 메모리를 기반으로 경량화 키 교환 메카니즘을 사용하여야 하며, 취약점을 해소할 수 있는 새로운 기법이 요구된다.

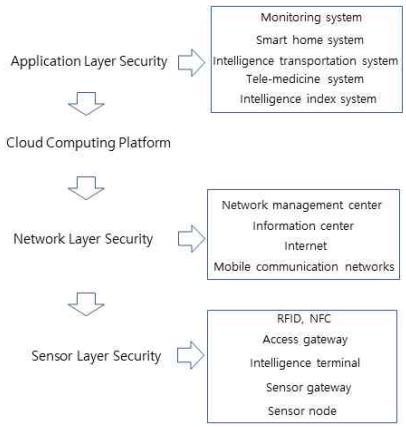

그림 4. IoT 기반의 각 계층의 보안 요소
Figure 4. Hierarchical Security Factor based on IoT

(그림 4)는 IoT에 기반한 각 계층의 구조에서 보안을 위한 요구사항을 나타내고 있다. 이기종의 기기가 상호 연결된 사물 인터넷 환경에서 실시간으로 이상 징후를 탐지하고 대응할 수 있는 인공지능 기반의 네트워크 보안 기술 개발되고 있다. 또한 이기종의 네트워크를 상호 연결하고 통신 보안을 제공하는 IoT 보안 게이트웨이의 개발이 많이 연구되고 있다. 특히, 악성코드의 감염을 탐지하고, 외부의 해킹으로 부터 운영체제 및 소프트웨어의 위변조 방지 기술 및 디바이스, 소자 등의 오작동으로 인한 시스템의 다운 등을 탐지 및 방지하는 기술이 내장되어야 한다. 또한, IoT 기기의 탈취 및 도난으로 인한 분실 및 해킹 및 악성코드, 멀웨어 등을 통한 악의적인 시스템의 성능 저하 및 불법 복제 등을 통한 중요 데이터의 유출을 방지를 위한 기술, 및 보안을 위한 임베디드 소프트웨어 및 하드웨어 기술이 요구되며, 다음과 같은 문제점을 해결해야 한다 [12].

1) 실시간 트래픽을 제어할 수 있는 모니터링 및 보안 관제 기술

2) 하드웨어적 보안 구현으로 고속의 암호와 및 고비도의 보안 적절성 해결 문제

2) 분산 시스템에서의 프로토콜을 위한 다중 처리의 분산 접근 방법 문제

3) 에지단의 노드에 대한 하드웨어적 보안 모듈 탑재 시의 안정성 문제

표 2. 유비쿼터스 헬스케어 시스템의 공격의 예
Table 2. Example of attacks model of ubiquitous healthcare system

에이전트	공격 유형
태그 및 모바일	도청, 트래픽 폭주, Replay 공격, 서비스부인 공격, 종단의 정보 센싱 기술, 환자의 상황 인식 기술, 위치 탐지 및 추적 기술, 프라이버시 기술
네트워크	관용 암호화 엔진 및 모듈, SSL 및 TLS 의 보안 프로토콜 기술, 센서 및 GPS 기반의 이동 통신 기술, 게이트웨이 기반의 네트워크 보안 기술
데이터 베이스	환자의 개인 의료정보, 환자 처방 기록, 데이터베이스 속성, 스키마 및 보안 기술
무선망 및 센서망	기밀성, 사용자 인증, 생체 인증, 디바이스 인증 디바이스 인증, 권한 부여, 물리적 보안, 센서 네트워크 보안
공격	도청, 트래픽 폭주 제어, 메시지 변조 및 무결성 문제, 재전송 공격, 서비스 부인 봉쇄 기술, 디바이스 및 각종 센서 오동작 여부

<표 2>는 IoT를 이용한 헬스시스템에서의 각 영역에서의 외부 공격의 유형을 나타낸다. 따라서, IoT 서비스를 위한 계층 구조의 보안 인프라가 요구되며, 특히 서비스의 연속성 운영을 위한 제어, 프로토콜, 암호화 엔진, 보안 모듈, 통신시스템에 대한 융합기술이 요구되며, 대표적인 고려 사항은 다음과 같다 [13].

▪ 소프트웨어 구현 시, 경박단소한 시스템 구현을 위해 임베디드 소프트웨어 구조의 보안 취약점을 검증하고, 표준 알고리즘을 구현하기 위한 시큐어 코딩 기술이 필요하다.

▪ 임베디드 시스템을 구현하기 위한 경량화 기술의 개발이 요구된다.

▪ 해킹 및 제3자로 부터의 위협 및 위험 요소를 제거할 수 있는 신개념의 기술이 필요하다.

▪ 암호화 기능을 내장한 기기에 대한 인증 및 강화된 알고리즘의 고비도의 성능을 확인하기 위한 성능 평가 및 품질 보증 기법 등이 필요하다.

V. 결 론

제4차 산업혁명의 발전으로 인하여, 사물인터넷을 기반으로 하여 네트워크들이 초연결성으로 인프라기 구축되고 있다. 이러한 사물인터넷을 응용한 시스템에서는 에지단에서의 노드가 제한된 자원으로 인하여, 저용량의 메모리, 저전력 등의 하드웨어 자원에서 물리적인 보안 취약성을 가지고 있다. 따라서, 본 논문에서는

표 3. IoT 보안에 대한 도전 문제점
Table 3. Simulation Parameters

IoT 보안 및 공격	- 대용량의 IoT 센서 - 내구성을 내장한 임베디드 시스템 - 약한 패스워드 - 제안된 제원 및 자원 - 빅 데이터 문제 - 노후된 보안 요소 - IoT 소자의 위협 - 위협 요소를 탐지 - 사용자 프라이버시 - 피싱 공격 - 빈번한 업데이트의 부족 - 접근 통제 및 인증 - 비신뢰 공격 탐지 - 저순위의 암호화 - 비밀 통신 - 봇넷의 증가

IoT의 기본 요소를 실장한 헬스케어 시스템의 기본적인 구조를 살펴보고, 각각의 구성 요소에서의 보안 취약점을 분석하였다. 이러한 분석을 통하여, 추후 융합 구조의 헬스케어 시스템을 구현할 경우, 외부의 공격에 대한 침해 사항을 사전에 방지할 수 있으며, 안전성 등을 확보할 수 있는 시스템을 개발하는데 도움을 준다.

References

[1] Khaled H. Almotairi, “Application of internet of things in healthcare domain”, Journal of Umm Al-Qura University for Engineering and Architecture volume 14, p.1 - 12, 2022. https://doi.org/10.1007/s43995-022-00008-8

[2] Fatma Alshohoumi, Mohammed Sarrab, Abdulla AlHamadani and Dawood Al-Abri, “Systematic Review of Existing IoT Architectures Security and Privacy Issues and Concerns“, International Journal of Advanced Computer Science and Applications, Vol. 10, No. 7, 2019, pp. 232-251. DOI: 10.14569/IJACSA.2019.0100733

[3] Jindong Zhao, Wenshuo Wang, Dan Wang, Xuan Wang and Chunxiao Mu, “ a wearable medical sensor assisted framework for health care based on blockchain and privacy computing“, Journal of Cloud Computing, Article number: 11:96 (2022). https://doi.org/10.1186/s13677-022-00373-8

[4] Mouza Bani Shemaili, Chan Yeob Yeun, Khalid Mubarak, Mohamed Jamal Zemerly. A New Lightweight Hybrid Cryptographic Algorithm for The Internet of Things, The 7th International

Conference for Internet Technology and Secured Transaction, pp. 87-92, 2012.
[5] Antonio F. Skarmeta, Jose L. Hernandez Ramos and M. Victoria Moreno, A decentralized approach for security and privacy challenges in the Internet of Things, 2014 IEEE World Forum on Internet of Things, pp. 67-72, 2014.
[6] By JeongGil Ko, et al, Wireless Sensor Networks for Healthcare, Proceedings of the IEEE, Vol. 98, No. 11, November, pp. 1947-1960, 2010.
[7] Shang-Wei Wang, et al, RFID applications in hospitals: a case study on a demonstration RFID project in a Taiwan hospital, Proceedings of the 39th Hawaii International Conference on System Sciences, pp. 1-10, 2006.
[8] Saad Khan, Simon Parkinson and Yongrui Qin, "Fog computing security: a review of current applications and security solutions", Journal of Cloud Computing: Advances, Systems and Applications, 6:19, 2017. DOI 10.1186/s13677-017-0090-3
[9] Zhijie Sun1, Dezhi Han1, Dun Li1, Xiangsheng Wang, Chin Chen Chang and Zhongdai Wu, "A blockchain based secure storage scheme for medical information", Journal on Wireless Communications and Networking, 2022:40, 2022
[10]Lihua Song, Xinran Ju, Zongke Zhu and Mengchen Li, "An access control model for the Internet of Things based on zero knowledge token and blockchain", Journal on Wireless Communications and Networking, 2021:105, 2021. https://doi.org/10.1186/s13638021019864
[11]Jindong Zhao, Wenshuo Wang, Dan Wang, Xuan Wang and Chunxiao Mu, "PMHE: a wearable medical sensor assisted framework for health care based on blockchain and privacy computing", Journal of Cloud Computing: Advances, Systems and Application, Vol.11, No.96, pp. 1-17, 2022. https://doi.org/10.1186/s13677-022-00373-8
[12]Saad Khan, Simon Parkinson and Yongrui Qin, "Fog computing security: a review of current applications and security solutions", Journal of Cloud Computing: Advances, Systems and Applications, 6:19, 2017. DOI 10.1186/s13677-017-0090-3
[13]Senthil Kumar, Preeti Mishra, Nour Moustafa and Rahul Chauhan, "A holistic survey on the use of emerging technologies to provision secure healthcare solutions", Computers and Electrical Engineering, Volume 99, 107691, 2022. https://doi.org/10.1016/j.compeleceng.2022.107691