The Journal of the Convergence on Culture Technology (JCCT)
Vol. 9, No. 3, pp.707-714, May 31, 2023. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2023.9.3.707

JCCT 2023-5-82

사물인터넷 기반의 스마트 홈 네트워크에서의 취약점 및 보안 이슈 분석

Analyses of Security Issues and Vulnerability for Smart Home Network based on Internet of Things

김정태

Jung Tae Kim

요 약 제4차산업혁명의 기반이 되는 사물 인터넷이 많은 시스템에 응용되고 있으나, 사물인터넷과 연결되는 다양한 종류의 센서, 에지 노드, 등과 같은 하드웨어 구조에 적합한 저사양의 메모리, CPU 연산능력 및 경박단소한 센서노드 등으로 구성된다. 따라서, 기존의 보안 알고리즘으로 저용량의 노드에 사용할 수 없어, 새로운 제한된 하드웨어 구조 및 초경량의 암호 알고리즘이 요구되고 있다. 본 논문에서는 사물인터넷(IoT)에 연결된 스마트 홈 네트워크에서 야기될 수 있는 취약점 및 보안 문제점을 분석하고, 외부의 공격에 대한 다양한 종류의 보안 이슈 문제를 해결하기 위한 방법, 다양한 종류의 디바이스 보호를 위한 정합기술, 안전한 보안을 위한 IoT(Internet of Things)에서의 요구사항 및 응용 방법에 대해서 분석하였다.

주요어 : 스마트 홈 네트워크, 보안, 취약점, 센서 노드, 사물인터넷

Abstract The Internet of Things, which is the key factor of the 4th industrial revolution, are apt to apply to many systems. The existing security mechanism cannot be realized with limited resources such as low capacity of devices and sensors. In order to apply IoT system, a new structure and ultra-lightweight encryption is required. In this paper, we analyzed security issues that can operate in Internet-based smart home networks, and to solve the critical issues against these attacks, technologies for device protection between heterogeneous devices. Security requirements are required to protect from attacks. Therefore, we analyzed the demands and requirements for its application by analyzing the security architecture and features in smart home network.

Key words : Smart home network, Security, Vulnerability, Sensor node, Internet of Things

Ⅰ. 서 론

최근들어, 통신기법의 발전, 반도체 기술의 혁신 등의 융합으로 인하여, 인터넷의 급속한 속도 향상으로 전개되고 있다. 이러한 융합기술을 기반으로, 모든 인터넷의 초연결성으로 인하여, 제4차산업혁명이 실현되고 있는 추세이다. 기존의 센서, 노드, 엔드 포인터의 포그 등의 디바이스 간의 연결을 통하여, 사물인터넷 환경으

*정회원, 목원대학교 전기전자공학과 교수
접수일: 2023년 3월 30일, 수정완료일: 2023년 4월 14일
게재확정일: 2023년 5월 8일

Received: March 30, 2023 / Revised: April 14, 2023
Accepted: May 8, 2023
*Corresponding Author: jtkim3050@mokwon.ac.kr
Dept. of Electrical and Electronic Engineering, Mokwon Univ, Korea

로 융복합되고 있는 실정이다. 그 대표적인 예인 스마트 홈 네트워크는 스마트폰이나 컴퓨터를 사용하여, 원격으로 사물을 제어하고 모니터링할 수 있도록 연결된 기기 및 가전제품들을 연결한 네트워크이다. 이러한 스마트 홈 네트워크의 개념은 집주인들에게 집안의 전자기기들을 더욱더 편리하고, 효율적으로 에너지를 관리하고, 안전하게 외부에서 통합 제어할 수 있는 기능을 제공하는 것이다. 하지만, 스마트 홈 네트워크는 보안과 개인정보 보호 문제를 많이 가지고 있다 [1]. 이들 기기들은 해킹이 되어, 비인가된 제3자에게 정보가 노출될 수 있으며, 이 기기들을 이용해, 다른 기기나 네트워크를 공격하는 위험도 존재한다. 그 대표적인 응용 분야가 스마트 홈 네트워크이다. 사물인터넷 기술을 통하여 집안의 가전제품을 제어할 수 있는 기술적인 혁신을 가져다 주었다. 현재, 집안의 많은 다양한 가전제품들은 제조 회사의 규격을 통하여 설계 제조되고 있다. 스마트 환경을 이루기 위해서는 모든 기기가 동일한 표준을 기반으로 설계가 이루어져야 한다. 현재까지는 주로 회사 자체의 기술로, 가전기기들이 각각의 통신 프로토콜과 사양을 통하여, 구현되고 있어, 독자적인 기술에 의해 시스템의 성능을 좌우하고 있다. 이러한 서로 다른 스마트 홈 기기를 통합할 수 있는 IoT 표준인 “매터(Matter)”가 2022년부터 본격적으로 모든 스마트 홈 네트워크의 기기와 서비스에 대한 표준을 위한 연구가 진행 중에 있다. 현재까지 스마트 홈 네트워크의 보안 분야는 여전히 심각한 문제를 내포하고 있다. 최근, 아파트 월패드 해킹사고와 가정용 CCTV 및 IPTV 등의 해킹 사고에서 볼수 있듯이, 가정 내의 모든 전자기기 제품과 네트워크의 연결에 많은 보안 문제점을 포함하고 있다. 가정용 공유기가 해킹을 당할 경우 모든 공유기에 연결되어 있는 모든 기기들의 통신이 유출될 수 있어, 사생활에 상당한 침해를 일으킬 수 있다. 현실적으로 각종 전자기기 자체의 제조과정에서의 미처 해결하지 못한 취약성도 존재하고, 발견하지 못한 취약점도 존재하므로 추후에 큰 피해를 가져올 수도 있다. 최근에 월패드의 해킹 사고로 신문 방송에서 홈 네트워크 보안에 대한 문제점을 많이 소개하고 있다. 기존의 홈 네트워크의 구조는 사용자가 외부에서 앱 등을 이용하여 중앙서버, 동 게이트웨이를 거쳐 본인이 해당하는 세대의 집에 접근하는 구조로 구성되어 있다. 특히 아파트 등의 공동 주택의 경우, 전체의 세대가 하나의 공용 네트워크 망에 연결된 구조로 이루어짐으로 인해, 한 세대가 해킹되면 다른 모든 세대에 까지 그 취약성으로 인해 피해를 보는 구조로 되어 있다. 일반적으로 스마트 홈 네트워크는 주로 인터넷 망을 기반으로 연결되어 외부에서의 접근 경로가 다양하여, 보안적인 취약성이 증가하게 되었다. 이에 따른 기본적인 문제 해결책으로 기존의 아파트의 세대별 네트워크 망을 물리적 혹은 논리적으로 분리해야 한다는 방향으로 접근하고 있다. 망 분리만을 통하여서도 기본적인 보안 취약점 중 일부분만을 해결할 수 있어, 단말기 간 기기의 통신을 위한 데이터를 암호화하거나, 각각의 세대별 단말장치 등을 인증하는 다양한 방법의 해결책이 제시되고 있다. 현재 진행 중인 매터 표준 기술을 준수하는 기기들은 강력한 인증서 관리 기술을 적용함으로 인해 외부의 해킹에는 비교적 안전한 편이다. 이러한 표준화 기술을 통하여, TPM(Trusted Platform Module), SE(Security Engine) 등과 같은 안전한 하드웨어에 인증서를 저장하는 방법을 취하여, 데이터의 안전한 전송과 데이터의 저장 시 암호화 기술을 통해 데이터를 암호화하기 때문에 인증서의 탈취 및 데이터의 유출을 막을 수 있다 [2]. 메타의 비표준 기기가 허브 혹은 게이트웨이를 통해 매터 표준 기기와 통신을 할 경우라도, 비표준 기기의 해킹을 통해, 각가의 허브 등을 중간 매개체로 하여 데이터를 탈취할 수 있는 상황이 발생할 수 있다. 스마트 홈 네트워크에 연결되는 수많은 다양한 기기들이 존재하기 때문에, 다양한 종류의 펌웨어, 운영체계, 하드웨어와 연관된 취약점을 관리하기는 매우 현실적으로 어려운 실정이다. IoT(Internet of Things) 환경에서 가장 많이 발생하는 보안적인 위협요소는 허가하지 않은 제3자가 무단적으로 기기 등에 접속하는 것과 각종 기기 등의 취약점으로 인해 해킹을 당하는 경우로 생각해 볼 수 있다. 따라서 본 논문에서는 현재까지의 보안 및 취약점 관련 연구를 분석하여, 사물인터넷 기반의 스마트 홈 네트워크의 구조를 알아보고, 그 취약점을 분석하여, 안전한 보안 대책을 수립하는데 도움을 주고자 함을 목표로 하고 있다.

II. 관련 연구

일반적으로 IoT 기반의 스마트 홈 네트워크는 기기의 저전력, 저사양, 연산능력 등의 제한된 자원으로 인

하여, 기존의 암호학적 기반 기술을 적용하기에는 많은 문제점을 내포하고 있다. 따라서 많은 연구의 주제들은, 주로 보안 취약점 분석 및 위협 요소 등을 해석하는 데 주안점을 두고 있다 [3]. Tommaso 등은 스마트 홈을 위한 보안성이 향상된 프레임워크인 “Network Sentiment”를 제안하였는데, 그는 사용자가 인식할 수 있는 위험 레벨에 따라서, 스마트 홈 네트워크 보안 레벨을 정적으로 적용할 수 있는 방법을 제안하였다 [4]. Talal A. 등은 사물인터넷에 기반한 스마트 홈 네트워크 환경에서의 사이버 공격, 위협 요소 등에 대해 분석하고 그 해법을 제시하였다. 특히 주요 취약점을 발생시키는 요소로, 이기종의 기기 접속, 오래된 프로토콜, 강력하지 않은 암호화 기술, 제한된 저장 메모리 용량과 저사양의 CPU, 보안에 취약한 기존의 프로토콜, 저강도의 인증 기술 등을 제시하였다 [5]. 박중오는 클라우드 서비스를 기반으로 하여, 스마트 홈 네트워크 환경하에서 비밀성을 보장하는 데이터 통신을 위한 메시지 통신 프로토콜을 설계하였다. Mamun Abu-Tair는 기존의 시스템을 위한 보안성을 평가하기 위해, 기존 무선 네트워크 환경에서 응용하는 표준 알고리즘인 WPA2 및 AES와 SSL/TLS 및 WPA를 상호 비교 분석하여, 기존의 공격 방법 및 취약점을 기초로 하여 보안강도의 안전성을 분석하였다 [6]. 결과적으로, 많은 연구자들은 802.15.4 기반의 대표족인 프로토콜인 CoAP(Constrained Application Protocol), MQTT(Message Queue Telemetry Transport)와 IPv6 (6LoWPAN) 대역에서의 저전력 WPAN(Low Power Wireless Personal Area Networks) 등을 응용하여 구현하고 있다 [7]. Kozlov 등은 스마트 홈의 서로 다른 환경하에서 보안 위협 요소 및 프라이버시에 대해 분석하였으며, 특히 보안, 프라이버시, 제3자 인증과 관련된 프라이버시 제어 기법 및 스마트 홈에서 소비된 에너지에 대한 분석을 통하여 안전한 망에 대한 위협 요소의 레벨을 정하여 분석하였다 [8].

III. 스마트 홈 네트워크의 구조

일반적인 홈 네트워크의 구조는 기존의 단독 주택 혹은 아파트와 같은 구조에서는 각종 전자기기 등은 독자적으로 운영되는 구조로 되어 있다. 그러나, 스마트 홈 네트워크의 경우 (그림1)에서 보는 바와 같이, 댁내의 전자기기들이 외부의 모바일 폰을 통하여 직접적으로 제어될 수 있는 환경으로 인하여, 보안 취약점에 많이 노출되는 구조로 구현되어 있다. 따라서, 본 논문에서는 이러한 취약점을 해소하기 위하여, 댁내 망과 외부망을 분리하는 구조로 댁내에 진입 시 내부의 게이트웨이를 통하여 댁내의 모든 전지기기 및 센서 등을 제어할 수 있는 이중 구조를 제시하고 다양한 종류의 취약점과 공격 요소에 대해 분석하였다.

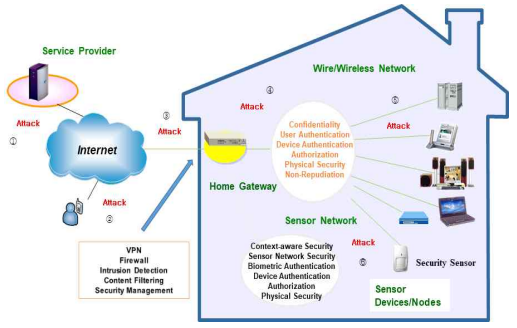

그림 1. 스마트 홈 네트워크의 기본 구조
Figure 1. Basic Architecture of Smart Home Network

일반적으로 안전하고 익명성을 보장하기 위한 통신망을 구성하기 위해서는, 정보보호의 5대 원칙인 보안 메카니즘의 기밀성(Confidentiality), 무결성(Integrity), 상호 인증(Mutual Authentication), 가용성(Availability), 익명성(Anonymity) 등을 반드시 보장해야 한다. 따라서 이러한 사물인터넷 구조의 환경하에서는, 다양한 이기종의 기기 및 센서 노드들을 연결하기 위한 프로토콜의 변환 등을 위한 구현이 필수불가결하다. 따라서, 유선망과 무선망의 통합 환경하에서는. 특히 무선 및 모바일의 경우, 유선에 비해, 무선의 특징적인 문제점으로 인하여, 통신망에서 취약성이 발생할 수 있다. 이에 대한 최적화된 보안 구조를 먼저 분석하여야 하며, 그 대표적인 보안 요구의 고려사항 및 공격은 요소들은 <표1, 2>와 같이 기술된다 [9]. Saeid Pirasm는 그의 논문에서 스마트 홈에 대한 사회적인 이슈에 대해서 정의하였다 [10].

일반적으로 암호 알고리즘으로 핵심적으로 구현하기 위해서는, 주로 블록 단위로 암복호화를 처리하는 블록

암호(Block cipher)와 단위 비트별로 암복호화를 처리하는 스트림 암호(Stream cipher) 방식을 주로 사용하는데, 그 대표적인 방식은 다음과 같다.

- 블럭 암호화: Blowfish, AES128-CBC and AES256-CBC.
- 스트림 암호화: Chacha20, AES128-CTR, AES256-CTR and DES3.

그러나, 스마트 홈 네트워크와 같이 사물인터넷의 에지 혹은 센서 단의 데이터 보호를 위해서는 경량화 혹은 초경량화의 암호화 알고리즘의 적용이 요구된다. 특히, 다음과 같은 표준 방식인 ISO/IEC 29192-3:2012 Lightweight Cryptography Standard에 의해 구현되고 있으나, 제한적인 자원에 의해 취약성을 여전히 내포하고 있다 [11].

표 1. 보안 요구사항 및 보안성 쟁점 도전
Table 1. Security requirement and Security issue challenges

보안 요구사항 (Security requirement)	보안적인 도전(Security challenges)
- 비밀성(Confidentiality) - 무결성(Integrity) - 인증(Authentication) - 가용성(Availability) - 부인봉쇄 (Non-Repudiation) - 인가(Authorization) - 견고성(Resiliency) - 고장방지능력 (Fault tolerance) - 자기복원력(Self-recovery and management)	- 계산적인 제약(Computational limitation) - 메모리 제약(Memory limitation) - 에너지 제약(Energy limitation) - 이동성(Mobility) - 축소성(Scalability) - 다양한 통신 미디어 (Communication media) - 디바이스의 다양성 (Multiplicity of devices) - 동적인 망구조 (Dynamic network topology) - 다중의 프로토콜 (Multi-protocol network) - 동적인 보안 갱신 (Dynamic security updates) - 물리적인 저항성 (Tamper-resistant packages)

Ⅳ. 스마트 홈 네트워크 환경하에서의 주요 보안 요구사항

일반적으로, 외부에서 스마트 홈 환경에 접근하기 위해서는, 휴대폰, 모바일 등의 단말기를 사용하여 개별의 디바이스들에 접근을 주로 하고 있으며, 각각의 디바이스 및 센서 노드에 대한 취약점이 발견되기 쉽다. (그림2)는 스마트 홈 네트워크에서 발생할 수 있는 취약점에 대한 대표적인 공격들을 소개하고 있다. 스마트 홈 네트워크의 플랫폼을 구성하고 있는 각각의 영역에 대한 취약점으로 현실적으로 모든 것을 해결하기에는 기술적으로 많은 어려움을 가지고 있다. 사물인터넷 환경에 기반한 스마트 홈의 구현 시, 센서 노드의 저사양, 저전력 및 메모리의 저용량 등으로 기존의 암호 알고리즘을 구현하기에는 현실적으로 불가능하며, 이로 인한 취약점이 현존하게 된다. 따라서, 현재에는

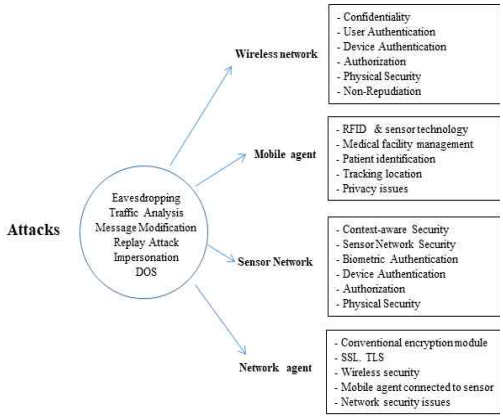

그림 2. 스마트 홈 네트워크에 대한 다양한 공격
Figure 2. A Variety of Attacks on Smart Home Network

표 2. 스마트 홈의 특징 및 정의
Table 2. Definition and Characteristics of smart homes

Definition	Characteristics of smart homes
Technology	Sensors
	Devices
	Integrated systems
Services	Control/Monitor
	Energy management
	Support and assist
	Anticipate and respond
Users needs	Cost-efficiency
	Comfort
	Emotional
	Security
	Health care
	Quality of life
	Sustainability

주로 계산량이 적고 기능이 작은 경량의 보안 알고리즘을 구현하는 방법으로 연구가 진행되고 있다. 일반적으로, IoT(Internet of Thiongs) 시스템은 이기종, 리소스의 제약 및 동적 환경과 같은 기존의 시스템 구현

시의 요구사항이 선행적으로 분석되어야 한다. 따라서, 네트워크, 클라우드, 사용자, 공격자, 플랫폼 및 서비스 분야에서 각각의 보안 요구사항이 선결적으로 분석 및 해결되어야 한다. 그러나 여전히 암호학적인 부문에서 상호 간에 보안적인 이슈 및 문제점을 가지고 있다. 특히 사물인터넷을 통한 통신 연결의 경우, 기존의 암호학적인 알고리즘을 사용할 경우, 구현할 수 있는 자원인 CPU, 메모리 등의 제한적인 사양으로 인해 경량화된 보안 알고리즘을 통하여 구현하여야 한다. 그러나

표 3. 보안의 정의와 관련된 스마트 홈의 특징
Table 3. Characteristics of smart homes related to definition

Definition	Characteristics of smart homes
Privacy and security	Smart systems for surveillance
	Smart system for detection
	Smart system for identification
Reliability	Smart system for forecasting emergencies
	Smart system for remote control devices
	Smart system for environmental situations
	Privacy protection
Satisfaction	Safe internet connection
	Reducing energy consumption
	Easier access to services
	Better education
	Increasing the health of residents
Trust on controlling devices	Operation of different devices with each other
	Owners ability to change smart device settings

제한적인 자원으로 인한 취약성은 여러 가지의 형태로 해결해야 할 문제점으로 남겨져 있다. 특히, 무결성으로 인한 정보의 왜곡, 데이터의 유출로 인한 개인 사용자의 프라이버시와 같은 보안성 문제의 위협이 항상 존재한다. 특히 외부의 해킹 공격으로 인해, 재전송 공격, 스푸핑, 중간자 공격, 스니핑과 같은 다양한 알려진 공격기법에 노출되고 있으며, 알려지지 않은 무수한 공격에는 여전히 취약하다 [12]. <표3>은 대표적으로 고려해야 하는 보안 문제, 신뢰성 문제, 효율성 문제, 제3자 인증 문제 등의 사항을 만족할 수 있도록 고려해야 한다. Nikos Komninos 등은 스마트 그리드 응용 시스템에서의 보안 문제 및 대책을 기반으로 분석하여, 스마트 홈 네트워크에서의 보안 문제점에 대해 분석하였다. 그는 스마트 그리드 환경에서의 스마트 홈 시스템에 대한 가장 대표적인 위협 요소 등을 분석했으며. 특히, 스마트 홈과 관련된 보안 대책을 다음과 같이 요약하였다 [13].

1) 비밀성과 보안(Confidentiality and privacy): 대칭/비대칭 암호화 알고리즘, 영지식 증명 시스템 및 데이터 난독화 문제

2) 무결성(Integrity): 암호화 해싱 기술, 디지털 워터마킹, 타임 스탬프, 세션 키 및 시퀀스 번호.

3) 인증(Authenticity): 키 암호화 해시 기능, 해시 기반 인증 코드 및 MAC 첨부 메시지

4) 부인봉쇄(Non Repudiation): AMI 통신 및 AMI 트랜잭션 로깅을 위한 스마트 미터 및 고유 키로 상호 검사

5) 가용성(Availability): 하드 코딩된 시퀀스, 이상 기반 IDS 및 사양 기반 IDS에 따른 대체 주파수 채널

6) 권한 부여(Authorization): 속성 기반 암호화, 속성 인증서 및 속성 기반 액세스 제어 시스템

Abdullahi Arabo는 서로 다른 환경에서의 스마트 홈의 연결에서의 사이버 보안에 대한 대책을 분석하였으며, 특히 서로 다른 디바이스 간의 상호 연동을 위한 요구사항과 이와 관련된 여러 가지의 문제점을 제시하였다. 또한 스마트 폰 혹은 모바일 단말기 등을 사용하여, 여러 가지의 수요자들의 요구사항을 수용할 수 있는 방법에 대해서 분석하였다 [14]. 강원민 등은 스마트 홈에서 각종 기기의 연결을 위한 개선된 보안 프레임워크를 제안하였고, 보안 강도 등을 비교 분석하였다 [15]. 일반적으로 이러한 보안 문제를 해결하기 위한 대표적인 방법으로는 다음과 같은 문제점을 고려하여 구현하여야 한다.

1) 네트워크 보안 측면: 네트워크 보안이 가장 중요한 부분입니다. 강력한 암호 알고리즘을 사용하고, 이중 인증을 활성화하며, 데이터 전송 중 기밀성을 보장할 수 있는 고강도의 암호화 기법을 사용하는 것이 선제적인 조건이다.

2) 소프트웨어 업데이트 측면: 모든 기기, 센서 노드 등과 같은 하드웨어 측면과 소프트웨어를 최신의 보안 패치로 업데이트로 유지하는 것이 중요한 부분인데, 이는 이미 알고 있지 않는 제3자에게 취약점이 악용되는 것을 사전에 방지할 수 있다.

3) 기기 접근 제한 측면: 스마트 홈 네트워크에 접근 가능한 기기의 수를 제한함으로써, 보안성을 높일 수 있다. 또한, 스마트 홈 기기 전용의 게이트웨이 등의 중간 역할을 하는 네트워크를 생성하고, 인증된 사용자만이 접근 및 통제가 가능하도록 제한하는 것이다.

4) 방화벽 사용 측면: 방화벽을 사용하면, 비인가된 접근 및 악성 트래픽을 차단하여 스마트 홈 네트워크를 보호할 수 있는 환경을 가질 수 있으나, 수많은 외부의 공격에 대한 보안정책이 필요하다.

5) 활동

모니터링 측면: 스마트 홈 네트워크의 정상적 혹은 비정상적인 활동을 정기적으로 모니터링하여, 보안상의 취약점을 혹은 이상 징후의 현상을 탐지하고 대응할 수 있어야 한다.

위의 조치들과 함께, 안전과 개인정보 보호에 우선순위를 두는 제조업체에서 출시한 안전하고 보호된 스마트 홈 기기를 선택하는 것이 중요하다.

V. 안전한 보안 설계를 위한 방법

스마트 홈 네트워크의 안전성과 보안성을 강화하기 위해서는, 다양한 종류의 보안 기능을 적용하고, 이를 안전하게 통합 관리할 수 있는 조치를 취해야 한다. <표4>는 이러한 요구사항을 만족하기 위한 스마트 홈 네트워크 구성에서의 기능을 정의하고 설명한다.

표 4 스마트 홈의 구성 요소
Table 4. Element of smart homes

분류	특징
홈 서버	- 데이터 접근 통제 기능 - 디바이스, 센서노드의 등록 및 삭제 기능 - 보안관제 모니터링 기술 - 보안정책 수립 및 분석
홈 게이트웨이	- 접근제어, 인증 문제 - 데이터의 암복호화 기능 - 안전한 알고리즘을 통한 봉안 등급 관리
외부의 단말기 및 서비스 제공자	- 홈 디바이스와 홈 게이트웨이의 통신 구간에 안전한 데이터 관리 - 복제방지 기능, 안전한 데이터 수집 및 저장 - 송수신 과정에서의 인증 문제

첫 번째로, 데이터의 접근통제를 위한 홈서버의 경우, 디바이스 혹은 센서노드의 등록 및 삭제 과정에 대한 모니터링을 위한 보안관제 기능이 구현되어야 하며, 보안정책의 수립과 개선을 위한 분석이 요구된다.

두 번째로, 외부로부터 홈 내부로 접근하기 위한 중간단계로 홈 게이트웨이를 설치 운영함으로 인해, 접근제어, 인증 문제, 데이터의 암복호화 기능, 모니터링을 위한 안전한 보안등급의 알고리즘으로 구현되어야 한다.

마지막으로, 외부의 단말기 혹은 서비스 제공자의 경우, 스마트 홈 디바이스 통신 구간 혹은 홈 게이트웨이 구간에서 안전한 디바이스 및 센서노드의 데이터 관리를 위한 펌 웨어 관리, 데이터 복제방지 기능, 안전한 데이터 수집 및 저장 및 송수신과정에 따른 상호 인증 기능이 적용되어야 한다.

이러한 IoT 기기의 인증을 위해, 신뢰할 수 있는 환경의 소프트웨어(TEE)를 보호하기 위해 기기 내에 독립된 메모리 공간에 보안 알고리즘을 임베디드화 하여 데이터의 무결성 및 정보의 기밀성을 유지할 수 있다. TEE(Trust Execution Environment) 환경을 지원하지 않는 기기의 경우, TPM, SE 등과 같은 보안 칩을 추가로 적용하여 활용할 수 있다. TPM은 암호화 알고리즘의 연산과 키 관리를 위한 하드웨어 칩을 의미하며, SE는 각종 기기 혹은 센서 내에서 인증서와 사용자 데이터를 보호하는 하드웨어 기반의 암호화 저장 장치를 말한다. TEE, TPM, SE의 기술은 어렵지는 않지만, 기존의 기기 등을 교체해야 하는 문제점을 가지며, 이 기술을 적용하면, IoT의 단말 가격을 상승하는 문제점을 가질 수 있다. 이러한 기존에 구축된 IoT 환경에 적합한 다수의 기법 및 방법이 제안되고 있는데, 그 대표적인 방법이 제로 트라스트(Zero Trust)이다. 이 기술의 기본적인 개념은 외부로 부터의 모든 기기들의 접근을 검증하고, 모니터링하는 보안 전략을 유지하는 것이다. 기존의 보안은 사전에 인가된 각종 기기들은 까다로운 인증 절차없이 적당한 권한 부여를 받는 것을 확인하여 연결하는 구조로 되어 있다. 그래서 해커들은 기기의 인증서를 탈취하여 정상적인 기기로 위장하여 연결하면, 무단으로 접근하여 설정된 권한 등급 등을 변경하여 데이터를 유출 혹은 시스템을 파괴할 수 있는 단점을 가진다. 제로 트라스터의 기법을 통하여 정상적으로 권한을 부여받은 기기들도 매번 접속 시 기기를 검증하고, 사용자의 행위를 감사함으로 인해 외부의 해킹 혹은 접근을 막을 수 있는 장점을 가진다. (그림3)은 임베디드 기술을 이용하여 센서 노드에 암호화, 메모리 저장, 통신 등과 같은 기능을 센서의 구성도를 보여 주고 있다.

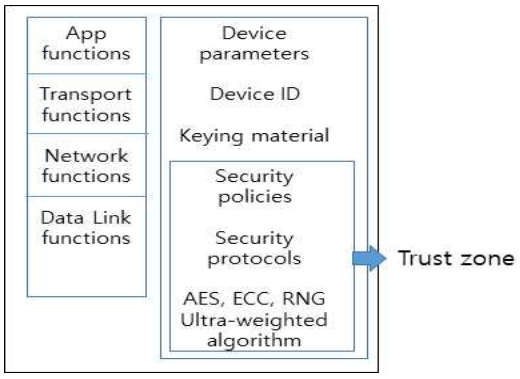

그림 3. 센서 노드의 구성
Figure 3. Configuration of sensor node

안전한 보안 기능을 위하여, 다음과 같은 구성 요소를 필수적으로 고려해야 한다 [16, 17].

가. 안전한 구조설계

- IoT 기능을 내장한 센서 노드 등의 보안 수준을 유지하고, 해킹 혹은 취약점을 통한 침해사고의 위험을 확산 방지하기 위한 보안 아키텍처(Secure Architecture)를 설계하여야 한다.

- 제한된 자원의 사용으로 인한, 저전력, 저사양의 암호 알고리즘 및 프로토콜의 개발을 통해 프라이버시의 보호에 대한 대책을 마련해야 한다.

나. 핵심 요소의 기술 개발

- IoT 서비스를 안정적으로 운영을 할 수 있는 핵심적인 임베디드 시스템 기술을 제공하여야 한다.

- 센서, 노드, 통신 프로토콜 등에 대한 보안기술을 적용하고, 보안 품질 및 보증을 위한 정책 기반을 분석하여야 한다.

- IoT 소프트웨어 개발 과정에서 발생할 수 있는 취약점 제거를 위한 시큐어 코딩을 적용하여야 한다.

- 소형화, 저전력의 IoT 디바이스 및 센서 기술, 유무선 네트워크 환경에 적합한 초경량의 암호 알고리즘 및 안전성이 보장된 인증 기술을 적용해야 한다.

- 스마트 홈 네트워크에서 운영 중인 시스템에서 야기될 수 있는 다양한 보안 결함 및 외부의 공격자 및 해킹들로 부터의 위협을 방지하기 위한 접근통제, 침입탐지 기능 등을 내장한 임베디드 보안기술을 적용하여야 한다.

- 근래에는 인공지능 기술 등을 융합한 신기술을 구현하여 자동 탐지 및 추적 등의 기술이 요구된다.

- 공인된 기관에서 H/W, S/W의 보안 품질 보증(Security Quality Assurance)을 적용해야 한다.

Ⅵ. 결론

본 논문에서는, 제4차산업혁명의 기본이 되는 사물인터넷망을 이용한 스마트 홈 네트워크에서 발생할 수 있는 취약점과 보안 문제에 대해서 분석하였다. 기존의 암호화 기술로는 제한적인 메모리 용량, 저사양의 CPU 자원 등의 저사양으로 인하여, 사물 인터넷망에서 사용되고 있는 센서 노드 및 저사양의 디바이스에 적용하기에는 불가능하다. 따라서, 저사양의 암호학적 기법으로는 안전성을 보장하지는 못한다. 이러한, 안전성 문제를 보장할 수 있는 초경량의 암호 알고리즘의 개선이 필수불가결하고, 센서 노드 및 디바이스에 대하여 다중 인증 등의 기법을 확인하여 각각의 노드에 대한 보안을 강화하며, 이를 통하여 외부 공격으로 발생되는 문제 등을 경감시킬 수 있다. 따라서, 본 논문에서는 IoT 보안에서 요구되는 요구사항 및 안전한 보안을 위한 설계 방법에 대해서 분석하였다.

References

[1] Tommaso Pecorella, Laura Pierucci and Francesca Nizzi, “Network Sentiment” Framework to Improve Security and Privacy for Smart Home“, Future Internet, 2018, Vol 10, No. 125; https://doi.org/10.3390/fi10120125
[2] Jung-Oh Park, ”A Message Communication for Secure Data Communication in Smart Home Environment Based Cloud Service“, Journal of Convergence for Information Technology, Vol. 11, No. 7, pp. 21-30, 2021. https://doi.org/10.22156/CS4SMB.2021.11.07.021
[3] Niharika Panda and M. Supriya, ”Efficient Data Transmission Using Trusted Third Party in Smart Home Environments“, EURASIP Journal on Wireless Communications and Networking, 2022, N.118, https://doi.org/10.1186/s13638-022-02200-9.
[4] Won Min Kang, Seo Yeon Moon and Jong Hyuk Park, ”An Enhanced Security Framework

for Home Appliances in Smart Home“ Human-centric Computing and Information Sciences, 2017, Vol.7: No.6 ,https://doi.org/10.1186/s13673-017-0087-4

[5] Saeid Pira, "The Social Issues of Smart Home: A Review of Four European cities' Experiences“, European Journal of Futures Research, (2021) 9:3, https://doi.org/10.1186/s40309-021-00173-4.

[6] Mamun Abu-Tair, Soufiene Djahel, Philip Perry, Bryan Scotney, Unsub Zia, Jorge Martinez Carracedo and Ali Sajjad, “Towards Secure and Privacy-Preserving IoT Enabled Smart Home: Architecture and Experimental Study“, Sensors 2020, 20, 6131; https://doi.org/10.3390/s20216131.

[7] Zaied Shouran, Ahmad Ashari and Tri Kuntoro Priyambodo, "Internet of Things(IoT) of Smart Home: Privacy and Security", International Journal of Computer Applications (0975 – 8887) Vol. 182, No. 39, February 2019, DOI: 10.5120/ijca2019918450.

[8] Talal A. Abdullah, Waleed Ali, Sharaf Malebary and Adel Ali Ahmod, “A Review of Cyber Security Challenges, Attacks and Solution for Internet of Things Based Smart Home”, International Journal of Computer Science and Network Security, Vol. 19, N.9, Sep 2019, pp. 139-146.
http://paper.ijcsns.org/07_book/201909/20190917.pdf

[9] Romano Fantacci, Tommaso Pecorella, Roberto Viti and Camillo Carlini, Short Paper: Overcoming IoT Fragmentation Through Standard Gateway Architecture, 2014 IEEE World Forum on Internet of Things (WF-IoT), 2014, pp.181-182.

[10]Soo-Mok Jung, “Reversible Data Hiding Technique using Encryption Technique and Spatial Encryption Technique”, The Journal of the Convergence on Culture Technology, Vol. 7, No. 1, pp. 632-639, February 28, 2021. https://doi.org/10.17703/JCCT.2021.7.1.632

[11]Oh, SoYun and Han, KwangHee, "Effect of Education about Blockchain Technology on Trust, Security, and Technology Acceptance Model of Virtual Assets“, The Journal of the Convergence on Culture Technology, Volume 8 Issue 6 pp. 675-683, 2022. https://doi.org/10.17703/JCCT.2022.8.6.675

[12]Sung Wook Lee, “Secured Authentication Scheme and Charging & Discharging System Operation for Electric Vehicles”, The Journal of the Convergence on Culture Technology, Vol. 7, No. 1, pp. 551-557, February 28, 2021 .https://doi.org/10.17703/JCCT.2021.7.1.551

[13]Nikos Komnins, Eleni Philippou and Antreas Pitsillides, “Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures”, IEEE Transaction Survey & Tutorials, 2014, Vol. 16, No. 4, pp. 1933-1954. DOI: 10.1109/COMST.2014.2320093

[14]Abdullahi Arabo, “Cyber Security Challenges within the Connected Home Ecosystem Futures“, Procedia Computer Science, 2015, pp. 227-232. https://doi.org/10.1016/j.procs.2015.09.201

[15]Jung Tae Kim, “Analyses of Security Mechanism for Sensor Network based on Internet of Things”, 2015 Summer Conference of the Convergent Research Society among Humanities, Society, Science and Technology, 2015, pp. 40-44.

[16]Chibiao Liu and Jinming Qiu, “Study on a Secure Wireless Data Communication in Internet of Things Applications”. Internal Journal of Computer Sciences and Network Security, 2015, Vol. 15, No. 2, pp. 18-23. http://paper.ijcsns.org/07_book/201502/20150204.pdf

[17]D. Kozlov, J. Veijalainen, and Y. Ali, “Security and Privacy Threats in IoT Architectures”, In Proceedings of the 7th International Conference on Body Area Networks, 2012, pp. 100-102.