The Journal of the Convergence on Culture Technology (JCCT)
Vol. 9, No. 4, pp.639-647, July 31, 2023. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2023.9.4.639
JCCT 2023-7-78

사물인터넷 환경하에서 보안 이슈 및 요구사항 분석

Analyses of Security Issues and Requirements Under Surroundings of Internet of Things

김정태*

Jung Tae Kim*

요 약 인터넷 기술이 발전함에 따라, 기존의 유선과 무선망의 결합은, 이기종 시스템의 융복합 기술을 가져왔다. 기존의 산업 기술은 주로 산업, 제조업, 자동화 등의 굴뚝산업 분야에서 컴퓨터 기술을 기반으로 한 정보기술로 집중되고 있다. 신기술이 기존의 기술과 융합되는 기술로 개발되고, 향상됨에 따라 많은 다양한 응용 시스템이 등장하게 되었다. 기존의 기술과 융합된 대표적인 응용분야는 사물인터넷 서비스 분야이다. 사물인터넷은 각각 기존에 존재하는 기술을 기반으로 초연결성의 네트워크을 연결하는 제4차 산업혁명의 기반 기술이 되고 있다. 그러나, 저용량의 메모리, 저전력 및 낮은 컴퓨팅과 같은 IoT의 제한된 자원으로 인해, IoT 장치는 보안에 취약하고, 다양한 종류의 보안 문제로 노출된다. 따라서, 본 논문에서는 IoT 서비스 환경하에서 요구되는 보안 문제점 및 해결 방법에 대해서 리뷰 및 분석하였다.

주요어 : 사물인터넷, 보안 이슈, IoT, 센서 노드, 암호화

Abstract A variety of communications are developed and advanced by integration of wireless and wire connections with heterogeneous system. Traditional technologies are mainly focus on information technology based on computer techniques in the field of industry, manufacture and automation fields. As new technologies are developed and enhanced with traditional techniques, a lot of new applications are emerged and merged with existing mechanism and skills. The representative applications are IoT(Internet of Things) services and applications. IoT is breakthrough technologies and one of the innovation industries which are called 4 generation industry revolution. Due to limited resources in IoT such as small memory, low power and computing power, IoT devices are vulnerable and disclosed with security problems. In this paper, we reviewed and analyzed security challenges, threats and requirements under IoT service.

Key words : Internet of Things, Security Issues, IoT, Sensor Node, Encryption

Ⅰ. 서 론

인터넷 기술의 발전과 기존의 제조 산업의 기술적인 도약으로 인해, 산업 전반이 융합 및 첨단화하는 방향으로 발전되고 있다. 특히, 모바일 및 이동통신 기술과 연계한 스마트 팜, 환경 감시, 스마트 시티, 원격 제어, 산업 재해 및 안전, 스마트 헬스케어, 스마트 홈 네트워크 등의 신 성장 산업으로 지속적으로 융복합화되고 있다. 이러한 정보통신 기술은 인간과 인간, 인간과 정보, 인간과 사물을 연결하여, 인간-사물-공간 및 시스템을

*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 Electrical and Electronic Engineering

초연결하는 제4차 산업혁명의 시대를 지향하는 ICT(정보통신기술) 시대로 전개되고 있다. 이러한 기술들은 기존의 핵심 기술들인 IoT/IoE, WLL, W-LAN, 센서네트워크, 5G, SDN, 광정보전송, 나노포토닉스, 블록체인, 빅데이터, 클라우드, AI, 보안, UI/UX, 압축 부호화, 머신러닝, 고속압축 미디어 처리 등을 총망라한 융합 기술로 발전되고 있다 [1]. 이러한 융합 기술로 인하여, 초연결성을 이루는 IoT 응용 서비스 부분에서 보안 및 취약점 문제가 많이 대두되고 있다. 특히 의료 시스템의 경우, 환자의 개인적인 기록을 기록하고 각종 의료 기기에 적합한 고성능 기술 및 보안을 위해 최적화된 보안 프로토콜 및 메커니즘이 요구되고 있다. 일반적으로 보안의 주요 요소는 기밀성, 인증, 무결성, 가용성, 부인 방지 등의 5대 핵심 기술로 구성된다. IoT 서비스는 다양한 기기의 상호 연결 및 이기종의 네트워크를 가지고 복잡하게 초연결성 구조로 구성된다. 이러한 현상으로 인해, 상호 연결된 대규모의 서비스 및 장치 및 기기의 복잡성과 이질성 문제로 인해 다양한 보안 문제가 발생할 수 있다. 따라서, 최적화된 고강도의 보안 프로토콜 및 기술은 고성능 및 최고의 보안 수준으로 요구한다.

예를 들어, IoT 기반의 의료 시스템의 경우를 분석해보면, 네트워크의 외부와 의료 인프라 즉 내부의 데이터베이스 및 각종 기기 사이의 프로토콜에 많은 다양한 공격과 위협이 존재하고 있다. IoT 기반의 스마트 헬스케어 네트워크는 중간의 게이트웨이를 구성하기 위해서, 임베디드 센서 및 노드, 정보 이동을 위한 각종 에이전트, 유무선 센서 네트워크, 데이터베이스 에이전트 및 네트워크 에이전트로 구성된다. 최근에는 각종 정보시스템의 경우, 네트워크, 데이터베이스, 에지 혹은 센서 등에 대한 보안 및 개인 정보 보호와 프라이버시 관련 분야가 활발히 연구되고 있다.

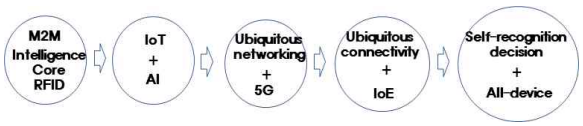

그림 1. 인터넷의 기술 발전
Figure 1. Trend of Technology by Development of Internet

(그림1)은 인터넷 기술의 발전으로 제4차 산업혁명을 이루는 기술적인 발전 방향을 나타내고 있다. 기존의 M2M(Machine to Machine) 기술 단계에서 반도체 제조공정의 발전, 광통신망의 확대 및 프로토콜의 개선 등으로 급속한 발전을 이루고 있다. 현재에는 IoT 기술에 인공지능(AI) 기술을 융합하는 기술로 발전되고 있다. 미래에는 모든 센서, 디바이스, 각종 기기들이 초연결성을 갖는 만물 통신(IoE)을 거쳐, 모든 기기들이 스스로 독립적으로 추론 및 판단할 수 있는 지능형 구조의 시스템으로 기술적인 발전이 전개될 예정이다. 최근에는 사물인터넷 망(Internet of Things)을 활용하여, 기존의 헬스 케어 시스템을 스마트 폰 등의 디바이스를 통해 환자의 진료 및 기록 상태를 모니터링 및 관리할 수 있는 응용 분야로 발전하고 있다. 이러한 고도화된 기술, 효율성 및 이동성 등의 장점에도 불구하고, 네트워크을 구성하고 있는 기본적인 장치, 노드, 디바이스 , 프로토콜 및 플랫폼 등에서 보안 취약점이 발생되고 있다. 이러한 보안 문제 이슈들은 사물인터넷에서 사용되는 디바이스 및 센서들의 제한된 자원인 메모리 용량 부족, 컴퓨팅 연산 능력의 저하 등으로 인하여, 기존의 암호화 알고리즘을 사용할 수 없는 문제로 야기된다 [2]. 따라서 본 논문에서는 이러한 보안 시스템 구현 시 고려해야 하는 보안 취약점에 대해서 리뷰를 통하여 분석하고자 한다.

II. 관련 연구

Fatma Alshohoumi 등은 사물인터넷 분야에서 발생할 수 있는 각종 보안 문제와 프라이버시와 관련된 문제점 및 최근의 보안 이슈에 대해서 분석하였다. 그는 특히 IoT 기술의 발전 과정과 이에 따른 기술적인 요구사항에 대한 첨단기술 등을 제시하였다. 특히 보안과 관련된 기술에 대하여 상호 간의 융합 분야에 대해 언급하였으며 (그림2)와 같이 기술하였다. 특히 Security와 Privacy에 대한 정의를 <표1>과 같이 정의하였다 [3].

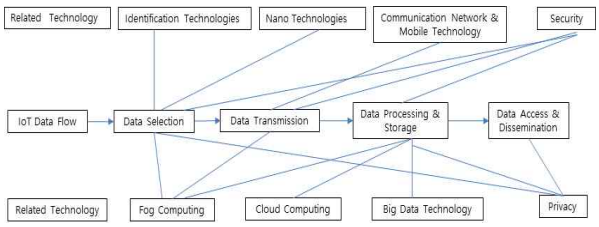

그림 2. IoT의 대표적 기술
Figure 2. Representative Technology of IoT

표 1. 암호의 정의 비교
Table 1. Comparison of Definition of Encryption

Security	Privacy
- Encryption - Authentication - Confident - Integrity - Availability - Digital Signature - Hacking - Validity - Safety - Access Control	- Authentication - Hidden Identity - Access Control - Trust - Unlinkability - Prevent Profiling - Prevent Lifecycle Detect - Prevent Data Misuse - Data Collection - Prevent Facilitate - Prevent Localization

인터넷을 연결하기 위해서, 기존의 컴퓨터, 정보시스템 등과 같이 대용량의 시스템의 경우, 자원의 제약을 고려할 필요 없이 기존의 네트워크 프로토콜 기술인 TLS(Transport Layer Securit)와 SSL(Secure Sockets Layer)과 같은 기존의 암호화 기술이 사용된다. 그러나 사물인터넷의 경우, 중앙처리장치의 저수준의 성능과 메모리 용량의 크기 등의 제한된 하드웨어 리소스를 가지기 때문에, 기존의 알고리즘을 적용할 수 없음으로, IoT 기기 등에 최적화된 초경량의 암호화 기술이 요구된다. 김용새 등은 대표적인 기술인 mbedTLS의 ECDSA 알고리즘을 응용하여, 다양한 초경량화 암호화 기술에 적합하도록 설계하여, IoT 기기 및 센서 노드 환경에서 구현하고, 성능을 측정하여, 그 결과를 비교 기술하였다 [4].

일반적으로, 센서 네트워크 및 사물인터넷은 한정된 하드웨어의 자원으로 인하여, 무선 환경에서 고비도의 비밀성 및 인증 메카니즘의 보안이 보장되지 못하며, 물리적 보안도 매우 취약점을 많이 가지고 있다. 따라서, 현재의 주요 연구 분야로는, 센서 네트워크에 대한 고비도의 비밀성을 보장하고 및 취약점 강화를 위하여, 주로 통신망에서의 프로토콜의 문제, 분산 및 응용 서비스 시스템에서의 문제, 센서 노드(Node) 및 에지(Edge)에 대한 물리적인 수명 및 암호학적인 비도 등에 관한 연구 주제를 채택하고 있다. Mouza Bani Shemaili 등은 IoT에 응용 가능한 시스템을 구성하기 위해, 기존의 암호 알고리즘의 구조를 분석하고, 초경량의 하이브리드 구조의 암호 알고리즘을 제안했다. 그는 고비도의 암호 알고리즘을 구현하기 위해, LFSR(Linear feed back shift register)의 단순성과 FCSR(Feedback with Carry Shift Register)의 비선형성을 결합하여 구현된 알고리즘을 비교 분석하였다 [5]. Kai Zhao 등은 IoT에서의 비밀성과 인증성을 보장하기 위하여, 프라이버시(Privacy)와 보안(Security)메카니즘을 분석한 후, 공개키 기반의 분산 접근제어 방식의 기술을 제안하였다. 특히 그는 보안 이슈를 해결하기 위해 경량 보안 프로토콜, 경량 암호 알고리즘의 설계, 하드웨어(Hardware) 및 소프트웨어(Software)의 설계 기법에 대해서 제시하였다 [6]. 남혜민 등은 제한된 하드웨어 자원을 가진 임베디드 환경하에서, 종단간 보안을 지원하는 개선된 MQTT-SN(Message Queueing Telemetry Transport for Sensor Networks) 모델을 제안하였다. 그는 기존의 프로토콜에 보안 필드와 인증 서버를 추가하여 보안 문제를 개선한 프로토콜을 구현하고, 실제의 프로토콜 상에서 전력의 소모량을 측정하여 평가하였다 [7]. 강동희 등은 IoT 환경하에서, 대표적인 네트워크 보안 프로토콜인 TLS의 성능 및 부하를 예측하였다. 또한, 그는 주요 암호화 알고리즘의 성능을 분석하기 위하여, IoT 기기의 사양에 따라, 최적의 조건을 맞추기 위한 네트워크 프로토콜의 보안 속성을 설정할 수 있는 기준을 제시하였다 [8].

III. 사물인터넷에서의 보안 취약점

IoT 시스템은 기존의 인터넷에서의 문제점 및 보안 이슈를 포함하고 있어, 다양한 요구 조건을 충족하여야 한다. 그 대표적인 조건은 각각의 응용 시스템의 애플리케이션에 따라, 다음과 같이 기술한다 [9, 10].

Device (기기)

1) 센서, 디바이스, 노드 및 에지 등에서 요구되어지는 성능과 요소가 다양하기 때문에, IoT에 적용되는 센서 등에 대한 최적의 경량화 보안 알고리즘이 필요하다. 기존의 보안 알고리즘은 CPU 성능, 메모리 크기, 소비 전력과 같은 제한된 자원으로 인해 적용될 수가 없다. 따라서, 저전력의 소자를 가진 초경량의 알고리즘과 같은 첨단 신기술이 요구되어 진다.

2) 중요한 정보를 제 3자 등의 비인가자로부터 보호하기 위해, 악성코드 탐지 및 해킹 방지를 위한 하드웨어 기반의 고도화된 보안 메커니즘을 임베디드(Embedded) 형태로 내장해야 한다.

네트워크 (Network)

1) 이기종의 네트워크 인프라 구조에서, 해킹 및 악성코드의 공격을 방어하고, 탐지하기 위한 신개념의 인공지능 기반의 네트워크 보안이 필수불가결하다.

2) 서로 다른 센서와 디바이스 간의 이기종의 구조로 상호 연결된 네트워크는 다양한 통신 메커니즘과 암호화, 인증 방식 등을 수용할 수 있는 구조의 보안 구조를 가져야 한다.

3) IoT 인프라 구조하에서, 상호간의 여러 가지 동작을 수행 함에 있어, 통합 구조의 상호 네트워킹을 운영하기 위해서 디바이스와 디바이스 간의 접근제어 및 상호 인증을 위한 메카니즘이 필요하다.

4) IoT 네트워크에 부착된 다양한 기기를 상호 연결하기 위해서는, IoT 서비스 환경에서의 통합 해킹 탐지 및 각각의 센서 데이터의 보호가 필수적이다. 특히 보안성 강화를 위한 고비도의 복잡성을 개선하기 위해, 각각의 프로토콜을 연결하고 전달하기 위한 보안 메카니즘을 수용하는 보안 게이트웨이(Security gateway)를 활용한다.

5) 악성코드에 감염된 사물인터넷 봇에 의한 대규모의 다양한 방향에서의 트래픽 공격을 방어하기 위한. 네트워크 모니터링 관리 및 보안관제 기술이 필요하다.

응용 서비스 (Application)

1) IoT 서비스 기기와 사용자 단말 서비스 기기 등에 대한 상호인증 접근제어가 지원되어야 한다.

2) 모든 기기에는 센서, 노드 등에 대한 외부의 인위적인 조작 및 비인가 접속을 보호하기 위한 개별 인증, 키 관리, 보안관제 및 접근제어 기능이 부가적으로 제공되어야 한다.

3) IoT 환경하에서 데이터를 분석, 개인식별, 위치추적 등 각각의 데이터에 대한 개인정보에 대한 침해 방지대책이 요구된다.

4) 대표적인 서비스인 홈 네트워크, 가전제품, 헬스케어 시스템, 교통, 안전 등을 위한 IoT 서비스를 지원하기 위해서는 신개념의 보안 플랫폼이 필수적이다. 예를 들어, 이러한 기술은 임베디드 시스템, 웨어러블 장비와 모바일 장비 등을 활용하여 적용할 수 있다. (그림 3)은 대표적인 IoT 시스템에 대한 각각의 노드의 특징, 위협 요소 및 보안에 대한 요구사항 및 대책을 보여 주고 있다. (그림4)는 IoT 서비스에 대한 대표적인 공격

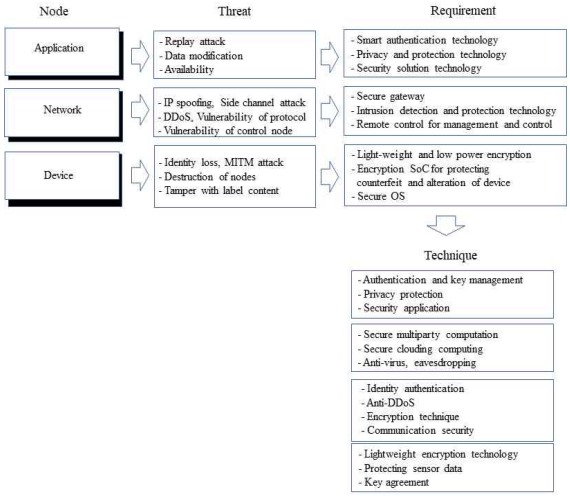

그림 3. IoT 구조의 일반적인 구성도
Figure 3. Configuration of Generalized Architecture of IoT

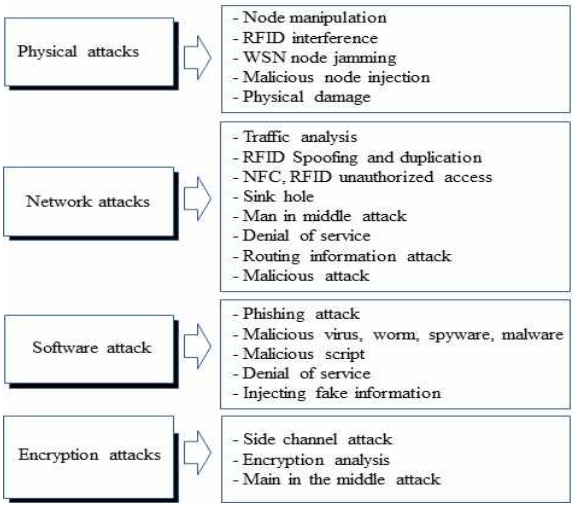

그림 4. IoT에 대한 일반적인 공격
Figure 4. Generalized attacks of IoT

및 내용을 나타내고 있다.

특히, 보안을 강화하기 위한 메카니즘 기법으로 메시지 암호화 방법 및 인증 기능을 제공해 주고 있다. 최근에는 새로운 구조의 초경량 암호 알고리즘인 SPECK SIMON, LEA, 등의 알고리즘이 개발되고 있다. 이러한 방식의 알고리즘은 OpenSSL 환경하에서, 초경량의 블록 암호 알고리즘의 구현에 적합하다. 또한, 저사양, 저성능 및 저전력의 통신에 응용 가능하고, IoT 환경에 적합하도록, 경박단소한 암호 엔진을 탑재하기 위한 기법을 개선하는 방법으로 발전하고 있다 [11, 12]. <표 2>는 기본적인 센서 노드에 대한 기술을 설명하고 있다.

표 2. 기본 기술의 요구사항
Table 2. Requirement of Basic Technology

RFID/Edge	To identify and track the data of things
Sensor/Node/Edge	To collect the data from node. To detect the changes of data in the physical states of things
Smart Technology	To enhance the power by devolving processing with different part of the network
Nano Technology	To make the smaller and smaller things by connecting each other

사물인터넷을 실현하기 위한 다양한 요구사항이 존재하는데, 그 대표적인 핵심 기술은 각 영역에서 다음과 같이 요약될 수 있다.

1) 에너지 및 저전력 : IoT 시스템 개발을 위한 필수 불가결한 기술이 초경량화 기술인데, 이러한 초경량화를 위한 저전력의 단일 칩셋 개발 및 저전력 회로 설계 기술을 통해 기기에서 소비되는 전력을 감소시킬 수 있는 기법이 필요하다.

2) 지능화 기술 : 기기들 상호 간에 연결되는 디바이스와 노드 간의 정보 교류를 위한 신기술의 인공지능을 통한 자율 정보 처리 기술이 요구된다.

3) 통합 통신망 : 각각의 디바이스와 디바이스 간의 통신을 연결하기 위하여 SoC(System on Chip) 형태로 구성하여 여러 종류의 주파수 밴드 대역 및 안테나 대역을 복합적으로 구성하여 단일 칩으로 제작할 수 있는 기술이 필요하다.

4) 집적도 : 시스템의 가격 단가를 줄이기 위하여, 고집적도의 반도체 기술을 이용하여, 단일 칩으로 구성하여, 칩의 면적을 줄이는 기술이 필요하다.

5) 상호운용성 : 상호 연결되는 디바이스 및 노드들을 상호 초연결성을 가지도록 하기 위해서는, 반드시 표준화를 통한 기기 및 각종 노드의 규격이 선행적으로 제정되어야 한다.

6) 표준화 : 표준화 과정을 통하여, 표준 알고리즘이 규정됨으로 인하여, 보안의 5대 원칙인 기밀성, 무결성, 부인 봉쇄, 서비스의 가용성, 감사 추적 기능을 제공하여야 한다. 또한, 이기종의 시스템을 초연결성을 가지도록, 다양한 프로토콜의 정합 기술이 제공되어야 하며, 또한 각각의 프로토콜, 센서, 노드 등에 대한 보안 절차 및 메카니즘이 필요하다. <표3>은 IoT 시스템을 구성하기 위한 요구사항을 요약하였다.

Ⅳ. 사물인터넷을 위한 경량 암호 성능

대표적인 경량화 암호 알고리즘인 LEA 암호 알고리즘은 현재까지 보고된 알고리즘 중에서, 블록 암호공격에 대한 해독 및 분석 능력이 비교적 안전하다고 알려진 Feistel 구조를 적용하여 설계되고 있다. 기본적인 구조로는 기존의 128 비트의 블록 크기를 기본으로 하여, 128 , 192, 256 비트 중에서 원하는 키 길이를 선택하여, 원하는 고비도를 구현할 수 있다. 기본적인 구조인 Feistel의 기본 구조는 라운드 함수 내에서 각 블록을 32 비트로 나누어 덧셈, 회전, 전치, XOR 등의 연산 기능을 사용하여, 암복호화를 수행하는 단순한 구조로 되어 있다.

표 3. 주요 기능의 요약
Table 3. Summary of Key Factor

Function	Requirements
Low-power	Optimization logical circuit based on low-power to operate sensor node
Intelligence	Artificial Intelligence capability for exchanging and sensing information and in different networking
Communication	Multi-band Antena technology for multiple communication between sensors
Integration	Integration for low cost and small chip area
Co-operability	Operability of standard for connecting a variety of protocols
Standization	Standard and matching interface techniques for enhancing security complexity

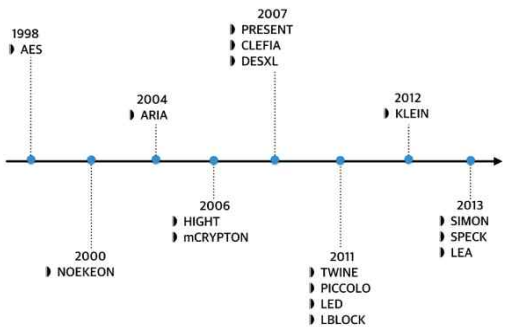

그림 5. 경량화 블록 암호 알고리즘의 발전 동향
Figure 5. Development Trend of Light-weight Block Encryption Algorithm t

(그림5)는 최근의 경량화 암호 알고리즘의 발전 동향을 보여 주고 있다 [13]. 하드웨어적 제약으로 인하여, 현재까지 많은 알고리즘 구조의 발전을 이루지 못하고

표 4 경량 암호의 사양
Table 4. Spec. of Ultra-weight Encryption

Algorithm	Block size	Gate Count	Structure
AES	128/256	3,100	SPN
PRESENT	64/128	1,391	SPN
CLEFIA	128/256	4,950	GPN
DESLX	64/184	2,168	Feistel
KLEN	64/96	1,360/1,700	SPN
mCRYPTON	64/128	2,420/2,949	SPN
LED	64	1,268	SPN
DESLX	64/184	2,168	Feistel
IDEA	64/128	-	Lai-Massey
LBLOCK	64/80	1,320	Feistel
SEED	128/128	-	Feistel
HIGHT	64/128	3,048	Feistel
ARIA	128	-	Feistel
LEA	128/192/256	3,490	Feistel
SIMON	128	2,532	-
SPECK	128	3,193	-
PICCOLO	64	1,539	-
TWINE	64	1,783	-
LED	64	2,329	-

표 5. 경량 암호 알고리즘의 성능
Table 5. Performance of Ultra-Encryption Algorithm

Algorithm	Algorithm		gate Count	Throughput @100MHz)
	block	key		
SIMON	128	128	2,532	182.9
SPECK	128	128	3,193	376.5
SIMON	64	128	1,728	133.3
SPECK	64	128	1,968	206.5
SIMECK	64	128	1,689	133.3
PICCOLO	64	128	1,539	193.9
TWINE	64	128	1,783	178.0
LED	64	128	2,329	133.3

있는 실정이나, 반도체 제조공정의 발전으로 인하여 기술적인 진전을 보여 주고 있다. 김동규 등은 초경량 암호 알고리즘의 최신 기술 동향을 분석하고, 그 구조를 비교하였다. 또한, 실제적인 크기를 계산하기 위해, 실제적인 회로설계의 구현을 통하여 게이트 수를 구하여 면적을 비교 분석하였다 [14]. <표4>는 경량 암호 알고리즘 구조 및 구현의 결과를 나타낸다. 표에서 보는 바와 같이, PICCOLO 알고리즘의 경우, 가장 작은 크기의 면적인 1,539 게이트로 구현되었다. 이는 초경량 암호 알고리즘들이 반도체 공정을 기술 발전에 힘입어, 사물인터넷 서비스의 특징인, 한정된 자원(Resource)만을 사용하는 초소형 사물인터넷 기기에 임베디드 시스템의 형태로 내장되기에 가장 유리할 것으로 판단된다. <표4>에서 보는 바와 같이, 암호화 성능은 처리율을 기준으로 보아, SPECK 알고리즘이 가장 좋은 성능을 보여준다. <표5>는 대표적인 경량 암호 알고리즘의 성능을 비교하였다.

이선근은 IoT 환경에 적합한 경량화 블록 알고리즘을 제안하였다. 기존 블록 암호 알고리즘을 경량화 암호 알고리즘과 같이 사용할 수도 있고, 센서부와 데이터저장부와 같은 기존의 기능을 거의 그대로 유지하면서, IoT 환경에 최적화된 방법을 제안하였다 [15]. 시스템의 품질 평가를 위한 QoS(Quality of Service) 품질을 측정하는 방법은, 예전부터 시스템 분석 및 설계 과정에서, 계층적 구조 모델을 사용하여 정립되고 있다. 이러한 측정 요소는 제한된 자원에 대한 분석을 통하여 주로 이루어지고 있다. 그러나, 특히 사물인터넷과 같은 융복합 시스템 형태에 대한 모델이 정립되지 못하고 있다. 따라서, 모하매드 등은 그의 논문에서 이러한 요소들의 항목을 분석하여, 시스템의 성능을 분석하고자 하였다. 주요 항목은 Security, Performance, Usability, Reliability, Robustness, Interoperability, Scalability 과 같다. 시스템의 성능 평가 및 품질 검증을 측정할 수 있는 방법은 다양하므로, 각각의 시스템에서 요구하는 서비스 요소에 대한 각각의 항목에 적합한 요소를 선택한다. 따라서 표준안으로 제정되기에는 많은 문제점을 내포하고 있다 [16].

제한적인 하드웨어 자원으로는 적은 메모리 용량, 저전력의 소비량, 컴퓨팅 파워 등이 대표적이다. 암호 엔진을 센서 노드 내에 내장시키기에는 작은 면적으로 인하여, 저용량의 암호 알고리즘으로 구현되어야 한다. 이로 인하여, 보안 및 취약점 문제점을 가져올 수 있다. (그림6)은 일반적인 센서 노드의 내부 구성도를 보여주고 있다. IoT의 대표적인 보안 및 취약점 위험 요소로는 센서, 노드, 디바이스, 장치, 에지, 시스템, 인프라 등의 오동작 및 작동정지 등으로 인하여 보안 이슈가 야기된다. 헬스케어 분야의 경우, 사람의 생명 및 자산을 위협할 정도로 많은 위협 요소로 작용하고 있다. 이러한 문제점을 해결하고, 감소시키기 위한 방법으로, IoT 응용시스템에 대한 최적의 보안기술이 필수 불가결하다. 따라서 (그림7)은 대표적인 IoT 보안 서비스 기술에 대한 요구사항이다 [17].

Ⅴ. 사물인터넷에서의 요구되는 보안 사항

암호화를 위한 최적화의 구현에 적합한 암호 알고리즘을 사용해야 하며, 대표적인 요구사항은 다음과 같다 [18]. <표6>은 대표적인 블록 및 공개 암호 알고리즘을 나타내고 있다.

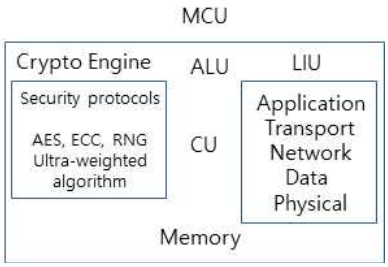

그림 6. 센서 노드의 구성도
Figure 6. Configuration of Sensor Node

- 암호모듈 검증 대상 암호 알고리즘 사용 (KS X ISO/IEC 19790* 또는 FIPS 140-2**)
- 대표적인 암호 알고리즘 : ARIA, SEED, HIGHT, KCDSA, EC-KCDSA, AES, Triple-DES, RSA, ECDSA 등

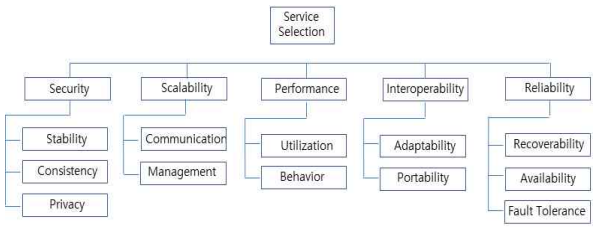

그림 7. 기본적인 IoT 보안 프레임워크
Figure 7. Basic IoT Security Framework

표 6. 대표적인 암호 알고리즘의 예
Table 6. Example of Representative of Encryption Algorithm

Algorithm	Examples
Block	AREA, SEED, LEA, HEIGHT, AES, Triple-DES
Public	RSA, ECC
Hash	SHA2. SHA3, HMAC

- 공개키 알고리즘의 경우, 보안 강도의 요구사항에 따른 키 길이의 증가가 요구된다.
- 비 검증 대상 암호 알고리즘의 지원 시, 초기값을 가진 비활성화 작은 메모리 및 저용량의 하드웨어자원의 제한으로 인하여, 기존의 암호 알고리즘의 사용이 어려운 경우, 대표적인 경량화 암호 알고리즘인 HIGHT 및 LEA를 주로 사용한다.

=> 보안 강도 112비트 이상의 암호 알고리즘의 사용을 권고한다.

=> KISA 및 NIST에서 배포한 각각의 표준 알고리즘에 대한 테스트 벡터값을 활용하여 실제 구현한 알고리즘의 성능 및 정확성을 검증한 후 사용한다.

1) http://seed.kisa.or.kr

블록 암호 알고리즘에 대한 부채널 공격에 대응하기 위한 다양한 기법의 사용을 권고하며 사용한다.

- 암호키 사용 시 발생하는 부가 정보(전력, 전자파량 등) 등을 검증하여야 한다.

2) http://csrc.nist.gov/groups/STM/cavp

표 7. 암호 알고리즘의 요구사항
Table 7. Requirement of Encryption Algorithm

Bit	lock	Hash	Public				Effective Period
			Factoring	discrete logarithm		ECC	
				Public	Private		
112	112	112	2,048	2,048	224	P-224/ B-233	~2023
128	128	112	3,072	3,072	256	P-256/ B-283	2030~
192	192	192	7,680	7,680	384	P-384/ B-409	
256	256	256	15,360	15,360	512	P-512/ B-571	

다양한 구조의 시스템에서, 다양한 보안기술이 요구되고 있다. <표7>은 대표적인 암호 알고리즘의 요구사항을 나타낸다 [19]. 이러한 요구 사항들은 센서, 디바이스, 노드, 기기들의 보안 모듈 설계를 위한 구현상의 편리성 및 기능의 확장성을 고려하여야 한다. 따라서 이러한 구현을 위해 요구되는 특이 사항은 다음과 같다.

- 어떤 서비스 영역에서도 적용 가능하고, 표준화되고, 최적화된 기능의 보안 모델이 요구된다.
- 다양한 종류의 사물인터넷 통신을 위한 응용 서비스 시스템에는 최적의 보안 알고리즘을 내포해야 한다.
- 초연결성으로 이루어진 모든 통신은 상호 암호화가 구현되어, 개별 인증이 되어야 한다.
- 모든 센서 노드의 접근은 상호 인증되어야 하고, 권한 부여의 기능을 가져야 한다.

Ⅵ. 사물인터넷에서의 요구되는 보안 사항

6.1 대표적으로 해결해야 할 문제

▪ 기존의 소프트웨어 개발과정에서 무시할 수 있는 보안 취약점을 제거하고, 보안성 강화를 위한 여러가지의 암호학적인 기술을 융합한 시큐어 코딩 기술이 필요하다.

▪ 메모리, 중앙처리장치, 배터리 등의 반도체 소자의 소형화, 논리소자의 저전력화 및 경량화를 위한 자원 제약 조건으로 인하여, 불필요한 기능 및 회로의 설계를 최소화하고, 초경량화의 암호화 기술이 필요하다.

▪ 해킹 및 외부의 제 3자로 부터의 위험을 제거 혹은 경감할 수 접근통제, 침입탐지 등을 사용한다. 따라서, 기존의 방법에 비해, 개선된 AI 기반의 자율 탐지 기술 등의 신개념 기술이 필수 불가결하다.

▪ 정보통신기기 등의 하드웨어 및 소프트웨어의 보안성 적합 인증을 강화하고, 보안 기능의 성능을 확인할 수 있는 보안 메카니즘의 적합성을 평가할 수 있는 규격 등이 필요하다.

6.2 안전한 구조설계

▪ IoT 서비스를 지속적으로 유지하기 위하여, 고비도의 보안 수준을 유지하고, 침해, 안전사고 및 위험 확산 방지를 위한 프로토콜의 설계, 보안 아키텍처 (Secure Architecture) 및 고비도의 암호 알고리즘의 개발이 확립되어야 한다.

▪ 보호되어야 할 핵심 자산을 방어하고, 외부의 위협을 식별하고, 현재의 보안 평가 수준을 평가하여 외부 및 내부의 위협에 대응하기 위한 보안 정책 수립, 보안 시스템의 구성 및 이를 운영하기 위한 정책을 명확히 수립해야 한다.

▪ 향상된 저전력의 회로설계 기술 및 초경량화된 암호 알고리즘의 개발, 보안성이 강화된 프로토콜 개발 및 개인 프라이버시 보호에 관한 기술을 개발해야 한다.

6.3 핵심 요소의 안전한 개발

▪ IoT 서비스의 안정적인 운영을 위한 핵심 기술 요소인 소자, 제어, 구동, 통신, 임베디드 등에 대한 보안 핵심 기술을 적용하고, 보안성 및 품질 보증을 위한 정책적인 법률을 분석하고 지원해야 한다.

▪ IoT 시스템의 개발 시 소프트웨어 보안 취약점을 제거하기 위한 방법으로 시큐어 코딩(Secure coding) 기법을 고려하여 적용해야 한다.

▪ 소형화 기술, 저전력의 IoT 디바이스 및 소자, 네트워크 환경에 적합한 초경량 인증 및 암호화 기술의 적용 등을 융합하여 임베디드 기술로 개발될 수 있어야 한다.

▪ IoT 시스템 운영 중에서 발생할 수 있는 보안 결함 및 해킹의 위협으로부터, 시스템을 보호하기 위한 접근통제, 침입탐지 등을 위하여 임베디드 보안기술을 적용해야 한다.

▪ IoT H/W, S/W의 보안 품질 보증(Security Quality Assurance) 기준을 명확하게 적용해야 한다.

Ⅵ. 결 론

초고속의 정보통신 기술의 발전으로 인하여, 기존의 유선 인터넷망과 이동 통신망이 통합되어 융합되는 과정으로 발전하고 있다. 이러한 망 구조로 말미암아, 사물인터넷을 기반으로 한, 초연결성의 통신망으로 다양한 구조의 서비스를 위한 복합망으로 전개되고 있다. 따라서, 본 논문에서는 이러한 사물인터넷 망에서의 구조 및 요구사항을 알아보고, 특히, 시스템의 가용성을 위한 서비스 품질을 위한 항목을 리뷰하고 분석하였다. 또한 사물인터넷에서 발생할 수 있는 공개된 보안 문제점을 사전에 분석하고, 여러 가지의 보안 및 취약점 분석을 통해, 추후 IoT 시스템 설계 시에 도움이 되고자 한다.

References

[1] Hussain Shaikh, Jong-Ho Kim, “Factor Analysis of IoT Relative Advantages with TAM Model”, Journal of Next-generation Convergence Technology Association, Vol. 6, No. 2, pp. 193-201, 2022. https://doi.org/10.33097/JNCTA.2022.06.02.193

[2] Ji-Yeon Lee, “A Study on Cloud Service Certification Approach from SaaS Security Perspective”, Journal of Next-generation Convergence Technology Association, Vol. 6, No .10, pp. 1820-1830, 2022. https://doi.org/10.33097/JNCTA.2022.06.10.1820

[3] 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, pp. 232-251, 2019. DOI: 10.14569/IJACSA.2019.0100733.

[4] Young-Sae Kim and JeongNyeo Kim. "A Performance Analysis of Lightweight Cryptography in IoT Devices", The 28th Joint Conference on Communications and Information, pp. 327-328, 2018

[5] Caiming Liu, Yan Zhang and Huaqiang Zhang. "A Novel Approach to IoT Security Based on Immunology", Ninth International Conference on Computational Intelligence and Security, pp. 771-775, 2013.

[6] Kai Zhao and Lina Ge. "A Survey on the Internet of Things Security, Ninth International Conference on Computational Intelligence and Security", pp. 663-667, 2013.

[7] Hye-minNam and Chang-seop Park. "Modified MQTT-SN Protocol for End-to-End Security in a Constrained Embedded Environment", Journal of The Korea Institute of Information Security & Cryptology, Vol. 30, No., pp. 859-870, 2020. https://doi.org/10.13089/JKIISC.2020.30.5.859.

[8] Dong-hee Kang and Jae-DeokLim. "Network Security Protocol Performance Analysis in IoT Environment", Journal of The Korea Institute of Information Security & Cryptology, Vol. 32, No. 5, pp. 955-963, 2022. https://doi.org/10.13089/JKIISC.2022.32.5.955.

[9] Xiong Li, Zhou Xuan and Liu Wen. (2011) Research on the Architecture of Trusted Security System Based on the Internet of Things", 2011 Fourth Internal Conference on Intelligent Computation Technology ad Automation, 1172-1175.

[10]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. Vol. 20, No. 21., pp. 6131, 2020. doi:10.3390/s20216131.

[11]A. Juels. P. Syverson. and D. Bailey, "High Power Proxies for Enhancing RFID Privacy and Utility, Center for High Assurance Computer Systems", CHACS, LNCS Vol. 3856, pp. 210-226, 2015. DOI:10.1007/11767831_14

[12]M. Rieback. B. Crispo. and A. Tanenbaum. RFID Guardian, "A Battery Powered Mobile Device for RFID Privacy Management", Australasian Conference on informaiton Security and Privacy (ACISP) LNCS 3574, 184-194, 2015.

[13]Moon-si Hoon, Min-woo Kim and Tae-kyung Kwon, "Technology Trend of Ultra-weight En cryption for IoT Communication Surroundings", Korean Institute of Communications and Infor mation Sciences. Information and Communications Magazine. Vol. 33, No. 3, pp. 80-86, 2016.

[14]Dongkoo Kim and Hyeal Lee. "Implementation of Hardware and Trend of Ultra Encryption Algorithm", IDEC WEBZIN,http://www.idec.or.kr/webzine/?news_id=20191102.2019.

[15]Seon-Keun Lee. "A Study on Lightweight Block Cryptographic Algorithm Applicable to IoT Environment", Journal of the Korea Academia-Industrial cooperation Society, Vol. 19, No. 3, pp. 1-7. 2018. https://doi.org/10.5762/KAIS.2018.19.3.1.

[16]Mohammad Abdur Razzaque, Marija Milojevic-Jevric, Andrei Palade and Siobhan Clarke. "Middleware for Internet of Things: A Survey:, IEEE Internet of Things Journal. Vol. 3, No. 1, pp. 70-95, 2016. DOI: 10.1109/JIOT.2015.2498900

[17]Antonio F. Skarmeta, Jose L. Hernandez Ramos and M. Victoria Moreno. "A Decentralized Approach for Security and Privacy Challenges in the Internet of Things", IEEE World Forum on Internet of Things, pp. 67-72, 2014.

[18]Seminar Materials, "IoT Security Authentication Criteria Test, Case Study Top7", KISA, 2020. 9.18.

[19]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, 87-92, 2012.