한국사물인터넷학회논문지 Vol. 5, No. 2, pp. 103-110, 2019 https://doi.org/10.20465/KIOTS.2019.5.2.103

수용가 전력설비 관리를 위한 사물인터넷 플랫폼 연구

장경배*
고려사이버대학교 기계제어공학과 교수

A study on IoT platform for private electrical facilities management

Kyung-Bae Jang*
Professor, Dept. of Mechanical and Control Engineering, The Cyber University of Korea

요 약 본 논문에서는 사물인터넷(IoT) 기술을 적용하여 고객의 전력 시설을 효율적으로 관리하기 위한 인터넷 플랫폼을 제안한다. 효율적 관리를 위한 인터넷 플랫폼은 사물간의 연결을 위한 통신 방식과 그에 따른 프로토콜, 그리고 보안 요소로 구분하여 각 요소별 분석을 실시하였다. 이를 통해 전력 설비에 사용되는 기존 센서를 기반으로 센서와 서버 간의 데이터 신뢰성을 위한 통신 솔루션, 데이터 관리 서버 및 보안 솔루션에 대해 개발 방안을 제시하였다. 또한, 전력 설비 관리 플랫폼에서 사용될 수 있는 통신 모듈, 프로토콜 및 보안 알고리즘을 제안하고, 이를 관리하고 운영하기 위한 서버를 구축하는 방법을 제안한다.

주제어 : IoT 플랫폼, 자가용 전력 설비, 암호화 시스템, IoT 무선 센서 노드

Abstract In this paper, we suggested how the Internet of Things (IoT) technology could be applied to an internet platform that is used for managing the customer's power grid efficiently. For an internet platform with efficient management, analysis is done by several sections; communication method, and its protocol, and also security element. From this analysis, with currently used sensors, we have presented a development method for the sensor to server data reliable communication solution and data management server with a security solution. Moreover, this paper suggests a communication module that could be used for a power grid management platform, protocol and security algorithm and also a way to build a server for managing those systems and modules.

Key Words : IoT Platform, Electric Power Facilities, Cryptosystem, Wireless Sensor Nodes in IoT

1. 서론

최근 사물인터넷(IoT : Internet of Things) 기술의 발전으로 IoT 기능을 채택한 센서를 기반으로 사물인터넷을 수용가 전력설비인 수·배전반(특고압반, 고압반, 저압반,MCC 등)에 도입하려는 연구가 활발히 진행되고 있으며 실제 구현이 가능하게 되었다. 연구를 통해 전력설비의 상태정보(전압, 전류, 전력, 역률, 주파수 등)를 원격으로 확인할 수 있다[1]. 이는 통신기술 및 관련 디바이스의 발전으로 사물(things)이 유·무선을 통해 인터넷에 연결되어 모든 사물과 사람이 네트워크로 연결되는 초연결 사회(Hyper Connected Society)로 진화되는 것을 의미한다. 그러나 사물인터넷의 적용은 대상에 따라 여러 요소가 고려되어야 하며, 이를 효과적으로 대응하기 위하여 IoT의 기본 특성을 고려한 플랫폼 형태의 접근이 이루어지고 있다.

*교신저자 : 장경배(kbjang60@cuk.edu)
접수일 2019년 8월 16일 수정일 2019년 10월14일 심사완료일 2019년 10월 24일

사물인터넷 플랫폼은 센서 노드와 해당 데이터를 받아 처리하는 서버로 구성된다. 센서 노드와 서버의 데이터 전달은 유선과 무선으로 다양하게 구성되지만 IoT 분야의 센서의 경우 전원 및 면적, 그리고 가격의 제한으로 인하여 하드웨어 사양이 낮으며, 사용범위가 다양하므로 대부분의 데이터 통신은 무선으로 구성되어진다. 이에 따라 무선통신을 구성하는데 있어 현재 Wi-Fi, Bluetooth와 같은 기존 무선통신 방식과 BLE(Bluetooth Low Energy)와 Zigbee, 그리고 Z-wave와 같은 IoT 특화된 근거리 통신방식과 LoRa와 SigFox와 같은 장거리 통신 방식이 적용되고 있다.

사물인터넷 플랫폼은 센서 노드와 데이터 수집 처리를 위한 서버와의 통신을 기반으로 구성되며, 이에 대해 통신 네트웍을 구축하여야 한다. 이에 따라 사물인터넷 플랫폼에서 사용하기 위한 네트웍 구성을 전용으로 할 수 있지만 비용 문제로 기존의 유·무선 네트워크를 활용할 수 있도록 여러 방향에서 연구되어지고 있다. 최근에는 MQTT(Message Queue Telemetry Transport)와 CoAP(Constrained Application Protocol)과 같은 인터넷 기반의 네트워크에서 사물인터넷에 적합하게 사용 가능한 프로토콜이 제안되고 있고 여러 플랫폼에서 적용되어지고 있다. 하지만 이러한 인터넷 망을 사용하기 위해서 가장 중요한 요소로 보안이 고려되어져야 한다. 이는 사물인터넷에 사용되는 정보에 대해 외부 해킹에 의한 문제가 언제든 발생할 수 있고 이에 대한 파급이 점차 증대되어 질 수 있다. 이에 따라 금융산업과 같은 보안이 발전된 방식을 사물인터넷에 맞추어 적용할 수 있도록 연구되어지고 있다. 사물인터넷의 경우 금융 서비스의 장비보다 가볍고 단순하므로 복잡한 연산을 보다 간단하게 하며, 보안 레벨도 높여야 하는 문제를 안고 있다. 이에 따라 본 연구에서는 최신의 사물인터넷에 적용 가능한 보안 알고리즘을 비교 분석하여 적용하기 위한 방법을 제안하고자 한다.

IoT 구성에서의 센서노드에 대한 데이터를 수집하여 처리하는 부분을 서버라고 하며, 이러한 서버의 구성은 최근에는 클라우드 기반으로 구성한다. 센서노드에서 구성되는 네트워크는 그에 대한 수와 데이터 양은 적을 수도 있지만 대규모로 구성될 수 있으며, 이러한 경우 빅데이터로 많은 처리 용량을 필요로 할 수 있다. 이에 따라 상용 서버를 클라우드 기반으로 대여하여 운영하는 업체가 생겨나고 있으며, 아마존(AWS)과 구글(Google), 그리고 MS(Microsoft) 같은 글로벌 업체가 시장에 빠르게 진입하고 있다.

전기 분야에서도 다양한 사물인터넷 플랫폼에 대해 논의가 이루어지고 있으며, 이를 통해 전기설비에 대한 안전관리 효율을 증대할 수 있도록 여러 단체들이 관심을 갖고 다양한 연구·개발을 진행 중에 있다[2, 12, 13, 14, 15]. 본 논문에서는 전력설비 관리를 위한 사물인터넷 플랫폼에서의 필요한 각 요소에 대해서 설명한다.

2. 본론

2.1 IoT 통신 방식

통신 모듈은 사물인터넷에서 일반적으로 실내 환경에서 주로 사용되는 고속 통신 방식을 기준으로 검토하였다. 이는 전력 설비의 대부분이 실내에 있으며, 센서에 따라 데이터 양이 상이하기 때문이다. 이에 따라 공용 통신 모듈을 제작하기 위해서는 환경에 따른 최대 요구 성능을 만족하여야 한다.

〈Table 1〉 IoT Commercial Communication Method

	Wi-Fi	BLE	Zigbee
Rang	10-100m	〉60m (10m for Classic BT)	Depends on specification
Power	Low	Very Low (High for classic BT and medium for others)	High
Latency	Low	3ms (compared to 100ms in classic BT)	Variable
Self healing	Yes	-	Yes
Topologies	Mesh, Star and Cluster-tree	Star	Star, Point-to-Point
Data transmission rate	Up to 250Kbps	1Mbps (BT v4.0: 25Mbps)	11Mbps & 54Mbps (250Mbps: WiFi Direct)
Bandwidth	2.4GHz, 915MHz & 868MHz	2.4GHz only(BT+HS:6-9GHz)	2.4, 3.6 & 5GHz
Transmission technique	DSSS DS/FA	Adaptive FHSS (Classic BT: FHSS)	DSSS, CCK & OFDM

표 1과 같이 Wi-Fi와 BLE, 그리고 Zigbee가 가장 많이 사용되고 있으며, 이에 따라 경제적으로도 경쟁력이 있다. 전력 설비의 경우 상시 전원 사용이 가능하여야 하며, 센서에 의한 고용량 데이터의 전송이 필요할 수 있어 Wi-Fi가 가장 적합하다고 판단하였다. 이외에도 최근 수 Km의 생활영역에 대해서도 배터리 교체 없이도 장기간 통신이 가능한 저전력 장거리 LPWA(Low Power Wide Area)가 사용되고 이다. 그 중 면허대역과 비면허대역

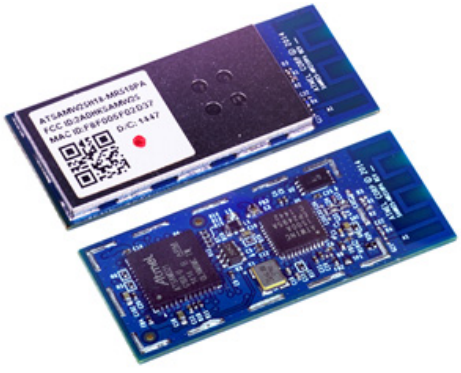
나눌 수 있으며 다양한 유형의 비면허대역 LPWA 네트워크 기술이 시장의 검증을 거쳐 상업적으로 운용 중이며, 최근에는 면허대역에서 운용되는 LPWA 네트워크 기술이 사물에 최적화되어 제공되어 지고 있다. 표 2를 통해 현재 대표적으로 사용되고 있는 주요 LPAW 기술 및 특성을 확인할 수 있다[3].

〈Table 2〉 LPAW Technology and Specificity Comparison

Main Technology	SIGFOX	LoRa	LTE-M	NB-IOT
Coverage	~13Km	~11Km	~11Km	~15Km
Frequency band	Unlicensed Band 8~900MHz 100Hz	Unlicensed Band 8~900MHz 125KHz	Licensed band LTE frequency 1.4MHz	Licensed band LTE frequency 200KHz
Communication speed	~100bps	~50Kbps	~1Mbps	~150Kbps
Roaming	No	No	No	No
Battery life	~10years	~10years	~10years	~10years
Availability (Korea)	Under review	SKT applied	Under review	Under review

전력설비 관리를 위한 측정 장비를 IoT 플랫폼에서는 센서라 정의할 수 있으며, 기존 센서를 활용하기 위해서는 통신 기능이 추가되어야 하며, 이에 따라 센서에 사용 가능한 통신 모듈을 제작하여야 한다.

그림 1과 같이 상용 Wi-Fi 모듈의 경우 PCB 형태로 사용자에게 제공되며, 외부 장비와 연동을 위한 UART와 ISP 같은 표준 통신 방식과 병렬연결을 위한 GPIO(General-purpose input/output)을 지원한다.



[Fig. 1] Commercial Communication Module

상용 통신 모듈은 대부분 안테나 일체형으로 구성되어지며, 센서의 데이터를 받아 외부 데이터 수집 장치에 전송한다. 이 경우 기존의 인터넷 망을 사용하여 원격에 있는 서버에 데이터를 전달함으로써 사용자가 원하는 설치 장소의 상태 모니터링을 가능하게 하며, 필요에 따라 제어도 가능하게 한다. 이러한 상용 모듈의 사용은 기존의 센서 시스템을 IoT로 쉽게 변경하여 적용할 수 있도록 해주며 시장의 변화에 빠르게 대응 할 수 있도록 한다.

2.2 통신 모듈 설계

IoT 플랫폼은 통신 모듈에서 사용하는 통신방식 이외에 데이터 전달 형태에 따라 여러 프로토콜을 사용할 수 있다. IoT 플랫폼의 경우 센서 노드에서 MCU의 성능을 고려하여 가급적 가벼운 프로토콜을 선호한다.

그러나 데이터의 중요도에 따라서는 안전성도 고려되어야 하며, 이러한 조건을 만족하는 IoT에 적합한 프로토콜은 표 3과 같이 개발되어지고 있으며, IoT 플랫폼 업체를 통해 사용되어지고 있다[4,5].

〈Table 3〉 IoT Commercial Communication Protocol

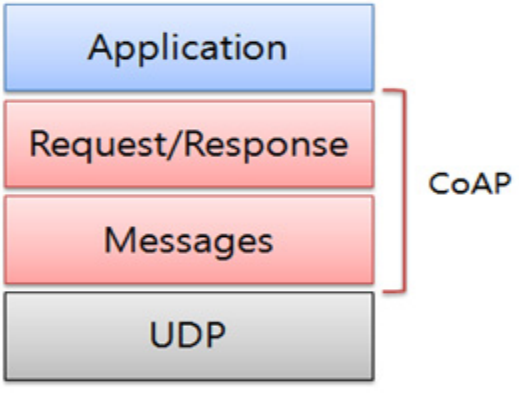
PROTOCOL	MQTT	CoAP	XMPP	HTTPI
Transport	TCP/IP	UDP	TCP/IP	TCP/IP
Messaging	Publish/Subscribe Request /Response	Request/Response	Publish/Subscribe Request /Response	Request/Response
Cellular	Excellent	Excellent	Excellent	Excellent
Low Power	Fair	Excellent	Fair	Fair
Primary	Message	Web service Document	Message	Web service Document
Energy	Low	Low	High	High

표 3에 설명된 프로토콜은 IoT에서 일반적으로 사용되는 표준 프로토콜이다. 사용자는 적용 환경에 따라 표준 프로토콜 중 선택하여 사용 할 수 있다. 최근에는 상이한 프로토콜에 대한 연동도 활발히 연구되고 있으며, 이는 향후 IoT 플랫폼이 상호 연동이 가능하여 여러 데이터의 조합으로 기존의 한계를 벗어나 효율성을 극대화 할 수 있는 다양한 방법을 찾을 것으로 보인다.

사물인터넷에서 사용되는 하드웨어 대부분은 제한된 리소스를 가지며, 이에 따라 적용 할 수 있는 통신 프로토콜은 저용량의 리소스를 사용하여 구현이 가능하여야 한다. 표 3에서 이러한 요구사항을 만족하는 것으로는 MQTT와 CoAP이 있으며, 최근에 IBM과 같은 다국적 기업에서는 MQTT를 적극적으로 지원하고 있다. MQTT 프로토콜은 외부 방해요소가 강한 환경에서 모니터링 센서, 측정 센서 등의 분석, 검출하는 소형 기기들의 신뢰성

있는 데이터 전송을 위한 프로토콜이다. 이는 OASIS (Organization for the Advancement of Structured Information Standards)에서 사물인터넷 표준 프로토콜로 선정했다. MQTT 프로토콜은 하단 프로토콜로 TCP를 이용하고 Broker는 서버를 통해 하단의 프로토콜 데이터를 중계한다. 이러한 중계 과정에서 사물기기들 사이에 전달되는 손실 데이터들을 복구하여 전달함으로써 신뢰성 높은 데이터 전송이 가능한 프로토콜이다.

CoAP은 IETF(Internet Engineering Task Force)에서 표준화한 프로토콜로 상대적으로 적은 전력을 소모하고, 신뢰성 있는 통신을 제공함으로써, 사물인터넷 환경에서 다양한 서비스를 제공할 수 있다. CoAP 프로토콜은 UDP 기반의 Request/Response 모델로 동작하며, 이 모델의 구조는 그림 2와 같이 UDP 기반의 CoAP(Message, Request/Response)가 있고 마지막으로 Application으로 구성되어 있다. 데이터 신뢰도를 위해 재전송 및 타이머 관리를 할 수 있다. 또한 보안을 위해 DTLS(Datagram Transport Layer Security)가 UDP와 CoAP 사이에 적용되기도 한다[6].



[Fig. 2] CoAP Hierarchy

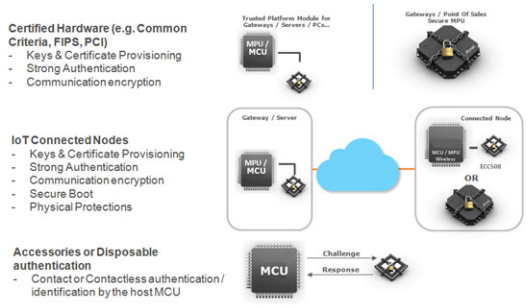
2.3 보안 설계

사물인터넷 플랫폼은 기본적으로 상용망을 사용하고 있으며 이는 외부로부터의 보안에 취약할 수 있다는 문제점을 가지고 있다. 이러한 문제를 극복하기 위해서 상용망에서의 보안 솔루션 연구가 많이 이루어지고 있으며, 현재 대부분의 금융 서비스 분야에서는 보안 솔루션이 사용되어지고 있다. 이에 따라 사물인터넷의 경우도 상용망을 통한 사용 환경에서 전력설비에 대한 관리 서비스를 안전하게 사용가기 위해 적용되는 사물인터넷 플랫폼 특성에 맞추어 개발되고 있는 보안 관련 암호체계를 검토하여 적용하여야 한다. 보안의 기본 요소인 인증과 기밀성, 그리고 무결성이 모두 보장되어야 하며, 이를 위해 최근에는 ECC(Elliptic Curve Cryptosystem) 기반으로 보안 알고리즘을 개발하여 적용하고 있다. 표 4와 같이 여러 보안체계 중에서 ECC가 성능대비 가장 낮은 리소스를 사용하도록 하며, 이는 사물인터넷 특성에 보다 적합한 알고리즘으로 평가되고 있다[7].

〈Table 4〉 Cryptosystem Type and Performance

Security Bit	Symmetric Encryption Algorithm	Minimum Size (bit) of Public Key	
		RSA	ECC
80	Skipjack	1024	160
112	3DES	2048	224
128	AES-128	3072	256
192	AES-192	7680	384
256	AES-256	15360	512

ECC(Elliptic Curve Cryptosystem)를 사물인터넷 기기에서 사용하기 위해서는 MCU에 모든 기능을 구현하기 보다는 이미 상용화된 경쟁력 있는 솔루션을 사용하는 것이 효과적이며, 이에 따라 그림 3의 여러 종류의 정보 보안에서도 IoT 분야에 적합하게 적용 할 수 있는 솔루션이다.

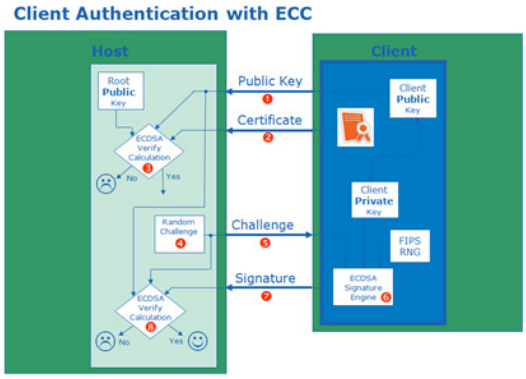


[Fig. 3] Types of security solutions

타원 곡선 알고리즘(Elliptic Curve Cryptography Algorithm)은 이산대수에서 사용하는 유한체의 곱셈군을 타원곡선군으로 대치한 암호체계로써, 표 4와 같이 다른 암호체계에 비교하여 짧은 키(Key) 사이즈로 대등한 안전도를 가지는 것이 큰 장점이다.

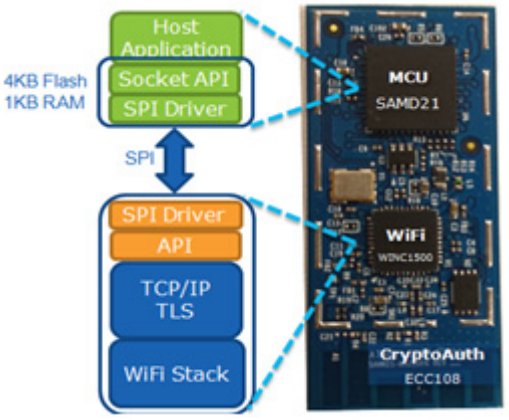
ECC 알고리즘을 이용한 암호 시스템은 난수와 결합한 공개키를 각 클라이언트(Client)에 공유하여 공격자가 유추할 수 없는 비밀 키로 동기화하고, 암호화하는 순

서로 그림 4와 같이 진행된다. 이와 같은 암호 시스템은 ECDSA(Elliptic Curve. DSA)을 통해 키에 대한 인증과 메시지를 암호화하며, 현재 ECC 알고리즘 기반으로 암호 기법 중 가장 많이 사용하는 암호 알고리즘이다. 메시지 암호화는 비밀 키 계산 이후 클라이언트 메시지와 비밀 키를 연산하여 호스트(Host) 송신 과정과 호스트가 비밀 키를 이용하여 암호화 된 메시지를 연산하는 과정으로 진행된다[8].



[Fig. 4] ECC operation flow chart

ECC 알고리즘은 그림 5와 같이 이미 상용화된 통신 모듈에 적용되고 있다. 이는 적용되는 센서의 MCU(Micro Controller Unit) 성능에 상관없이 개발된 보안 알고리즘을 일관성 있게 적용 가능하게 함으로써 경제성을 확보 할 수 있도록 한다. 최근에는 Wi-Fi 이외에도 BLE나 Zigbee와 같은 저전력 사물인터넷의 센서 노드에도 적용하기 위한 솔루션 개발이 이루어지고 있다.



[Fig. 5] Commercial communication module with ECC

2.4 서버 설계

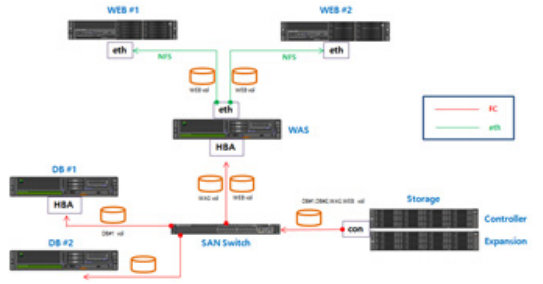
사물인터넷 서버는 실시간으로 외부 센서에 입력되는 데이터를 기반으로 하여 저장 및 분류를 통한 부가서비스를 제공하며, 이를 위한 하드웨어가 구축되어야 한다. 서버의 필요 성능은 실시간 데이터의 양에 따라 달라지며, 사물인터넷의 경우 센서가 동시에 접속을 통해 일정하게 데이터를 전달하는 특성이 있고 향후 지속적인 센서 추가에도 대응을 할 수 있는 구조가 되어야 한다. 본 논문에서는 위와 같은 조건을 만족하기 위한 서버 성능 및 구조의 한 가지 방법을 제시하고자 한다. 전압, 전류, 위상, 주파수 등의 다양한 전력상태 정보를 모니터링 하는 경우 서버의 필요한 성능은 각각의 아날로그의 입력 신호는 Phasor 연산을 위해 60Hz 기준으로 초당 128회의 샘플링과 10-bit의 분해능으로 디지털 변환하여 서버에 전달할 수 있는 성능이 되어야 한다. 이러한 경우 ±95% 신뢰도의 상태정보 값을 얻을 수 있다. 데이터 통신의 경우 단말이 아닌 인터넷을 통한 데이터 전달방식인 경우 지속적인 센서 추가에 대응할 수 있고 다양한 부가서비스를 제공할 수 있다.[1]

[Fig. 6] IoT Service Structure

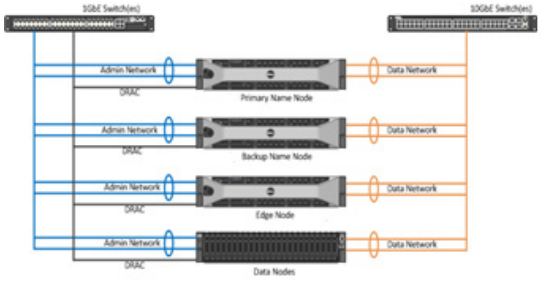
2.4.1 하드웨어 설계

사물인터넷 서버는 기존 클라우드 서비스 서버와 하드웨어적으로는 차이가 없다. 이에 따라 필요한 하드웨어 구성은 그림 7과 같이 일반 클라우드 서비스 서버와 동일한 구성을 갖는다. 다만, 최근에 빅 데이터 처리에 대한 성능의 한계성을 극복하기 위해서 분산처리를 목적으로 그림 7과 같이 Name Node와 Edge Node, 그리고 여러 대의 Data Node로 하드웨어를 분산하여 구성하며, 이를 관리하기 위하여 분산처리가 가능한 OS에 대량의 자료를 처리할 수 있는 분산 응용 프로그램을 프레임워

크를 설치한다. 최근에는 프리웨어 자바 소프트웨어인 아파치 하둡(Apache Hadoop, High-Availability Distributed Object-Oriented Platform)을 고려하고 있다[9,10].



(a) Web server hardware

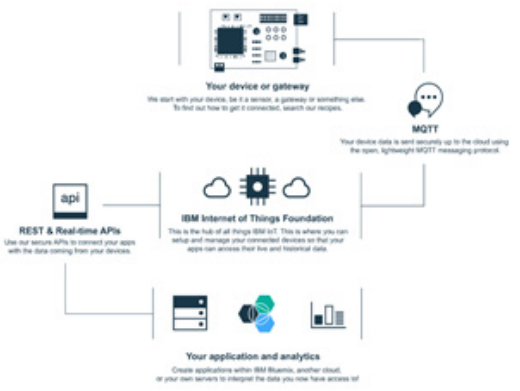


(b) Server Diagram

[Fig. 7] Server Structure

2.4.2 소프트웨어 설계

IoT 서버의 경우 IBM과 Google, 그리고 Microsoft와 같은 글로벌 소프트웨어 업체들이 클라우드 서비스를 기반으로 다양한 사물인터넷 관련 서비스를 개발하고 있으며, 국내의 경우 통신 사업자(SKT, KT, LG U+) 기반으로 각각의 독자적 플랫폼을 운영하고 있다. 전력설비의 경우 국내 통신사 플랫폼을 통해 운영하기에는 센서의 특성 및 분야 자체의 특수성으로 인해 보안 등의 기술이 더 강화된 형태로 설계되어 한다. 그림 8은 해외와 국내에서 주로 사용되는 IoT Platform 구성도를 각각 보여주고 있다. 해외의 경우 소프트웨어 업체가 직접 서버를 운영하여 고객에 대하여 유료 지원을 하는 방향으로 진행되며, 국내의 경우 통신사를 통해 서비스를 확대하는 방향으로 진행되고 있다. 전력분야의 경우 국가 기관이나 협회를 통해 DB 구축과 외부 원격 모니터링 서비스를 진행하고 있으나, 일반 고객을 상대로 Open Platform 서비스의 제공은 준비하고 있지 않다.



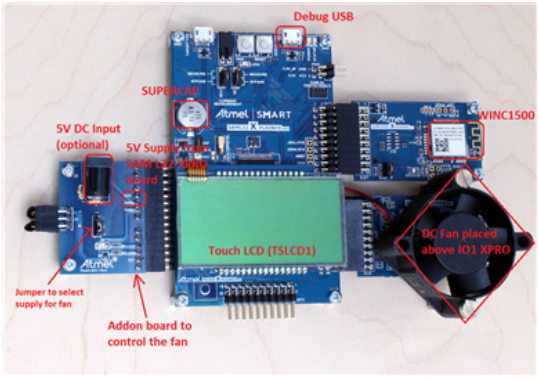
(a) Overseas IoT Platform Service

(b) Domestic IoT Platform Service

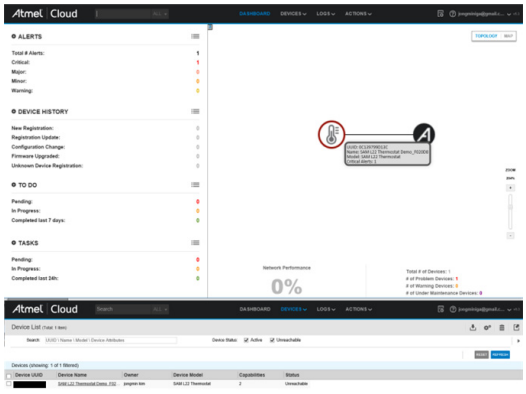
[Fig. 8] IoT Platform Structure

2.5 IoT 모듈과 서버 연동

본 논문에서는 IoT 모듈을 상용 제품을 사용하였으며, 해당 모듈에 프로그램 작성을 통해 상용 제품에서 지원하는 IoT 플랫폼 서비스를 제공하는 서버를 제작하였다. 또한, 반도체 회사에서 자사 제품의 보안 솔루션이 적용된 모듈에 대하여 자체 클라우드 서비스를 제공하고 있어 이를 IoT 모듈에 적용하였다. 설계된 IoT 모듈은 그림 9와 같이 ECC 기반의 보안 칩이 포함되어 있으며, 이를 기반으로 그림 10의 클라우드에 37Byte의 Activation Code을 이용하여 ECC 알고리즘을 기반의 상호 인증 시스템을 구현한다[11].



[Fig. 9] IoT Sensor Module



[Fig. 10] IoT Cloud

3. 결론

본 논문에서는 전력설비 관리를 위한 사물인터넷 플랫폼 적용을 위한 각 요소들을 분석하였다. 관련 요소로는 사물간의 연결을 위한 통신 방식과 그에 따른 프로토콜, 그리고 보안 요소를 분석하였으며, 이를 시스템에 적용하기 위한 기준을 제안하였다. 이에 따라 통신 방식의 경우 Wi-Fi 기반으로 IoT에 적합한 MQTT와 CoAP을 적용하며, 이에 대한 보안 부분에 대해서는 ECC을 적용함으로써 안전성을 확보하며, 이를 운영 유지하기 위하여 클라우드 시스템을 도입한다. 이는 기 개발된 기술에 대한 분석과 적용을 통해 현재 IoT 구축을 위한 기술적 환경과 적용 방식의 예를 보여줌으로써 향후 IoT 시스템 구축에 대한 효율적 접근이 가능하도록 하였다. 특히 상용망 사용에 대한 위험한 요소를 분석하고 보안함으로써 보다 경쟁력 있는 솔루션 구축이 가능하다.

본 논문은 제안된 내용에 따라 기존 전력설비와 신재생에너지 관련 신규 설비들에 의한 전기환경변화에 대응하기 위해서는 사물인터넷의 도입을 위한 기술적 요소를 연구함으로써 미래 전력설비 안전관리에 보다 효과적인 플랫폼 제공이 될 수 있도록 한다. 추후 실제 장비 적용을 통한 사례와 플랫폼을 통한 데이터 축척과 이에 따른 빅 데이터 활용에 대한 연구가 필요하다.

REFERENCES

[1] Y.D.Lee, "IoT-based Switchgear Status Monitoring System", Journal of The Institute of Information and Communication Sciences, Vol.20, No.1, pp.200-206, 2016.

[2] H.S.Choi and, W.S.Lee, "IoT Platform Technology and International Standardization Trend", Broadcasting and Media, Vol. 20, No, 3, pp.8-30, 2015.

[3] T.J.Park, "IoT LPWA Technology Trend, Korea Electronics and Telecommunications Research Institute", Korea Electromagnetic Engineering Society Vol.27 No.4, pp.29-31

[4] D.H.Kim, M.K.Kim, and Y. G. Hong, "IoT Applied Communication Technology: IoT Communication Technology", Information and Communication Open Course 32 (12 (Separate No.2)), pp.3-11, 2015.

[5] B.J.Kim and S.H.Cho, "IoT Middleware Lightweight Message Protocol Research Trends", The Korean Institute of Electronics Engineers' General Conference and Fall Conference, pp.674-676, 2014.

[6] O.O.Seo and D.H.Lee, "Lightweight Protocol and IETF CoAP Protocol for the Internet of Things(IoT) Environment, Information Technology Promotion Center", Weekly Technology Trends, pp.1-11, 2015.

[7] Kerry Maletsky, RSA vs ECC Comparison for Embedded Systems, Ateml-8951A-CryptoAuth-RSA-ECC-Comparision-Embedded-Systems-WhitePaper, PP.1-3, 2015

[8] N.H.Kim and C.S.Hong, "Secure MQTT Protocol based on Lightweight Encryption Algorithm", 43rd Annual General Meeting and Winter Conference, Korea Information Science Society, PP. 757-759, 2016.

[9] Armando Acosta, Kris Applegate, Dave Jaffe, Rob Wilbert, Intel® Distribution for Apache Hadoop™ on Dell PowerEdge Servers, A Dell Technical White Paper, PP.1-25, 2013.

[10] Y.T.Cho, W.J,Lee, I.K.Lee, E.H.Lee, and J.J.Choi, "Smart Grid Power Data Analysis using Hadoop-based Big Data System", Journal of the Korean Institute of Electrical Engineers Vol.64, No.2, pp.85-91, 2015.

[11] Atmel 42722A SAM L22 Thermostat IoT Node AT15347 Application Note, Atmel Corporation, PP.1-29, 2016.

[12] S.C.Jang and J.W.Lee, “Development of Intelligent IoT Exhaustion System for Bag Filter Collector”, Journal of The Korea Internet of Things Society Vol. 5, No. 1, pp. 29-34, 2019.

[13] J.Y.Lim, “An Analysis on the Trends and Issues of Convergence Technology Research”, Journal of The Korea Internet of Things Society Vol. 4, No. 1, pp. 23-29, 2019.

[14] T.K.Kim, “A Study on Smart Warning Triangle”, Journal of The Korea Internet of Things Society Vol. 4, No. 1, pp. 37-41, 2018.

[15] J.H.Hong, S.H.Kim, and K.H.Lee, “Design of video surveillance system using k-means clustering”, Journal of The Korea Internet of Things Society Vol. 3, No. 2, pp. 1-5, 2017.

장 경 배(Kyung-Bae Jang) [정회원]

- 1995년 2월 : 광주과학기술원 기전공학과(공학석사)
- 2006년 8월 : 고려대학교 일반대학원 전기공학과(공학박사)
- 1997년 2월 ~ 2000년 3월 : SK 하이닉스반도체 주임연구원
- 2000년 4월 ~ 2008년 8월 : 현대모비스 선임연구원
- 2008년 12월 ~ 2013년 5월 보건복지부 국립재활원 공업연구관
- 2014년 3월 ~ 현재 : 고려사이버대학교 기계제어공학과 교수

〈관심분야〉
사물인터넷, 제어시스템, 로봇