Journal of Korea Multimedia Society Vol. 20, No. 12, December 2017(pp. 1928-1939)
https://doi.org/10.9717/kmms.2017.20.12.1928

클라우드와 포그 컴퓨팅 기반 IoT 서비스를 위한 보안 프레임워크 연구

신민정†, 김성운††

A Study on the Security Framework for IoT Services based on Cloud and Fog Computing

Minjeong Shin†, Sungun Kim††

ABSTRACT

Fog computing is another paradigm of the cloud computing, which extends the ubiquitous services to applications on many connected devices in the IoT (Internet of Things). In general, if we access a lot of IoT devices with existing cloud, we waste a huge amount of bandwidth and work efficiency becomes low. So we apply the paradigm called fog between IoT devices and cloud. The network architecture based on cloud and fog computing discloses the security and privacy issues according to mixed paradigm. There are so many security issues in many aspects. Moreover many IoT devices are connected at fog and they generate much data, therefore light and efficient security mechanism is needed. For example, with inappropriate encryption or authentication algorithm, it causes a huge bandwidth loss. In this paper, we consider issues related with data encryption and authentication mechanism in the network architecture for cloud and fog-based M2M (Machine to Machine) IoT services. This includes trusted encryption and authentication algorithm, and key generation method. The contribution of this paper is to provide efficient security mechanisms for the proposed service architecture. We implemented the envisaged conceptual security check mechanisms and verified their performance.

Key words: Internet of Things (IoT), Everything to Everyone (E2E), Operational Technology (OT), Cloud Computing, Fog Computing, Message Integrity Code (MIC), Secret Tag (ST), Encryption, Security Check Mechanism (SCM).

1. 서 론

제3차 산업 혁명은 제한된 컴퓨터 기능 및 능력을 활용한 정보통신기술(ICT: Information and Communication Technology)이 산업에 적용되어 자동화를 통해 대량 생산하는 데에서 그 의의를 찾을 수 있다[1]. 반면에 현재 전개되는 제4차 산업 혁명은 인공지능과 빅 데이터를 활용하는 고도의 초지능성 컴퓨팅 기술들이 모바일 및 5G 기술을 활용하여 다양한 사물 인터넷(IoT: Internet of Things) 응용들을 광역화시키는 초연결성 정보통신기술과 결합된 형태로 다양한 산업 분야에 융합되어 고품질의 지능적 실시간 서비스를 실현하는 패러다임이다[1].

그러나 사람과 사물, 사물과 사물이 인터넷 통신

※ Corresponding Author : Sungun Kim, Address: (48513) Yongso-ro 45, Nam-gu, Busan, Korea, TEL : +82-51-629-6235, FAX : +82-51-629-6229, E-mail : kimsu@pknu.ac.kr
Receipt date : Sep. 6, 2017, Revision date : Oct. 19, 2017
Approval date : Nov. 9, 2017

† Master's degree, Dept. of Information & Communication Eng., Graduate School, Pukyong National University (E-mail : minjung3373@pukyong.ac.kr)
†† Professor, Dept. of Information & Communication Eng., Pukyong National University
※ This research work was supported by the Research Grant of Pukyong National University(2016).

망으로 연결되어 발생된 IoT기반의 막대한 데이터들을 수집 및 분석하여 시간과 공간의 한계를 뛰어넘는 초지능적 서비스를 실현하기 위해서는 이미 언급한 초연결성에 관계된 망 기술이 핵심 요소이다[1]. 여기서 초연결적 망 기술이란 유연한 광대역 정보통신망 구축 기술로 먼저 그 백본에는 인터넷이 활용된다. 그리고 백본망의 양 끝단에는 포그 컴퓨팅(Fog computing) 기술이 다양한 사물통신을 위한 접속망 기술로 적용되며 또한 다른 끝단에는 클라우드 컴퓨팅(Cloud computing) 기술이 초지능성 컴퓨팅 센터와 연결되는 개념이다[2].

클라우드 컴퓨팅 기술은 고비용의 저장 및 처리 시스템을 인터넷을 통해 임대 사용하는 온-디맨드 컴퓨터 환경이다[3]. 외부 서버에 정보가 저장됨으로써 시스템 활용도와 접근성 및 확장성이 뛰어나 초연결성 구현에 핵심적이고 경제적인 기술로 활용된다. 그러나 엄청난 수의 다양한 IoT 장치들의 전개가 필수적인 초지능적 서비스를 위한 유연한 사물 지능통신의 달성은 클라우드 컴퓨팅 기술만으로 이루어지기 어렵다. 즉 IoT 장치들로부터 기하급수적으로 생성되는 데이터들을 클라우드로 전송하여 분석하면 막대한 대역폭 소요와 실시간 데이터들에 대한 처리 지연이 발생하여 클라우드 컴퓨팅 기술만으로는 그 요구를 충족시키기 어렵다. 그래서 포그 컴퓨팅 기술이 문제점을 해결하는 대안으로 활용된다[2,4,5].

포그 컴퓨팅 기술은 목적된 서비스를 위해 지역 서버를 해당 범위 내에 배치된 IoT 장치들(센서 또는 각종 단말) 근처에 위치시켜 민감한 실시간 처리 데이터는 지역 서버에서 분산 처리하고, 필터링 후 저장이 필요한 데이터들은 한 단계 위의 서버에 보관하고 활용하여 클라우드 기술의 한계를 보완하는 패러다임이다[2,5]. 사물 인터넷과 포그 컴퓨팅 기술이 결합되어 데이터 수집과 분석 및 실행이 실행 장치와 가까운 위치에서 이루어지면 서비스 지연시간의 최소화, 망 대역폭의 효율적인 활용, 보안성 향상 등의 장점을 살릴 수 있다. 그러나 포그 컴퓨팅 기술만으로는 빅 데이터 활용 등을 위한 초지능적 서비스의 구현에 한계가 있으므로 클라우드와 포그 컴퓨팅 패러다임을 적절히 조합하여 위에서 언급된 여러 가지 제약들을 극복할 수 있다[2-5].

일반적으로 초연결성을 달성하는 망에서는 데이터 위조 및 변조 그리고 클라우드 및 포그 컴퓨팅 기술 적용 과정에서 발생하는 위협들이 존재하기 때문에 지역 서버 뿐 만아니라 클라우드 컴퓨팅을 위한 가상 서버에서의 정보 처리 및 전달 과정 등에서도 다양한 보안 문제가 대두된다[2,3]. 이를 극복하기 위해 본 논문에서는 공장 자동화나 생산 자동화 등에 활용되는 적합한 망 프레임워크를 제시하고, 이 환경(클라우드 및 포그 컴퓨팅 기반의 IoT 서비스를 위한 환경)에서 효율적으로 동작할 수 있는 보안 메커니즘을 구현한다. 일반적으로 공장 자동화나 생산 자동화 등의 IoT 응용 서비스에서 주고받는 데이터 프레임 길이는 짧고 실시간적인 특성을 가지므로 신속성이 가장 중요하다. 그래서 기존의 암호화 및 복호화 또는 메시지 무결성 인증 기술을 그대로 사용하는 것은 비효율적이다.

본 논문의 2장에서는 다양한 사물지능통신서비스 실현에 필요한 망 구축에 관련된 핵심 기술들을 설명하고 공장 자동화나 생산 자동화 등에 활용되는 적합한 망 프레임워크를 제시하며 이 환경에서 요구되는 보안 문제를 분석한다. 3장에서는 제시한 망 환경에서 효율적으로 동작하는 보안 메커니즘의 구현에 대해 기술한다. 4장에서는 제안된 보안 기술과 기존의 보안 기술을 비교하며 그 성능을 평가한다. 마지막으로 5장에서는 제안된 보안 기술의 적용 방안과 확장성에 대해 결론 맺는다.

2. 사물지능통신망 구축 기술

2.1 클라우드와 포그 컴퓨팅 기반 사물지능통신서비스를 위한 망구조

다양한 사물지능통신서비스를 원활하게 구현하기 위해서는 망 측면에서 초연결성이 보장되어야하고 실시간적인 데이터 흐름이 필수적이다. 먼저 Fig. 1은 일반적인 사물통신을 위한 망구조이다.

이 구조는 단순히 공장자동화나 생산자동화를 위

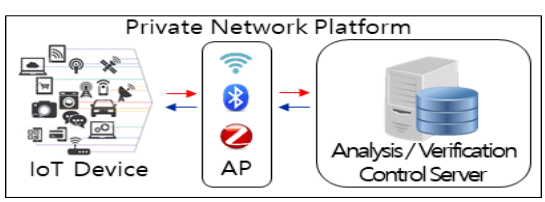


Fig. 1. Network architecture for general M2M IoT services.

해 IT 기술과 해당산업 분야 기술이 융합된 형태로 이미 일어난 사실의 분석 또는 형태 탐지나 검증 등의 수동적 서비스로 활용되는 사설망 환경이다. 위의 망구조는 가까운 미래에 발생할 사건에 대한 예측과 전망 및 전조 예고(초지능 컴퓨팅 기술이 요구됨.)등에 관계된 서비스로의 대비 및 대응 등에 한계가 있다. 이에 대한 대응으로 IT와 OT(Operational Technology) 기술의 융합이 필요하며 Fig. 2와 같은 클라우드 컴퓨팅에 기초한 망구조가 활용된다[6].

Fig. 2의 구조에서 클라우드 컴퓨팅 기술의 활용은 고비용의 저장 및 처리 시스템을 인터넷을 통해 임대 사용하는 온-디맨드 컴퓨터 환경으로 외부 서버에 차 후 활용될 정보가 저장됨으로써 시스템 활용도와 접근성 및 확장성이 뛰어나 초연결성 구현에 핵심적이고 경제적인 기술로 고려된다. 그러나 엄청난 수의 IoT 장치들의 전개가 필수적인 초지능적 서비스를 위해서는 클라우드 컴퓨팅 기술만으로는 유연한 사물지능통신이 이루어지기 어렵다. 즉 IoT 장치들로부터 기하급수적으로 생성되는 데이터들을 클라우드로 전송하여 분석하면 막대한 대역폭 소요와 실시간 데이터들에 대한 처리 지연이 발생하므로 지역망 영역에서 컴퓨팅 능력이 필요한 실시간 응용서비스들은 그 요구를 충족시키기 어렵다.

Fig. 3은 위에서 설명한 Fig. 1과 Fig. 2의 망구조들에서 발생되는 여러 가지 문제점들을 해결하기 위한 포그 및 클라우드 컴퓨팅의 융합 개념에 기반한

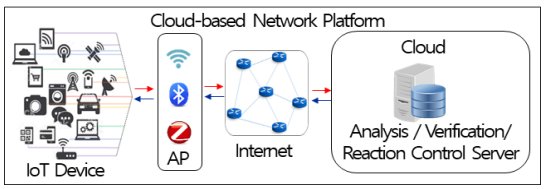


Fig. 2. Network architecture for Cloud-based M2M IoT services.

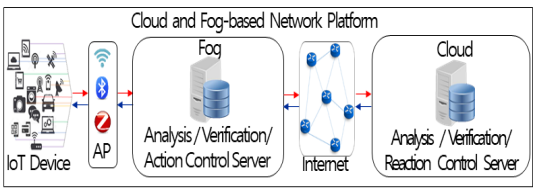


Fig. 3. Network architecture for Cloud and Fog-based M2M IoT services.

망구조이다.

여기서 포그 컴퓨팅 기술은 목적된 서비스를 위해 지역 서버를 해당 범위 내에 배치된 IoT 장치들(센서 또는 각종 단말) 근처에 위치시켜 민감한 실시간 처리 데이터는 지역 서버에서 분산 처리 및 대응하고, 필터링 후 저장이 필요한 데이터들은 한 단계 위의 서버에 보관하여 분석과 대비 및 미래 대응 등의 초지능성 서비스를 위해 활용함으로써 클라우드 기술의 한계를 보완하는 패러다임이다[4,5]. 결과적으로 포그 컴퓨팅 기술만으로는 빅 데이터 활용 등을 위한 초지능적 서비스의 구현에 한계가 있으므로 클라우드와 포그 컴퓨팅 패러다임을 적절히 조합하여 서론에서 언급된 여러 가지 제약들을 극복할 수 있다.

2.2 클라우드 컴퓨팅

클라우드 컴퓨팅의 주요 기능은 가상화이며, 가상화란 물리적인 자원을 이용하여 논리적인 서비스를 제공하고 해당 서비스를 다수의 사용자가 공유할 수 있도록 하는 기술이다. 즉 클라우드 컴퓨팅은 가상화되고 동적인 자원을 활용하므로 IoT 서비스를 제공함에 있어 중요한 IT 인프라 기술 패러다임이다.

클라우드 컴퓨팅은 제공되는 서비스에 따라 세 가지의 서비스 모델(Service model)과 서비스 전개 형태에 따라 세 가지의 배치 모델(Deployment model)로 나뉜다[2]. 서비스 모델은 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), 그리고 SaaS(Software as a Service)로 구분한다. IaaS는 처리, 저장, 접근망 등 IT 서비스 구현에 관계되는 기본 자원을 제공하는 모델이다. PaaS는 필요한 응용 프로그램들을 개발할 수 있는 플랫폼을 임대 제공하는 형태로 데이터베이스, 개발 프레임워크, 실행에 필요한 라이브러리 및 모듈 등을 제공한다. SaaS는 사용자에게 응용 프로그램을 제공하는 소프트웨어 모델로 원하는 서비스에 관계되는 프로그램을 구입하여 사용하는 형태이다[2].

한편 배치 모델은 사설(Private Cloud), 공용(Public Cloud) 그리고 혼성(Hybrid Cloud) 모델로 로 구분된다[2]. 사설 클라우드는 전용 클라우드 형태로 허가된 하나의 기업만이 접근 가능하므로 상대적으로 보안성이 좋은 모델이다. 공용 클라우드는 여러 기업이 하나의 클라우드를 공유하는 형태이며 자원이 어디에 위치하고 어디서 작동하는지 알기 어려워 보안

에 대해 여러 가지 위협 요소를 가진다. 혼성 클라우드는 사설 및 공용 모델이 조합된 형태로 적용될 서비스 환경의 특성에 따라 알맞은 모델을 교차적으로 사용할 수 있다는 장점이 있다.

2.3 포그 컴퓨팅

포그 컴퓨팅 기술은 클라우드 컴퓨팅의 서비스를 인터넷(혹은 외부 연결망) 경계 지점으로 확장시킨 패러다임으로 시스코가 제안하였다[5,6]. 즉 목적된 서비스를 위해 지역 서버를 해당 범위 내에 배치된 IoT 장치들(센서 또는 각종 단말) 근처에 위치시켜 민감한 실시간 처리 데이터는 지역 서버에서 분산 처리하고, 필터링 후 저장이 필요한 데이터들은 한 단계 위의 서버에 보관하고 다양하게 활용함으로써 클라우드 기술의 한계를 보완하는 패러다임이다[2-5].

사물 인터넷과 포그 컴퓨팅 기술이 결합되어 데이터 수집과 분석 및 실행이 실행 장치와 가까운 위치에서 이뤄지면 서비스 지연시간의 최소화, 망 대역폭의 효율적인 활용, 보안성 향상 등의 장점을 살릴 수 있다.

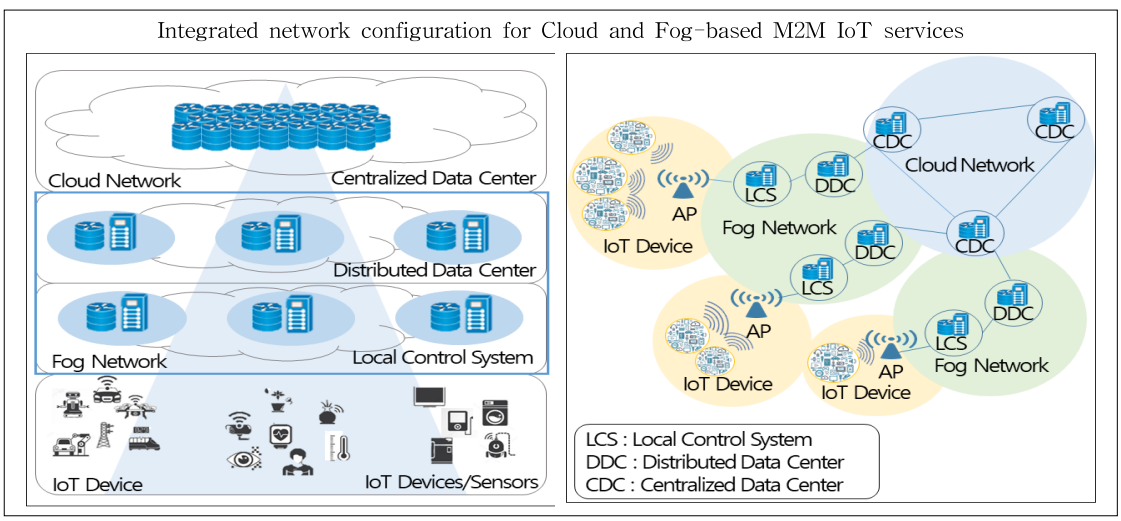
2.4 융합된 포그 및 클라우드 컴퓨팅

일반적으로 포그 컴퓨팅 기술만으로는 빅 데이터 활용 등을 위한 초지능적 서비스의 구현에 한계가 있으므로 클라우드와 포그 컴퓨팅 패러다임을 적절히 조합하여 위에서 언급된 여러 가지 제약들을 극복할 수 있다[2,4,5]. Fig. 4는 클라우드와 포그 컴퓨팅 개념을 조합한 망 개념도이다.

Fig. 4-a의 수직 구조에서 최하위 단은 다양한 IoT 장치들로 실시간 데이터 수집하여 바로 위층의 지역 제어시스템(LCS: Local Control System)으로 전달하고, LCS는 분석을 통한 IoT 장치 제어와 IT 서비스 제공을 위해 상위단의 분산 데이터센터(DDC: Distributed Data Center)로 전달한다. 그리고 DDC는 LCS으로부터 수신된 데이터들을 추후 OT 서비스 적용을 위해 필터링하여 상단인 클라우드 단의 중앙 집중 데이터센터(CDC: Centralized Data Center)로 전송함으로써 초지능적 서비스를 위해 활용하는 개념이다. 이 과정에서 다양한 CDC들은 상호 연동되어 포괄적인(Global) 망 형성을 함으로써 초연결성을 달성한다. Fig. 4-b는 포그 및 클라우드 컴퓨팅 개념이 IoT와 연동되어 초연결성 및 초지능성 서비스를 제공하는 해당 망의 수평 구조로 M2M을 넘어 E2E(Everything to Everyone)를 달성하는 개념이다[7,8].

2.5 보안 문제

일반적으로 초연결성을 달성하는 망에서는 데이터 위조 및 변조 그리고 클라우드 및 포그 컴퓨팅 기술 적용 과정에서 발생하는 위협들이 존재하기 때



(a) Vertical network configuration (b) Horizontal network configuration

Fig. 4. Integrated network configuration for Cloud and Fog-based M2M IoT services.

Table 1. Threats related to Cloud and Fog computing

Categories	Treats	Characteristics
Server related	Virtualization	Attackers steal information using shared memory through virtual environment[9]
	Management	Information leakage due to separation of ownership and management[9,10]
Network related	Malicious Intrusion	Concerns of malicious user or service intrusion such as DDos, Malware, Spamming, or etc.[9]
	Routing Hindrance	Routing hindrances such as Routing Information modulation and counterfeiting, sending error message, interrupting network transmission, or etc[9].
	Network Failure	Service interruption due to Network hindrance
Cryptography algorithm related	Encryption Algorithm	Threats for data integrity or restriction on use of database utilization services due to incorrect algorithm implementation[9-11]
	Key Generation	Threats for confidentiality and integrity of key due to third party involvement during generating the key[9-11]
	Integrity	Requires authentication mechanism against message modulation by attackers[9-11]
Human and disaster	Resource Management	Cloud does not have information about where the resources are running and cannot control it[10]
	Personal	Security threats by immoral managers
	Disaster	Service failure by earthquake, typhoon, or etc.

문에 지역 서버 뿐 만아니라 클라우드 컴퓨팅을 위한 가상 서버에서의 정보 처리 및 전달 과정 등에서도 다양한 보안 문제가 대두된다[3,4]. 다음 Table 1은 융합된 포그 및 클라우드 컴퓨팅기반의 사물지능통신서비스를 위한 망구조에서 발생 가능한 보안 위협을 요약한 것이다.

본 논문에서는 Table 1의 모든 보안 위협에 대처하는 방안을 제시하는 것이 아니라, 망 측면의 전송과정에서의 데이터 무결성(위조 및 변조에 대해)을 보장하는 보안 프레임워크를 연구한다. 이는 제시되는 방법이 모든 보안 위협에 대한 가장 근본적이고 핵심적이기 때문이다.

3. 제안된 보안 프레임워크

3.1 보안 프레임워크 접근 방향 및 관련 기술

포그 및 클라우드 컴퓨팅 개념에 기반 된 M2M이나 E2E 달성 사물지능통신서비스를 위한 망구조에서는 망간 전달 데이터의 안전성 보장을 위해 크게 두 가지로 접근할 수 있다[7,8]. 먼저 하나는 서비스 대상 데이터의 암호화와 복호화로의 접근이고 다른 하나는 보안 태그(Authentication tag)를 붙여 접근하는 방법이다. 암호화와 복호화로의 접근은 안전한 키의 생성 및 전달과 이를 활용한 암호화 및 복호화 알고리즘이 주된 관점으로 DES(Data Encryption Standard)나 AES(Advanced Encryption Standard)가 대표적인 예이다[11,12]. 이 방법은 내용 변조나 위조에는 대처가 어렵기 때문에 이를 보완하는 방법으로 보안 태그를 생성한 후 보내는 데이터와 함께 암호화 및 복호화 과정을 거치는 WPA(WiFi Protected Access) 또는 WPA2(WiFi Protected Access 2) 접근 방법이 있다[13]. 무선 환경에서 사용되는 보안 메커니즘인 WPA2는 AES 알고리즘을 기반으로 CBC-MAC(Cipher Block Chaining Message Authentication Code) 모드 및 CTR(Counter Mode) 모드를 통해 데이터를 암호화하고 무결성을 인증한다[13].

일반적으로 무선 LAN에서 많이 활용되는 WPA2를 본 연구에 적용할 수는 있으나 효율성에서 문제가 있다. 특히 공장 자동화나 생산 자동화 등의 IoT 응용 서비스에서 주고받는 데이터 프레임 길이는 짧고 실시간적인 특성을 가지므로 신속성이 가장 중요하

다. 더욱이 수많은 IoT 장치들로부터 기하급수적으로 생성되는 데이터들에 기존의 암호화 및 복호화 또는 메시지 무결성 인증 기술을 그대로 사용하는 것은 비효율적이다.

본 논문에서 제안하는 보안 프레임워크는 Fig. 5와 같이 3가지 방법들로 구성된다. 먼저 SCM 1(보안 검사 메커니즘 1: Security Check Mechanism 1)은 와이파이(WiFi) 구간에 적용되는 기술로 사설망 환경에서 시간과 효율성을 고려하여 간략화 된 WPA2 개념을 적용한다. 둘째로 SCM 2(보안 검사 메커니즘 2: Security Check Mechanism 2)는 사설망인 LAN 환경에서 적용되는 보안 기술로 송수신 LLC (Logical Link Control)들 간에 간단한 보안 태그를 생성 및 검정하는 개념이다. 셋째로 SCM 3(보안 검사 메커니즘 3: Security Check Mechanism 3)은 HTTP 통신에 대한 클라우드와 포그 컴퓨팅 망 사이에서 데이터 전달의 무결성 제공을 위해 사용되는 보안 태그로, WPA2 방법을 간략하게 적용하여 생성한다[14]. 이 과정에서 암호화 및 복호화 과정을 거치지 않는 이유는, 본 연구에서 제안한 사물지능통신서비스의 클라우드 개념이 전용의 사설 클라우드 형태로 허가된 하나의 사용자만이 접근 가능하므로 상대적으로 보안성이 좋은 모델이기 때문이다. 제안된 보안 메커니즘의 자세한 설명은 다음 3.2 소절에서 기술한다.

3.2 보안 기술 제안

3.2.1 키 생성

보안 태그 생성과 암호화 및 복호화 과정에서는 보안성이 보장된 키 생성 및 적용이 필수적이다. 본 논문에서 제안하는 보안 기술들도 키 생성과 적용 과정에서 보안성 유지가 필요한데, 일반적으로 사용되는 RADIUS 서버(인증 센터)를 이용하는 키 생성 및 인증 절차를 활용하는 것은 문제가 있다[15]. 왜냐하면 수많은 IoT 장치들에서 실시간적으로 발생하는 많은 양의 데이터에 키 생성 및 인증을 거친 후 이를 사용한 암호화 및 복호화 그리고 보안 태그 생성은 비효율적이다. 본 논문에서는 포그 컴퓨팅을 활용하는 사설망 환경에서 키에 대한 기밀성과 보안성을 자체적으로 유지하면서 효과적으로 암호화 및 복호화 그리고 보안 태그 생성에 사용될 수 있는 적합한 키 생성 방법을 제시한다.

먼저 Fig. 5의 보안 검사 메커니즘 1(SCM 1)과 보안 검사 메커니즘 2(SCM 2)에서 사용되는 키는 Fig. 6의 흐름도와 같이 해당 데이터를 전송하는 날짜(월과 일)와 시간(시와 분)을 활용하여 생성한다. 제안 방법은 적용할 4 바이트(첫 번째 바이트: 해당 월의 2진화된 값, 두 번째 바이트: 해당 일의 2진화된 값, 세 번째 바이트: 해당 시의 2진화된 값, 네 번째 바이트: 해당 분의 2진화된 값)로 구성된 시간 블록을 AES 방법에서 사용된 라운드 키 생성기능을 응용하여 키를 만든다[12].

Fig. 6에서 사용되는 $T_{\max}$ 값은 CSMA/CD 혹은 CSMA/CA MAC 프로토콜 동작 원리에 따라 MAC 프레임 송신 시작 시간에서 수신 완료 시간까지의 최대 허용 시간을 의미하며 수신측에서 수신한 시간에서 $T_{\max}$ 값을 뺀 값을 사용하여 임시키로 적용한다[13,16]. 그리고 기밀성을 더욱 강화하기 위하여 S-box(substitution-box) 치환 및 Rcon(round constant) 연산 과정의 반복 횟수를 증가시켜 사용할 수 있다. 단 제안된 키 생성 알고리즘은 사설망 환경에서 키 생성에 대한 기밀성이 완전히 보장된다는 가정

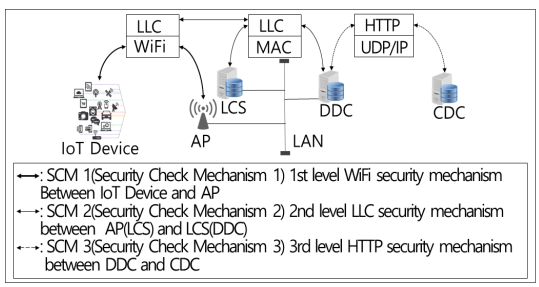


Fig. 5. Proposed security mechanism and framework.

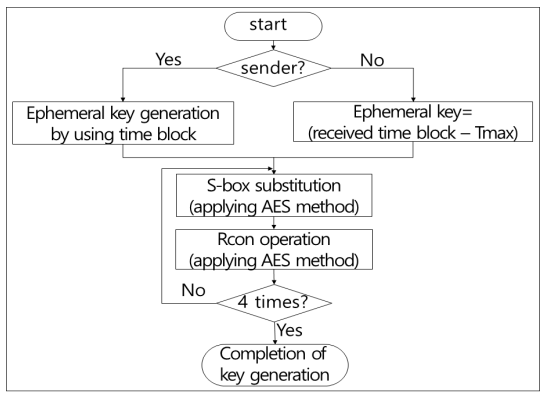


Fig. 6. Key generation method for SCM 1 and SCM 2.

에서 출발한다. 이 과정에서 $T_{\max}$ 값은 몇 백 마이크로초 스케일로 임시키가 다를 경우 보안 위배로 판단하여 재전송하여 해결한다. 이 과정에서는 키로 월, 일, 시, 분으로 사용하므로 적용상의 경험에 의하면 재 전송 횟수는 미미하다.

Fig. 7은 Fig. 5의 DDC(포그 단)와 CDC(클라우드 단) 구간에서 전용의 사설 클라우드 형태로 응용되는 HTTP 통신에 적용할 SCM 3 보안을 위해 8바이트 키를 생성하는 과정이다. 일반적으로 인터넷은 실시간 서비스를 위한 프로토콜이 아니기 때문에 키 생성 과정에서 비밀 값(secret value)을 정하여 사용하고 송수신자의 정확한 식별을 위해 또한 송신자 IP 주소와 수신자 IP 주소를 활용한다.

Fig. 7의 키 생성 과정 중에서 사용되는 비밀 값은 전용의 사설 클라우드 사용자가 정하며 보안 유지가 필요한 4 바이트 값이다. 키 생성 과정은 먼저 송신자 IP 주소와 수신자 IP 주소를 XOR한 값을 그림 7과 같이 4번의 S-box 치환과 Rcon 연산 과정을 거쳐 생성된 키의 첫 4바이트로 사용하고, 이것과 비밀 값을 XOR 연산하여 Fig. 7과 같이 4번의 S-box 치환과 Rcon 연산 과정을 거쳐 나머지 4바이트로 하여 전체 8 바이트의 키를 완성한다. 여기서 중요한 가정은 전용의 사설 클라우드의 사용이고 비밀 값은 절대 유출이 안 되는 상황을 가정한다. 또한 허용되지 않는 IP 주소를 사용하면 키의 일관성이 유지되지 않아 위조 및 변조에 대한 판별로 기밀성 유지가 가능하다. 이 방법에서도 물론 기밀성을 더욱 강화하기 위해서는 S-box 치환 및 Rcon 연산 과정의 반복 횟수를 증가시켜 사용할 수 있다.

3.2.2 SCM 1 보안 방법

본 논문에서는 IoT 장치와 AP간 통신 환경으로 무선 LAN 환경으로 한정한다. 일반적으로 무선 LAN 환경은 위조 및 변조 그 외에 다양한 보안에 대한 위협이 존재한다. 이런 이유로 WPA2에서는 보안 태그 생성과 이를 포함한 송신 데이터를 대상으로 암호화 및 복호화 과정을 거친다. 그러나 WPA2의 적용은 효율성에서 문제가 있다. 특히 공장 자동화나 생산 자동화 등의 IoT 응용 서비스에서 주고받는 데이터 프레임 길이는 짧고 실시간적인 특성을 가지므로 신속성이 가장 중요하다. 더욱이 수많은 IoT 장치들로부터 기하급수적으로 생성되는 데이터들에 기존의 암호화 및 복호화 또는 메시지 무결성 인증 기술을 그대로 사용하는 것은 비효율적이다. 이러한 이유로 사설망 환경에서의 실시간적 특성과 효율성을 고려하여 IoT 장치들과 AP 구간에 적용되는 보안 기술로 Fig. 8과 같이 간략화 된 WPA2 개념을 적용한 방법을 제안한다.

Fig. 8은 SCM 1에 의해 생성된 프레임 구조를 나타낸다. 먼저 보안 태그의 생성 과정은 Fig. 9와 같다. 먼저 송신 대상 데이터를 4 바이트 배수의 블록 단위로 구성하여 3.2.1 소절에서 생성한 4 바이트의 키와 XOR 연산으로 4 바이트의 OUT을 생성 한 후 이것을 마지막 데이터 블록까지 XOR 연산한 최종 결과인 4 바이트 블록을 생성한다. 여기서 송신 데이터가 4 바이트의 배수가 되지 않으면 모든 값이 0인 빈 바이트로 채워서 위의 계산을 수행한다. 보안 태그의 생성은 Merkle-Damgard방식 등의 적용을 향 후 연구할 예정이다.

Fig. 10은 Fig. 8의 송신 데이터와 보안 태그를 암

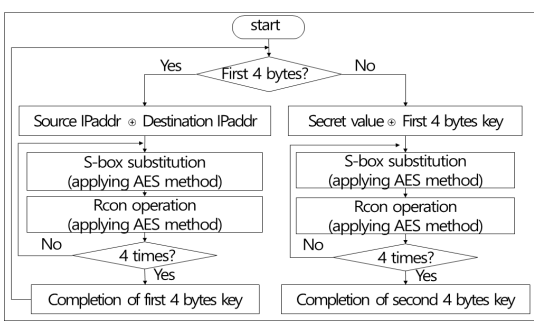


Fig. 7. Key generation method for SCM 3.

Frame Control	Duration ID	Addr1	Addr2	Addr3	Sequence Control	Addr4	Data	Security Tag	FCS
2 byte	2 byte	6 byte	6 byte	6 byte	2 byte	6 byte	N byte	4 byte	4 byte
802.11 MAC Frame							Encryption		

Fig. 8. SCM 1 frame structure.

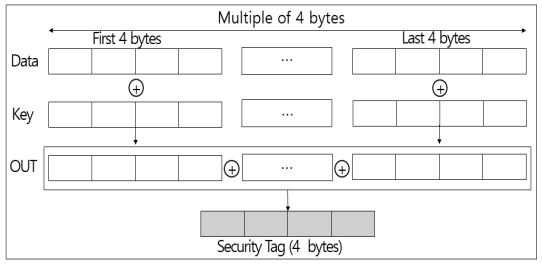


Fig. 9. Security tag generation for SCM 1.

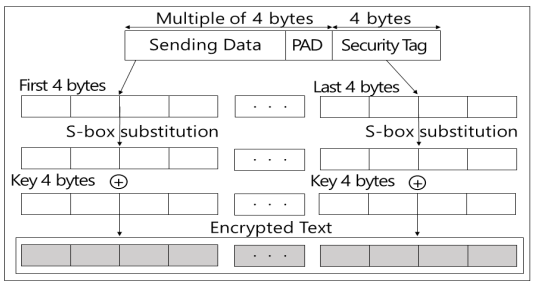


Fig. 10. Encrypted text generation for SCM 1.

호화하는 과정이다. 먼저 Fig. 9에서 생성된 보안 태그를 붙여 완성한 보안 프레임을 4 바이트로 분리한 후 각각 S-box로 치환 한 후 키와 XOR 연산하고 그 결과를 암호화된 블록으로 사용한다. 이러한 과정은 모든 분리된 블록을 대상으로 같은 연산을 수행한다.

3.2.3 SCM 2 보안 방법

IoT 장치의 LLC 계층(또는 LCS)에 입력되고 포그 단의 LCS(또는 DDC)의 LLC 계층을 통해 전달되는 응용 서비스 데이터는 폐쇄된 사설 유선 LAN 환경 기반으로 무선 환경에 비해 보안 위협에 덜 노출되므로 암호화와 복호화 과정 없이 보안 태그만 활용하는 방법을 제안한다. 이 방법이 적용되는 구간은 Fig. 5의 실선 구간으로 효율적인 전송을 통한 데이터의 무결성을 달성하기 위해 Fig. 11과 같이 간단한 연산으로 생성한 보안 태그를 활용하는 개념이다.

Fig. 11에 설명된 것과 같이 보안 태그의 생성은 송신 데이터를 4 바이트 배수로 만든 다음 4 바이트 단위 블록으로 구분하여 첫 블록부터 마지막 블록까지 XOR 연산 수행 후 그 결과를 3.2.1 소절에서 생성한 4 바이트의 키와 다시 XOR 연산하여 4 바이트의 보안 태그를 완성한다. 해당 보안 태그를 송신 데이터에 붙여 송신하고 수신측에서 결과 값을 검정함으로써 데이터 무결성을 보장한다. 이 과정에서 송신 데이터가 4 바이트의 배수가 되지 않으면 모든 값이 0인 빈 바이트로 채워서 위의 계산을 수행한다.

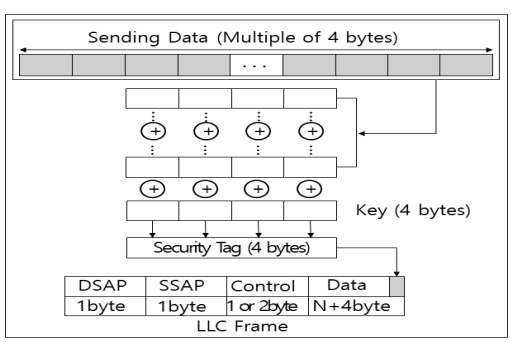


Fig. 11. Security tag generation for SCM 2.

3.2.4 SCM 3 보안 방법

SCM 3 보안 메커니즘은 인터넷을 활용하는 구간으로 클라우드 단의 CDC와 포그 단의 DDC 사이에서 간단한 HTTP 통신에 대한 데이터의 무결성을 보장하기 위한 방법이다. 클라우드 사용의 효율성과 효과적인 컴퓨팅 자원 활용 측면을 고려하여 암호화 및 복호화 과정은 없다. 즉 적용할 클라우드 환경을 여러 가지 방법들 중에서 전용의 사설 클라우드 형태로 가정하여 보안 태그 만을 활용하여 데이터의 무결성을 보장한다.

예를 들면 AES(128)는 16 바이트의 데이터 블록과 키로 S-box 치환, 행 이동 및 열 혼합, 그리고 라운드 키 추가 연산 과정을 10 라운드 반복하는 복잡한 알고리즘이다[11,12]. 본 논문에서는 전달 데이터 양과 클라우드 사용의 효율성과 효과적인 컴퓨팅 자원 활용 측면을 고려하여 AES의 연산 과정을 축소한 간략화 된 개념을 적용한다.

먼저 16 바이트 데이터 블록과 키를 8 바이트 축소하고 연산 과정도 행 이동 및 열 혼합 과정은 생략한다. Fig. 12에서 설명된 것처럼 전달 데이터의 8 바이트 단위로 구분하여 이를 S-box 치환 후 Fig. 7에서 생성한 키와 XOR 연산한다. 그리고 이 연산들을 10 라운드 대신 4라운드 반복 수행 하도록 구성한다. 이러한 과정을 남은 블록까지 수행한 후 생성된 모든 8 바이트 블록들을 XOR 연산을 통해 구해진 8 바이트를 보안 태그로 HTTP 응용 서비스 전달 데이터 뒤에 붙여 전송한다. 수신측에서 결과 값을 검정함으

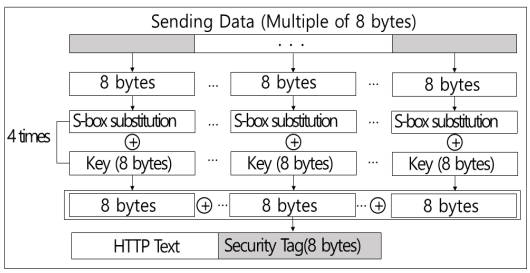


Fig. 12. Security mechanism for SCM 3.

로써 데이터 무결성을 보장한다. 이 과정에서 응용 서비스 전달 데이터가 8 바이트의 배수가 되지 않으면 모든 값이 0인 빈 바이트로 채워서 위의 계산을 수행한다.

4. 성능 평가

본 논문의 3장에서는 공장 자동화나 생산 자동화 등에 활용되는 적합한 망 프레임워크를 제시하고, 클라우드 및 포그 컴퓨팅 기반의 IoT 사물지능통신서비스를 위한 환경에서 효율적으로 동작할 수 있는 보안 메커니즘을 제시하였다. 제안된 보안 방법 SCM 1과 SCM 2 및 SCM 3는 기존에 무선 환경이나 유선 환경에서 적용되는 WPA2 또는 AES 보안 방법을 단순화하여 응용 서비스 모델에 적합하게 개선한 기술이다. 이에 대한 성능 평가는 뚜렷한 비교 대상이 없으므로 키 생성과 보안 태그 생성 및 암호화 및 복호화 과정에서 계산의 복잡성을 WPA2 또는 AES 개념을 적용한 경우와 제안된 방법을 적용한 경우를 간접적으로 비교 분석함으로써 달성한다.

4.1 키 생성방법 성능 비교

본 논문에서 제안하는 SCM 1과 SCM 2 및 SCM 3에서 생성하는 키 생성 방법은 제 3자인 보안 서버로부터 인증된 키를 받는 방법이 아니라 AES에서 라운드별 적용되는 키 생성 방법을 응용하고 간략화한 형태이다. 이는 다양한 사물들을 연결하여 언제 어디서나 상황에 맞는 지능적인 융합 응용 서비스 모델에 적합한 방법이다. Fig. 6 및 Fig. 7의 키 생성 방법의 성능 분석을 위해서는 AES 방법에서 임시키 생성 시간과 제안한 방법들의 시간 블록 구성(또는 송신자 IP주소 및 수신자 IP주소 그리고 비밀 값을 활용하여 임시키 생성)에 같은 크기의 시간이 요구된다고 가정하면, AES에 의한 키 생성 방법과 제안한 방법으로 계산에 걸리는 시간의 비교가 필요하다. AES 방법에서는 10 라운드 동안 사용할 키를 계산할 때 먼저 4의 배수에 해당하는 키 값 계산은 초기 임시키를 가지고 바이트 순환(t_0), S-box 치환(t_1), 원래 값과 XOR 연산(t_2), Rcon값과 XOR 연산(t_3)의 과정을 거친다. 한편 4의 배수 값이 아닌 라운드 키 생성은 단지 앞 라운드 값과 새롭게 계산된 라운드의 4의 배수인 키 값의 XOR 연산으로 구해진다. 여기서 비트 연산의 유사성을 감안($t_0 = t_1, t_2 = t_3, t_3 = 2t_1$로 가정)하면 키 생성 시간($T_{key(AES)}$, $T_{key(SCM1)}$, $T_{key(SCM2)}$, $T_{key(SCM3)}$)은 식 (1)과 식 (2) 및 식 (3)과 같이 정리된다.

$$T_{key(AES)} = 10((t_0 + t_1 + t_2 + t_3) + 3t_2) = 20t_1 + 50t_3 = 120t_1 \quad (1)$$

$$T_{key(SCM1)} = T_{key(SCM2)} = 4(t_1 + t_3) = 12t_1 \quad (2)$$

$$T_{key(SCM3)} = 8(t_1 + t_3) = 2T_{key(SCM1)} = 24t_1 \quad (3)$$

식(1), 식(2) 그리고 식(3)의 처리 시간으로 성능을 분석하면 Fig. 13의 그래프와 같이 제안된 방법이 훨씬 빠른 시간으로 키를 생성함을 알 수 있다.

4.2 제안된 SCM 1 보안 메커니즘 성능 분석

SCM 2와 SCM 3는 단순히 보안 태그만 생성하여 전송하므로 비교 분석할 대상이 뚜렷하지 않다. SCM 1의 무선 구간에서는 태그 생성과 암호화 과정을 거치므로 WPA2 방법과 비교함으로써 성능 분석을 달성한다.

WPA2 방법은 AES기반의 CBC-MAC 및 CTR 모드를 적용하여 메시지 무결성 코드를 생성하고 이것을 포함한 전체 전송 데이터의 암호화로 데이터의 무결성과 기밀성을 보장한다. 그러나 본 논문에서는 포그 컴퓨팅의 지역 서버에서 길이가 짧고 많은 양의 실시간 데이터에 대해 분산 처리 및 대응하므로 WPA2 방법을 적용하면 비효율적이다. 이를 해결하기 위한 간편한 방법으로 Fig. 9와 같이 보안 태그를 생성하고 이를 송신 메시지의 뒤에 부착한 후 Fig. 10의 방법으로 암호화하여 데이터의 무결성과 기밀성을 보장하는 방법을 제안하였다. 제안된 방법은 WPA2 방법을 최대한 간략하게 적용하여 보안성을

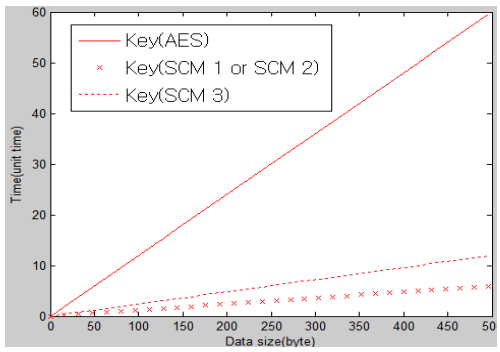


Fig. 13. Comparison of key generation time.

보장한다.

제안된 방법의 성능 비교를 위해 WPA2 방법과 제안된 보안 태그 생성 및 암호화 방법인 SCM 1을 시간 처리 신속성에 따라 Fig. 14와 같이 분석하였다. 분석 과정에서 사용되는 변수들로 송신 데이터 길이 L(PAD 부분 포함), 1 바이트 XOR 연산 소요 시간(t_1), 1 바이트 S-box 치환 소요 시간(t_2), 한 블록(16 바이트)에 대한 행 이동 소요시간(t_3), 그리고 한 블록에 대한 열 혼합 소요시간(t_4)들을 정의한다. 여기서 1 바이트 XOR 연산 시간과 1 바이트 S-box 치환 시간은 동일하다고 가정하고, 한 블록 행 이동 시간은 수행 시간은 t_2의 4배로 가정하며 t_4는 t_1의 28배($t_1=t_2, t_3=4t_1, t_4=28t_1$)로 가정한다.

식 (4)는 위에서 설명한 개념을 AES의 10라운드 수행에 소요되는 시간을 수치화한 것으로 AES의 1 라운드(S-box치환, 행 이동 및 열 혼합, 라운드키 추가) 수행에 소요 시간에 10 라운드를 곱한 후 마지막 10번째 라운드는 열 혼합수행 과정을 생략하므로 t_4 값을 차감하였다.

$$T_{AES}=10(16t_1+16t_2+t_3+t_4)-t_4=612t_1 \quad (4)$$

식 (5)는 WPA2의 CBC-MAC 방법으로 MIC를 만드는 과정에서 요구되는 처리 시간에 대한 수식이다. CBC-MAC 방법은 16바이트 단위의 연산 수행 과정으로 16바이트의 초기 블록 및 각 중간연산 결과들에 대한 T_{AES} 과정과 AES적용 결과 값과 데이터 블록과의 XOR 연산 과정을 총 $L/16+2$번을 수행한다.

결과적으로 식 (6)은 WPA2의 CTR 방법으로 암호화를 하는 과정에서 요구되는 처리 시간에 대한 수식이다. CTR 방식은 16바이트 단위의 연산 수행 과정으로 각 카운터 블록에 대한 T_{AES} 과정과 AES 적용 결과와 데이터 블록 및 MIC블록의 XOR연산 과정을 $L/16+1$번을 수행한다.

$$T_{MIC(WPA2)}=(T_{AES}+16t_1)\times(L/16+2) \quad (5)$$

$$T_{ENC(WPA2)}=(T_{AES}+16t_1)\times(L/16+1) \quad (6)$$

식 (7)은 식 (5)와 식 (6)을 통한 WPA2에 의한 전체 보안 처리 시간 T_{WPA2}를 나타낸다.

$$\begin{aligned} T_{WPA2} &= T_{MIC(WPA2)}+T_{ENC(WPA2)} \\ &= (T_{AES}+16t_1)\times(L/8+3) \end{aligned} \quad (7)$$

다음 식 (8)은 SCM 1의 Fig. 9의 보안 태그를 만드는 과정에서 요구되는 처리 시간에 대한 수식이다. SCM 1은 4 바이트 단위의 연산 수행 과정으로 4바이트의 데이터 블록과 키의 XOR연산을 총 $L/4$번 수행하고 그 결과 블록들 간의 XOR연산을 총 $L/4-1$번 수행함으로써 보안 태그를 생성한다.

그리고 식 (9)는 Fig. 10에 기술된 SCM 1의 암호화 처리 시간에 대한 수식이다. SCM 1은 식 (8)을 통해 생성된 보안 태그와 전송할 데이터 블록에 대해 4바이트의 단위로 S-box치환을 한 후 키와 XOR연산 과정을 총 $L/4+1$번 수행하여 암호화가 이루어진다.

$$\begin{aligned} T_{TAG(SCM1)} &= 4t_1\times L/4+4t_1\times(L/4-1) \\ &= 4t_1(L/2-1)=2t_1(L-2) \end{aligned} \quad (8)$$

$$T_{ENC(SCM1)}=(4t_1+4t_2)\times(L/4+1)=8t_1(L/4+1) \quad (9)$$

식 (10)은 식 (8)과 식 (9)를 통한 SCM 1에 의한 전체 보안 처리 시간 T_{SCM1}을 나타낸다.

$$T_{SCM1}=T_{TAG(SCM1)}+T_{ENC(SCM1)}=4t_1(L+1) \quad (10)$$

Fig. 14는 식 (7)과 식 (10)의 처리 시간에 대한 분석으로 WPA2 방식에 대한 그래프에서 초기 값이 0으로 시작되지 않는 이유는 식 (5)의 MIC생성 과정에서 초기블록 3개에 연산 때문이다. 결과적으로 SCM 1에 의한 방법이 보안 태그의 생성과 암호화 과정에서 훨씬 신속하게 처리되는 것을 볼 수 있다.

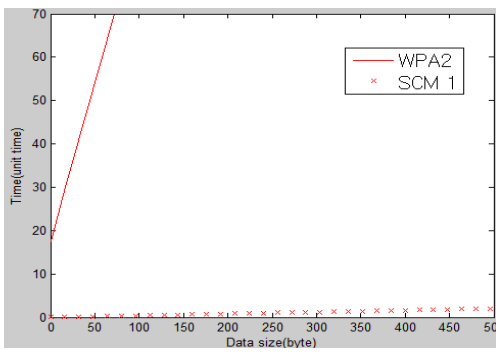


Fig. 14. Processing time comparison between WPA2 and SCM 1 applied methods.

5. 결 론

본 논문에서는 IoT를 기반으로 하는 초지능적 서비스를 성공적으로 구현하기 위해 백본망의 양 끝단에 포그 컴퓨팅기술과 클라우드 컴퓨팅 기술을 적용

하여 사물지능통신서비스를 위한 망 프레임워크를 제안하였다. 제안된 망은 포그 컴퓨팅 개념을 적용한 지역서버를 IoT장치 근처에 위치시켜 대역폭낭비 및 시간지연을 최소화 하면서 망 트래픽을 제어하며 실시간으로 데이터처리를 할 수 있도록 하고, 클라우드 컴퓨팅 기술을 통해 상호 연동되어 데이터의 장기적인 저장과 처리로 초연결성 구현을 달성한다.

구체적으로 공장 자동화나 생산 자동화 등에 활용되는 클라우드 및 포그 컴퓨팅 기반의 IoT 서비스를 위한 적합한 망 프레임워크를 제시하고 이 환경에서 효율적으로 동작할 수 있는 보안 메커니즘을 적용하는 것이 주된 목적이다. 또한 다양한 전사적 보안 위협에 대처하는 방안을 제시하는 것이 아니라, 망 측면의 전송 과정에서의 데이터 무결성(위조 및 변조에 대해)을 보장하는 보안 프레임워크를 제안하였다. 그러므로 새로운 보안 방법을 제안하는 것이 아니라 실제 적용 관점에서 확장성있고 실용적인 적용에 그 관점이 있다.

제안된 망구조에서 무선 또는 유선 환경에 따라 데이터 무결성 보장을 위한 보안 방법을 다르게 제시하였고 또한 유선 환경에서도 개방된 정도에 따라 효율적인 메커니즘을 제안하였다. 무선 환경에서는 보안 위협에 많이 노출되므로 SCM 1 방법을 통해 보안 태그 생성 및 부착과 암호화를 통한 보안성을 강화하였다. 유선 환경에서는 보안성 요구의 정도에 따라 단순히 효율적이고 신속한 보안 태그 생성 및 적용으로 접근하였고, 성능평가를 통해 제안된 보안 메커니즘들의 간단함을 검증하였다.

향후 블루투스 또는 지그비등 다양한 무선 환경과 여러 가지 형태의 포그 컴퓨팅 및 클라우드 컴퓨팅 응용들에 적용할 수 있도록 LEA(Lightweight Encryption Algorithm)[17]과 Diffie-Hellman 자동키 생성방식[18] 및 Merkle-Damgard 보안 태그 생성 방법[19]등을 활용한 확장성에 대한 연구가 필요하다.

REFERENCE

[1] S. Chae, Y. Yang, and T. Han, "The Fourth Industrial Revolution and Multimedia Converging Technology: Pervasive AR Platform Construction Using a Mobile Robot based Projection Technology," *Journal of Korea Multimedia Society*, Vol. 20, No. 2, pp. 298-312, 2017.

[2] M. Diaz, C. Martin, and B. Rubio, "State-of-the-art, Challenges, and Open Issues in the Integration of Internet of Things and Cloud Computting," *Journal of Network and Computer Applications*, Vol. 67, pp. 99-117, 2016.

[3] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud Computing: State-of-the-art and Research Challenges," *Journal of Internet Services and Applications*, Vol. 1, No. 1, pp. 7-18, 2010.

[4] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog Computing and Its Role in the Internet of Things," *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, pp. 13-16, 2012.

[5] A.V. Dastjerdi and R. Buyya, "Fog Computing: Helping the Internet of Things Realize Its Potential," *Computer*, Vol. 49, Issue 8, pp. 112-116, 2016.

[6] D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, "6TiSCH: Deterministic IP-enabled Industrial Internet(of Things)," *IEEE Communications Magazine*, Vol. 52, No. 12, pp. 36-41, 2014.

[7] E. Borgia, "The Internet of Things Vision: Key Features, Applications and Open Issues," *Computer Communications*, Vol. 54, pp. 1-31, 2014.

[8] J.S. Zielinsku, "Internet of Everything (IoE) in Smart Grid," *Przeglad Elektrotechniczny*, Vol. 91, No. 3, pp. 157-159, 2015.

[9] P.A.F. Vitti, D.R. dos Santos, C.B. Westphall, C.M. Westphall, and K.M.M. Vieir, "Current Issues in Cloud Computing Security and Management," *Secuware 2014*, pp. 36-42, 2014.

[10] S. Sarkar, V.K. Bharadwaj, and G. Priya, "Security Issues and Challenges in Cloud Computing," *International Research Journal of Engineering and Technology*, Vol. 3, No. 10, pp. 1143-1146, 2016.

[11] R. Arora and A. Parashar, "Secure User Data in Cloud Computing Using Encryption Algor-

ithms," *International Journal of Engineering Research and Applications*, Vol. 3, No. 4, pp. 1922-1926, 2013.

[12] NIST, *Advanced Encryption Standard(AES)*, Federal Information Processing Standards Publication 197(FIPS-197), 2001.

[13] IEEE, *PART 11: Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11i, 2004.

[14] IETF, *Hypertext Transfer Protocol (HTTP/1.1): Authentication*, RFC 7235, 2014.

[15] IETF, *Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions*, RFC 6929, 2013.

[16] IEEE, *IEEE Standard for Ethernet*, IEEE Std 802.3, 2012.

[17] D. Hong, J.K. Lee, D.C. Kim, D. Kwon, K.H. Ryu, and D.G. Lee, "LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors," *Proceeding of International Workshop on Information Security Applications*, pp. 3-27, 2013.

[18] IETF, *Diffie-Hellman Key Agreement Method*, RFC 2631, 1999.

[19] J.S. Coron, Y. Dodis, C. Malinaud, and P. Puniya, "Merkle-Damgård Revisited: How to Construct a Hash Function," *Proceeding of Annual International Conference on Advances in Cryptology*, pp. 430-448, 2005.

신 민 정

2017년 2월 부경대학교 정보통신공학과 (공학사)
2017년 3월~현재 부경대학교 정보통신공학과 석사과정
관심분야 : 무선네트워크 보안기술, IoT, 포그 컴퓨팅, 클라우드 컴퓨팅

김 성 운

1982년~1985년 한국전자정보통신 연구소 연구원
1985년~1995년 한국통신연구개발원 선임연구원 실장
1989년~1993년 프랑스 파리 7대학 석·박사
1995년~현재 부경대학교 정보통신공학과 교수
관심분야 : 무선네트워크 보안기술, 센서 네트워크, 전송망 및 액세스망 기술, IoT, 포그 컴퓨팅, 클라우드 컴퓨팅