Journal of Convergence for Information Technology
Vol. 10. No. 7, pp. 7-13, 2020
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2020.10.07.007

IoT기반 클라우드 융합환경에서 안전한 접근제어를 위한 인증서 관리기법 설계

박중오
성결대학교 파이데이아학부 조교수

A Design of Certificate Management Method for Secure Access Control in IoT-based Cloud Convergence Environment

Jung-Oh Park
Assistant Professor, Division of Paideia, Sungkyul University

요 약 4차 산업혁명의 핵심 IT기술인 사물인터넷은 타산업과 융합되어 사용자로부터 다양한 서비스를 제공하고 있다. IoT 융합기술은 사용자의 편의성 증대에 따른 통신환경에 대한 커뮤니케이션 패러다임을 이끌고 있다. 하지만 빠르게 발전하는 IoT 융합기술에 대한 보안 방안 마련이 시급하다. IoT는 디지털 윤리와 개인정보보호와 밀접한 관계를 가지고 있어, 타 산업에 IoT 도입에 따른 위협요소 대책안을 마련해야한다. 보안사고 발생 시 정보유출, 이미지 실추, 금적적인 손해, 인명피해 등 다양한 문제가 나타날 수 있다. 그러므로 본 논문에서는 IoT기반 클라우드 융합 환경에서 안전한 접근제어를 위한 인증서 관리기법을 제안한다. 디바이스 및 사용자 등록, 메시지 통신 프로토콜, 디바이스 갱신 및 관리 기법을 설계하였다. 공격기법 및 취약점에 따른 안전성 분석을 수행하였으며, 기존 PKI 기반 인증서 관리기법 대비 효율성 평가결과 약 32%의 감소된 수치를 확인 할 수 있었다.

주제어 : 메시지 통신 및 인증 프로토콜, 사물인터넷, 융합환경, 접근제어, 클라우드 컴퓨팅 서비스

Abstract IoT which is the core IT of the 4th industrial revolution, is providing various services from users in the conversion with other industries. The IoT convergence technology is leading the communication paradigm of communication environment in accordance with the increase of convenience for users. However, it is urgently needed to establish the security measures for the rapidly-developing IoT convergence technology. As IoT is closely related to digital ethics and personal information protection, other industries should establish the measures for coping with threatening elements in accordance with the introduction of IoT. In case when security incidents occur, there could be diverse problems such as information leakage, damage to image, monetary loss, and casualty. Thus, this paper suggests a certificate management technique for safe control over access in IoT-based Cloud convergence environment. This thesis designed the device/user registration, message communication protocol, and device renewal/management technique. On top of performing the analysis on safety in accordance with attack technique and vulnerability, in the results of conducting the evaluation of efficiency compared to the existing PKI-based certificate management technique, it showed about 32% decreased value.

Key Words : Message Communication & Authenticaion, IoT, Convergence Environment, Access Control, Cloud Computing

*Corresponding Author : Jung-Oh Park(pjo21@naver.com)

Received May 07, 2020
Revised June 8, 2020
Accepted July 20, 2020
Published July 28, 2020

1. 서론

사물인터넷은 DATA, AI, 블록체인, 클라우드 기술과 융합되어 '지능형 사물인터넷' 형태로 발전되고 있다. 인간의 개입을 최소화하여 주변상황 인지와 자율적인 대응을 수행할 수 있다. 스마트 홈, 스마트 팩토리, 스마트 카, 스마트 헬스케어 등과 융합되어 수많은 분야에서 사용하여 사용자로부터 편의성을 제공하고 있다[1,2].

하지만, 사물인터넷 기술은 기존 무선인터넷 환경에서 발생하는 취약점을 계승하여 인증, 접근통제, 무결성 부재에 따른 보안위협이 있다. 융합 환경에 따른 신규 보안위협이 발생되고 있으며, 데이터 위변조, 사생활 침해, 금적적인 피해에 따른 사고건수가 늘어나고 있다[2,9].

그러므로 본 논문에서는 IoT기반 클라우드 융합환경에서 안전한 통신을 수행하기 위한 인증서 관리 기법을 설계하도록 한다.

본 논문은 구성은 다음과 같다. 2장에서는 IoT 기반 클라우드 융합환경 기술 사례와 IoT기반 클라우드 융합환경 보안위협 및 보안 요구사항에 대해서 연구한다. 3장에서는 디바이스 및 사용자 등록 절차, 메시지 통신 프로토콜, 디바이스 갱신 관리 프로토콜에 대해서 제안한다. 4장에서는 제안된 프로토콜의 안전성 분석과 효율성 평가에 따른 성능평가를 수행한다. 5장에는 본 논문의 결론으로 향후 연구 계획을 제시한다.

2. 관련연구

2.1 IoT기반 클라우드 융합 환경 기술 사례

사물인터넷(IoT)은 ICT시장의 신산업을 이끌어가는 핵심 부가가치 산업으로 발전되고 있다. 특히 스마트폰 확산으로 인해 센서와 함께 디바이스간의 융합 및 연결성이 확보되어 사용자로부터 다양한 서비스가 제공되어 편의성이 증대되고 있다. ICT 산업의 핵심인 ICBM(Iot, Cloud, Big Data, Mobile)이 성장동력으로 연구되고 있으며 무선 인터넷 기반의 IoT서비스가 생활영역에서 점차 확대되고 있다[3].

이러한 IoT 활용에 따른 부가가치 규모는 2020년까지 19조 달러로 달할 것으로 전망하고 있으며, 활용할 수 있는 환경은 공장, 도시, 건강, 소매, 작업장, 교통, 가정에서 사물인터넷 활용 수준에 따라 최대 12조 달러의 경제적 파급효과가 발생할 것으로 전망한다[1-3].

하지만 CCTV, 스마트 홈, 스마트 헬스케어 등 IoT 분양에서 다양한 보안 위협이 발생되고 있다. 기존 무선 네트워크 환경에서 발생하는 취약점을 계승하고 있으며, 신규 및 변종 공격에 따른 피해도 발생하여 사용자에 따른 피해규모가 증가하고 있다. 이를 해결하기 위해 사용자로부터 안전하게 사용할 수 있는 IoT 제품·서비스의 보안가이드들이 제시되고 있다.

2.2 IoT기반 클라우드 융합환경 보안위협 및 보안 요구사항

IoT기반 클라우드 융합환경의 특성상 저장된 데이터에 따른 위치파악이 힘들다는 점을 볼 때 보안 취약점이 노출될 수 있다. 특히 Public 클라우드 서비스를 사용시 데이터에 저장하는 것에 따른 신뢰성과 안전성이 문제될 수 있다[3-5,8]

클라우드 서비스 등장 이전 기존 DRC(Data Recovery Center)에서 존재하던 보안위협하고 클라우드 환경에서 대표적인 취약점인 "Data Storage"에 따른 문제를 보완할 수 있는 접근제어에 따른 설계가 필요하다[4,6].

클라우드 서비스 환경에서 가용할 수 있는 서비스 자원에 대한 분류는 Public Cloud, Private Cloud, DRC가 있으며, 보안위협에 따른 범주 및 위협의 예는 아래 Table 1과 같다[7-10].

Table 1. Distinguish from cloud security threats

Category	An example of a threat
Virtualization Issues	VM Escape.Hoping.Image Modulation, Hypervisor based rootkit
Duplicated confidence boundary	Overlapping security boundaries due to Multi-Tenancy
Network intrusion	Network traffic eavesdropping, malicious intermediaries
Service attack	Service distortion, wrapping, web service language scanning
Devolution	Counterfeit alteration, identifier management, and anonymity of access authority
Overload attack	DoS, DDoS attack, rapid creation of virtual machines

위 언급된 클라우드 환경에 따른 취약점 및 보안위

협을 해결하기 위해서는 기술적, 보안정책, 관리적, 법제도에 따른 연구가 필요하다. 기술적에서는 기존 보안 위협과 가상화 환경에서 발생하는 취약점에 따른 보안이 필요하다.
그리고 관리측면 및 법제도를 보안하여 사용자가 안전하게 사용할 수 있는 방안이 필요하다.

IoT 디바이스 통신 환경에서 암호화를 수행해야 한다. 안전성을 보장하는 보안 통신 프로토콜인 HTTPS(SSL/TLS 등) 기반 암호화 프로토콜을 사용해야한다. 그리고 보안 위협을 방지하기 위한 사용자 인증, ID, Password 외 IP나 MAC 주소를 필터링 할수 있는 접근제어 설정이 필요하다. 마지막으로 디바이스 펌웨어 인증 및 보안설정을 수행하여 안전하게 사용할 수 있는 보안정책 강화가 요구된다. 클라우드 보안 문제와 해결책은 아래 Table 2로 제시하였다[8-10].

Table 2. Cloud Security Issues and Solutions

Threats	Solution plan
Succession of existing security threats	- Strengthen encryption, hashing, digital signatures, duplicate monitoring, etc. - Multi-level authentication and connection management
Threats through Gishing	- Protection of transmitted data through encryption - Encryption and key management for stored data
Management side problem	- Education and Validated Recruitment of Insiders - Achieve certification that complies with international cloud security standards
Legal system problem	- Pre-check legal issues and introduce system design - International standard

3. IoT기반 클라우드 융합환경에서 안전한 접근제어를 위한 인증서 관리 기법 설계

본 장에서는 IoT기반 클라우드 융합환경에서 사용자가 클라우드 서버에 접근시 안전하게 통신을 수행이 가능한 인증서 관리기법을 제안한다. 디바이스 등록, 메시지통신 기법 설계, 디바이스 인증값 관리 프로토콜에 대해서 제안한다. 논문 프로토콜에 대한 약어는 Table 3과 같다.

Table 3. Abbreviation for the proposed protocol

Abbreviation	Description
MS:OSS	Management Service : Operational Support Server
CSS	Cloud Computing Server
Application	Application of User
IOT_{IV}	Initialization vector of IoT
IOT_{Nonce}	Random Number of IoT
H()	Hash Function
$Gateway_{SN}$	Serial Number of Gateway
$Signature_{Value-i}$	Certification Value
$USER_{IMEI}$	Intel Management Engine Interface of User
$DATA_{IoT-Gathering}$	Gathering of Data
$USER_{PI}$	Personal Information of User
$Gateway_{Info}$	Information of Gateway

3.1 디바이스 등록 및 인증서 생성 절차

본 절에서는 디바이스 등록 및 인증서 생성 절차에 따른 프로토콜을 제안하며, Fig 1과 같다.

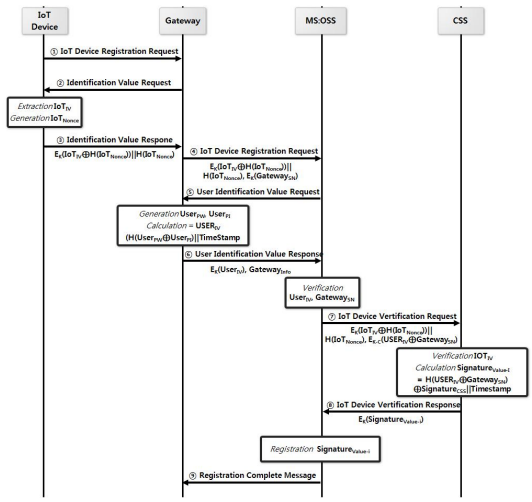

Fig. 1. Procedure for registering devices and generating certificates

1. 사용자는 IoT 디바이스를 활용하여 게이트웨이로부터 등록 요청을 수행한다,

2. 게이트웨이는 수신된 메시지를 확인 후 IoT 디바이스로부터 인증값을 요청한다.

3. IoT 디바이스에서는 IoT_{IV}, IoT_{Nonce}를 추출 후 암호화를 수행하여 게이트웨이로부터 인증값 요청 메시지를 전송한다.

$E_K(IoT_{IV} \oplus H(IoT_{Nonce}) \| H(IoT_{Nonce})$

4. 게이트웨이는 MS:OSS로부터 수신된 메시지와 게이트웨이의 식별값이 포함된 데이터를 암호화를 수행하여 IoT 디바이스 등록 요청메시지를 전송한다.

$E_k(IoT_{IV} \oplus H(IoT_{Nonce}) \| H(IoT_{Nonce}),$
$E_k(Gateway_{SN})$

5. MS:OSS는 게이트로부터 사용자 신원 확인값을 요청한다. 메시지를 수신한 게이트웨이는 사용자로부터 사용자의 패스워드, 정보 입력받은 후 사용자의 신원값을 생성한다.

$User_{IV} =$
$(H(User_{PW} \oplus User_{ID}) \| TIMESTAMP$

6. 사용자는 MS:OSS로부터 신원값을 송부하고 MS:OSS는 수신한 데이터를 검증한다.

$E_k(User), Gateway_{Info}$

7. MS:OSS는 CSS로부터 디바이스의 해쉬함수 수행한 IoT_{Nonce}, 게이트웨이 식별값, 사용자 식별값을 연산한 IoT 장비 검증 요청 메시지를 전송한다.

$E_k(IoT \oplus H(IoT_{Nonce}) \| H(IoT_{Nonce}),$
$E_{K-C}(User_{IV \oplus} Gateway_{SN})$

8. CSS는 MS:OSS 수신된 메시지를 검증 후 서명값을 생성하여 검증값에 대한 응답메시지 $Signature_{Value-i}$를 전송한다.

$Signature_{Value-i}$
$= H(User_{IV} \oplus Gateway_{SN}) \oplus$
$Signature_{CSS} \| Time\ Stamp$

9. MS:OSS는 검증값에 대한 메시지를 저장 후 게이트웨이로부터 등록 완료메시지를 전송한다.

3.2 메시지 통신 프로토콜 절차

본 절에서는 사용자가 클라우드 서버에 접속 후 등록된 디바이스에 따른 데이터 요청하는 메시지 통신 프로토콜에 대한 절차를 제안하며, Fig 2와 같다.

1. 사용자는 스마트폰 어플리케이션을 사용하여 사용자 패스워드, IMEI 값을 포함한 현재상황 데이터를 CSS에게 전송한다.

$Gateway_{Info}, User_{PI},$
$E_k(User_{PW}, User_{IMEI})$

2. CSS는 MS:OSS로부터 사용자 신원값에 대한 요청메시지를 전송한다.

$User_{PI}, E_k(User_{PW}, User_{IMEI})$

3. MS:OSS는 수신한 메시지를 복호화 후 검증한다. 이후 CSS로부터 사용자 응답메시지를 전송한다.

4. CSS는 Gateway로부터 디바이스로부터 수집된 메시지를 전송한다.

$User_{PI}, Gateway_{info}$

5. 게이트웨이는 IoT 디바이스로부터 수집된 데이터를 요청하는 메시지를 전송한다.

$E_k(IoT \oplus H(IoT_{Nonce}))$

6. IoT 디바이스는 수신된 데이터를 복호화 후 검증한다. 이후 세션키로 암호화하여 수집된 데이터를 전송한다.

$E_{SK}(Data_{IoT-Gathering})$

7. 게이트웨이는 CSS로부터 수집된 데이터를 전송 후 CSS는 수신된 데이터에 따른 세션키를 추출하여 $Gateway_{Info}$, $User_{PI}$를 분석한다.

$E_{SK}(Data_{IoT-Gathering})$

8. CSS는 사용자로부터 현재상황에 따른 요청된 데이터를 전송한다.

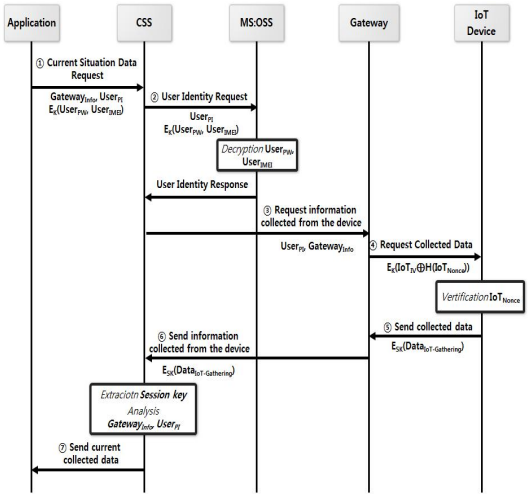

Fig. 2 Message Communication Protocol Procedures

3.3 디바이스 인증값 관리 프로토콜

본 절에서는 디바이스 및 사용자에 따른 접근제어를 강화하기 위한 인증값 관리 프로토콜을 설계하며. Fig 3과 같다.

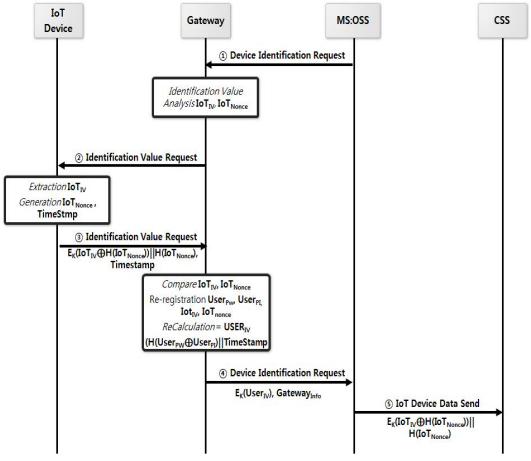

Fig. 3 Device Authentication Value Management Protocol

1. MS:OSS는 게이트웨이로부터 식별값 인증 메시지를 전송한다.

2. 게이트웨이는 IoT_{IV}, IoT_{Nonce}를 분석 후 IoT 디바이스로부터 식별값 요청메시지를 전송한다.

3. IoT 디바이스는 IoT_{IV}를 추출 후 IoT_{Nonce}, TIMESTAMP를 생성한다.

4. IoT 디바이스는 생성된 데이터를 암호화 후 게이트웨이로 전송한다.

$$E_k(IoT_{IV} \oplus H(IoT_{Nonce}) \| H(IoT_{Nonce}) \; Time\ stamp$$

5. 게이트웨이는 수신된 데이터에 따른 식별값을 검증 후 $User_{PW}$, $USER_{PI}$, IoT_{IV}, IoT_{Nonce}에 따른 값을 재계산 후 $User_{IV}$를 생성한다. 이후 MS:OSS로부터 식별값을 전송한다.

$$E_k(User_{IV}), Gateway_{Info}$$

6. MS:OSS는 CSS로부터 검증된 식별값을 전송하여 인증값관리를 요청한다.

4. 성능평가

4.1 안정성 분석

중간자 공격 : IoT기반 클라우드 융합환경에서 취약한 디바이스, 게이트웨이 접근하여 데이터 정보 누출에 따른 중간자 공격이 발생한다. 이를 보안하기 위해 디바이스 등록과정에 따른 IOT_{IV}, $Signature_{Value-i}$ 을 생성 후 관리한다. 메시지 통신과정에 서명값 $Signature_{Value-i}$와 $User_{PI}$, 검증 후 수집된 데이터를 E_{SK}로 암호화 하여 데이터를 전송함으로써 중간자 공격에 대해 안전하다.

재전송 공격 : 기존 유·무선 통신과정에서 발생하는 재전송 공격에 대한 위협요소를 막기 위해서 MS:OSS에서 서명값 $Signature_{Value-i}$ 와 암호화 수행된 사용자 $USER_{PW}$, $USER_{IMEI}$ 를 확인함으로써, 재전송 공격시 실패하게 된다.

인증서 갱신 관리 측면 : 사용자, 디바이스 접근제어와 인증서 관리를 보안하기 위해서 관리 프로토콜을 설계하였다. 게이트웨이를 통한 주기적인 디바이스 식별값 관리를 수행 시 사용자의 $USER_{PW}$, $USER_{PI}$, IoT_{IV}, IoT_{Nonce}에 따른 계산을 수행하여 인증서를 재계산한다. 또한 MS:OSS에서 수집된 데이터를 관리하는 게이

트웨이의 $Gateway_{Info}$를 확인함으로써 인증서 변조를 예방할 수 있다.

데이터 변조에 따른 방안 : 공격자가 특정 디바이스를 탈취 후 식별값에 대한 정보를 변경 후 데이터 변조에 따른 취약점이 발생한다. 제안한 접근제어 관리기법은 CSS. MS:OSS. Gateway에서 $User_{IV}$, IoT_{IV}, IoT_{Nonce}에 따른 인증을 수행함으로써 인가된 사용자만 접근이 가능하다.

4.2 효율성 평가

본 절에서는 제안한 프로토콜에 따른 효율성 평가를 수행한다. 하드웨어 Intel(R) Core i7-4970(3.6GHz), 8.00 GB 메모리와 Windows 10 Pro 64Bit PC환경에서 Eclipse Java 어플리케이션을 활용하여 성능평가를 수행하였다.

기존의 PKI기반 인증서 관리기법과 제안한 프로토콜과의 효율성을 비교분석하였다. 우선 인증서 등록 및 통신절차에서 기존 PKI는 등록대행 기관, 인증기관을 통해 인증서를 발급 후 다른 개체로부터 검증을 수행시 검증기관, 인증기관을 거쳐서 총 4번의 암복호화 인증과정과 전자서명에 따른 1번의 암복호화 과정을 수행한다. 제안한 프로토콜에서는 등록 및 통신과정에서 3번의 암복호화 및 2해쉬함수 검증을 수행함으로써 절차가 간소화된다. 기존 PKI 기반 인증서 관리 시스템과 제안한 인증서 관리 프로토콜은 비교분석 차트는 Fig 4와 같다.

Table 4. Comparison of Proposed Protocol and Existing System

	Generate Certification of PKI Based	Proposed Signature Issuing and Validation Techniques
Signature Verification	0.324633	0.17887
1 Times	1.623165	1.152769
10 Times	15.12383	11.21212
50 Times	78.98151	54.98129
100 Times	151.9841	101.9847

(unit : nanosecond)

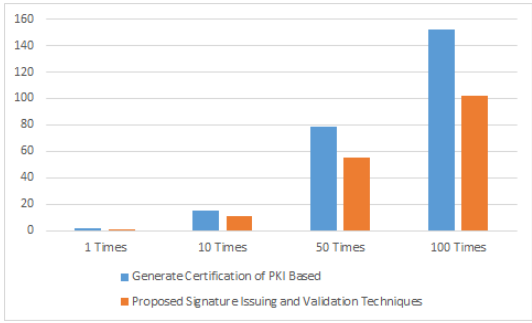

Fig. 4 Comparing and analyzing the effectiveness of generating and managing certificates according to the amount of issuance

PKI기반 서명값 검증은 RSA 2048 알고리즘 제안프로토콜의 서명값 검증 알고리즘은 SHA384를 수행하였다. 제안하는 인증서 관리 프로토콜은 다수의 개체를 검증(100회) 시 약 32% 감소되었다. 그러므로 다수의 중소형 IoT 디바이스에 대한 인증 및 서명값 검증을 수행할 때 제안한 프로토콜을 활용하면 기존 기법 대비 높은 효율성을 확인할 수 있다.

5. 결론

본 논문에서는 IoT기반 클라우드 융합환경에서 사용자 및 디바이스에 대한 안전한 통신을 수행하기 위해서 인증서 관리 기법에 대한 프로토콜을 설계하였다. 디바이스 및 사용자 등록절차, 메시지 통신 절차, 디바이스 갱신 절차에 따른 프로토콜을 설계함으로써 접근권한에 따른 메시지를 송신할 수 있도록 제안하였다.

IoT기반 클라우드 융합환경에서 발생하는 중간자 공격, 재전송 공격기법과 인증서 관리 측면, 데이터 변조에 따른 방안에 대해서 안전성을 분석하였다. 효율성 평가부분에서는 기존 PKI기반 인증서 관리 기법과 제안 프로토콜을 분석하여 약 32%의 감소된 수치를 확인 할 수 있었다.

본 논문에서 제안한 기법은 IoT기술이 융합된 사례뿐 만아니라, 클라우드 고도화 환경(Fog)기반에서도 접목하기 위한 경량화 프로토콜 연구가 필요하다. 또한 신규 및 변종 공격에 따른 대응기법 분석과 차단할 수 있는 연구가 요구된다.

REFERENCES

[1] H. W. Kim. (2014). Security/Privacy Issues in the

Internet of Things Environment. *TTA Journal, 153*.

[2] H. J, Lee, (2012). *Security Consieration for use of Secure Cloud Services*.

[3] Y. S. Lee. (2015). *N. Security Requirements for Drone-based IoT Services*, TTA.

[4] J. I. Lee. (2015). Convergent Case Study of Research and Education: Internet of Things Based Wireless Device Forming Research. *Journal of the Korea Convergence Society, 6(4),* 1-7.
DOI : 10.15207/JKCS.2015.6.4.001

[5] K. H. Lee. (2013). A Security Threats in Wireless Charger Systems in M2M. *Journal of the Korea Convergence Society, 4(1),* 27-31.
DOI : 10.15207/JKCS.2013.4.1.027

[6] S, J. Oh. (2015). A Study on Organizations Adopting Convergence-based Smart Work for Overcoming Constraints and Achieving Performance. *Journal of Digital Convergence, 13(6),* 113-124.
DOI : 10.14400/JDC.2015.13.6.113

[7] Y. J, Park. (2015). Development of a ICT Convergence Business Model based on Smart Phone. *Journal of Digital Convergence, 13(6),* 81-89.
DOI : 10.14400/JDC.2015.13.6.81

[8] Y. S. Jung. (2019). An IoT Information Security Model for Securing Bigdata Information for IoT Users. *Journal of Convergence for Information Technology, 9(11),* 8-14.
DOI : 10.22156/CS4SMB.2019.9.11.008

[9] D. J. Choi. (2019. 9. 18). Next Generation IoT Security in the 5G Era. *ITFIND, pp1-15.*

[10] I. K. Park & J. Kwak. (2018). Permission Management System for Secure IoT Devices in Android-Based IoT Environment. *KIPS Transactions on Computer and Communication Systems, 7(2),* 59-66.
DOI : 10.3745/KTCCS.2018.7.2.59

박 중 오(Jung-Oh Park) [정회원]

· 2000년 7월 : 성결대학교 컴퓨터공학과 졸업
· 2003년 3월 : 명지대학교 전자계산교육 석사
· 2011년 8월 : 숭실대학교 컴퓨터공학 박사
· 2016년 3월 ~ 현재 : 성결대학교 조교수
· 관심분야 : PKI, Network security, 암호학
· E-mail : pjo21@naver.com