Journal of Convergence for Information Technology
Vol. 10. No. 4, pp. 18-24, 2020
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2020.10.04.018

소사이어티 5.0 기반 IoT 사용자에 대한 다중 접근방식의 프라이버시 접근 모델

정윤수[1], 연용호[2*]
[1]목원대학교 정보통신융합공학부 교수, [2]목원대학교 소프트웨어 교양학부 교수

A Privacy Approach Model for Multi-Access to IoT Users based on Society 5.0

Yoon-Su Jeong[1], Yong-Ho Yon[2*]
[1]Professor, Department of information Communication Convergence Engineering, Mokwon University
[2]Professor, Department of Software Liberal Art, Mokwon University

요 약 최근 일본을 중심으로 소사이어티 5.0에 대한 연구가 활발히 진행되고 있다. 소사이어티 5.0은 IoT 센서를 이용한 다양한 분야에서 사용되고 있다. 본 논문은 소사이어티 5.0 기반의 IoT 사용자에 대한 다중 접근방식의 프라이버시 접근 모델을 제안하고 있다. 제안 모델은 가상 환경에 IoT 장치의 중요 정보를 서로 동기화하는 다중화 방식을 사용하였다. 제안 모델은 IoT 정보의 가중치를 확률 기반으로 누적 처리함으로써 IoT 정보의 효율성을 향상시켰다. 또한, IoT 정보에 속성 정보를 연계 처리되도록 세분화하여 IoT 정보의 정확도를 향상시킨다. 성능평가 결과, IoT 장치 수와 IoT 허브장치 수에 따라 IoT 장치의 효율성이 평균 5.6% 향상되었다. 정확도는 정보 수집 및 처리에 따라 평균 15.9% 향상되었다.

주제어 : 소사이어티 5.0, 사물인터넷, 프라이버시, 다중 접근, 빅데이터

Abstract Recently, research on Society 5.0 has been actively carried out in Japan. The Society 5.0 is used in various areas using IoT sensors. This paper proposes a privacy approach model of multiple approaches to IoT users based on Society 5.0. The proposed model used multiple methods of synchronizing important information of IoT devices with one another in the virtual environment. The proposed model improved the efficiency of IoT information by accumulating the weight of IoT information on a probability-based basis. Further, it improves the accuracy of IoT information by segmenting it so that attribute information is linked to IoT information. As a result of the performance evaluation, the efficiency of IoT devices has improved by an average of 5.6 percent, depending on the number of IoT devices and the number of IoT hub devices. Accuracy has improved by an average of 15.9% depending on information collection and processing.

Key Words : Society 5.0, IoT, Privacy, Multi Access, Big data

1. 서론

정보통신기술이 발전하면서 사회와 산업 환경은 많은 변화가 이루어지고 있다[1]. 특히, IoT(Internet of Things) 센서를 통해 수집된 대용량의 정보를 AI(Artificial Intelligence)가 처리·분석하는 기술 연구는 독일의 인더스트리 4.0 (Industry 4.0)과 일본의 소사이어티 5.0(Society 5.0)가 있다. AI 기술은 빅 데이

*Corresponding Author : Yong-Ho Yon(yhyon@mokwon.ac.kr)
Received February 27, 2020
Revised March 25, 2020
Accepted April 20, 2020
Published April 28, 2020

터를 분석하여 다양한 형태로 물리적 공간으로 공급하여 산업과 사회에 새로운 가치를 재창출하고 있다. 특히, AI 기술은 다양한 사회분야(홈 서비스, 의료 서비스, 공장 자동화 등)에 융합되어가고 있다[2]. 그러나, 현재까지 운영 중인 AI 기반의 다양한 기술들은 다양한 분야에서 사용되고 있지만 보안 문제를 완벽하게 해결하지는 못하고 있다[3]. 특히, IoT 센서를 이용한 초소형 무선 장치들은 기존 통신 장비에 비해 통신 보안 요구사항이 추가로 요구되고 있다. 현재 컴퓨팅 시스템에 저장되어 처리되는 데이터는 암호화 한 후 저장되지만 이에 대한 보안 정책 및 대응 기술들이 필요하다.

본 논문에서는 빅데이터와 융합하여 서비스되고 있는 IoT 사용자의 정보를 안전하게 처리할 수 있는 소사이어티 5.0 기반의 IoT 사용자에 대한 다중 접근방식의 프라이버시 접근 모델을 제안한다. 제안 모델은 IoT 장치에 손쉽게 접근하지 못하도록 IoT 장치를 가상 환경에 여러 그룹으로 분류한 후 IoT 허브 역할을 수행하는 장치의 정보를 사용자의 중요 정보와 동기화하는 다중 접근 방식을 사용하고 있다.

제안 모델은 다음과 같은 목적을 가진다. 첫째, 수집된 정보의 가중치는 확률 기반으로 누적 처리함으로써 IoT 정보의 효율성을 향상시킨다. 둘째, 가상 환경에 다중 그룹으로 분류된 IoT 정보는 계층적으로 관리함으로써 IoT 정보의 안전성을 보장받는다. 셋째, IoT 정보의 속성 정보는 사용자의 중요 정보와 연계 처리함으로써 IoT 정보의 정확도를 향상시킨다.

이 논문의 구성은 다음과 같다. 2장에서는 인더스트리 4.0과 소사이어티 5.0를 비교한다. 3장에서는 소사이어티 5.0 환경의 IoT 사용자의 IoT 정보 보안 모델을 제안하고, 4장에서는 제안 모델의 보안 평가와 성능평가를 수행하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 인더스트리 4.0 vs. 소사이어티 5.0

인더스트리 4.0(Industry 4.0)은 독일에서 제창한 개념으로서, 기계들이 서로 모니터링하고 생산과 유지 보수에 대한 분권화된 의사결정을 내릴 수 있는 스마트 팩토리를 구축하고자 하였다. 반면, 소사이어티 5.0(Society 5.0)은 2017년 6월 일본이 제창한 개념으로서, 4차 산업 기술을 사회 전반(고령화, 구인난, 자연재해 등)에 활용하여 사회 문제를 해결하고자 한 성장 로드맵을 의미한다.

4차 산업 기술 중 하나인 독일의 인더스트리 4.0과 일본의 소사이어티 5.0 의 차이는 Fig. 1과 같다. 독일의 인더스트리 4.0과 소사이어티 5.0의 가장 큰 차이점은 Fig. 1처럼 4차 산업혁명에서 다루는 IoT, 빅데이터, 인공지능, 로봇 등을 가상공간과 현실공간에서 융합되도록 한 후 다양한 사회문제를 해결할 수 있도록 효율성과 형평성을 개선하는데 있다.

소사이어티 5.0은 일본을 중심으로 빅데이터와 AI를 이용하여 경제발전과 사회적 문제를 동시에 해결하기 위해서 이미 산업을 변화시키고 있는 사물인터넷, 사이버 보안, 인공지능, 로봇 기술들이 사회를 변화시키고 있다.

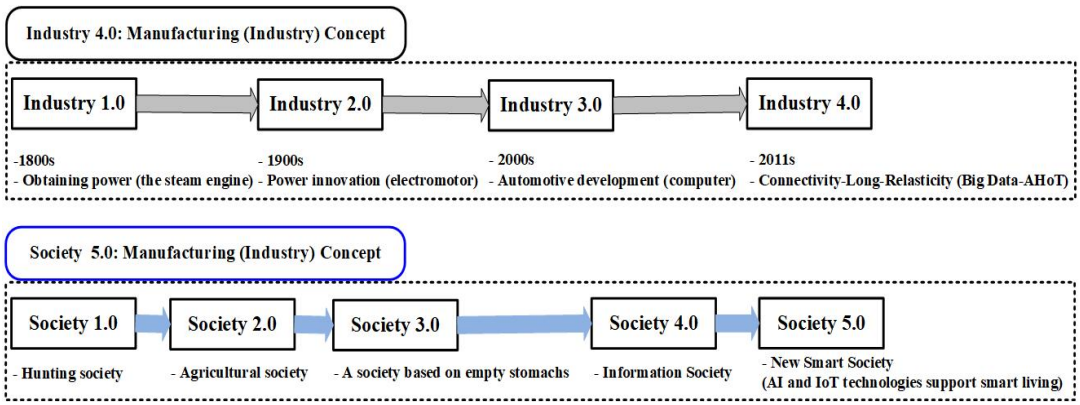

Fig. 1. Compared to Industry 4.0 vs. Society 5.0

2.2 기존 연구

소사이어티 5.0 기반 융합기술은 인공지능, 빅데이터, 클라우드 관련 기술들과 응용들을 융합한 고성능컴퓨팅(High-Performance Computing) 기술들이 다양한 분야에서 사용되고 있다[4]. Wu et al. 기술은 스마트 시티에 지능형 항구를 운영할 경우 지능형 항구에서 사용하는 포트 개념과 기본적인 기능 모듈을 소개하고 있다[5]. Belfkih et al. 모델은 지능형 항구에서 자동 인식 시스템을 이용하여 IoT를 효과적으로 처리할 수 있는 스마트 포트의 개념을 소개하고 있다[6]. Valsamis는 선박 항행 및 궤도 예측과 관련한 자동 인식 개념에 대한 연구를 수행하였다[7].

클라우드 시스템과 관련된 융합기술 연구는 IoT와 관련된 접근제어 및 동기화 연구를 중심으로 연구되고 있다. Celesti et al. 은 IoT 클라우드 서비스의 기능을 향상시킬 수 있도록 하이퍼 바이저 기반의 경량화된 접근 방식을 제안하였다[8]. Dar et al. 은 클라우드 환경에 최적화된 플랫폼을 이용한 가용성과 확률 정보를 얻기 위한 가상화 프레임워크를 제안하였다[9].

3. 소사이어티 5.0 기반 다중 접근 방식의 IoT 정보 접근 모델

3.1 개요

AI 기술은 다양한 장치로부터 데이터를 정확하면서도 빠르게 수집·분석하기 때문에 대부분의 IoT 장치에서 활용되고 있지만, 대부분의 IoT 장치들은 수집된 정보를 특별한 정책 없이 가공·분석하는 문제점이 있다[10-14]. Fig. 2처럼 제안 모델은 계층적 형태의 IoT 그룹을 H_G: $\{0,1\} \rightarrow Z_N$으로 표현한 후 IoT 정보를 H_{Info}: $\{0,1\}^* \times Z_N \rightarrow Z_{Info}$ 처럼 나타낸다. 제안 모델은 Fig. 2처럼 계층을 가상의 환경으로 IoT 장치들을 서로 인접하지 않도록 행렬 형태로 나타내도록 계층적 구조를 해쉬 체인으로 묶는다.

제안 모델은 IoT 장치의 중요 정보를 안전하게 관리하기 위해서 서로 다른 IoT 장치 간 송·수신되는 중요정보는 Fig. 1처럼 계층적 구조로 구성한 후 2가지 형태로 비교 검증하는 것이 특징이다. 첫째, 계층적 구조를 가지는 IoT 장치의 중요정보는 쌍대 비교를 통해 검증을 수행한다. 또한, IoT 장치의 중요 정보는 확률 기반의 중요도를 IoT 장치 수만큼 반복적으로 누적하여 IoT 장치의 중요정보에 대한 유사도를 검증한다. Fig. 3은 소사이어티 5.0 환경에서 IoT에 다중 접근하는 제안 모델의 과정을 다이어그램으로 나타내고 있다.

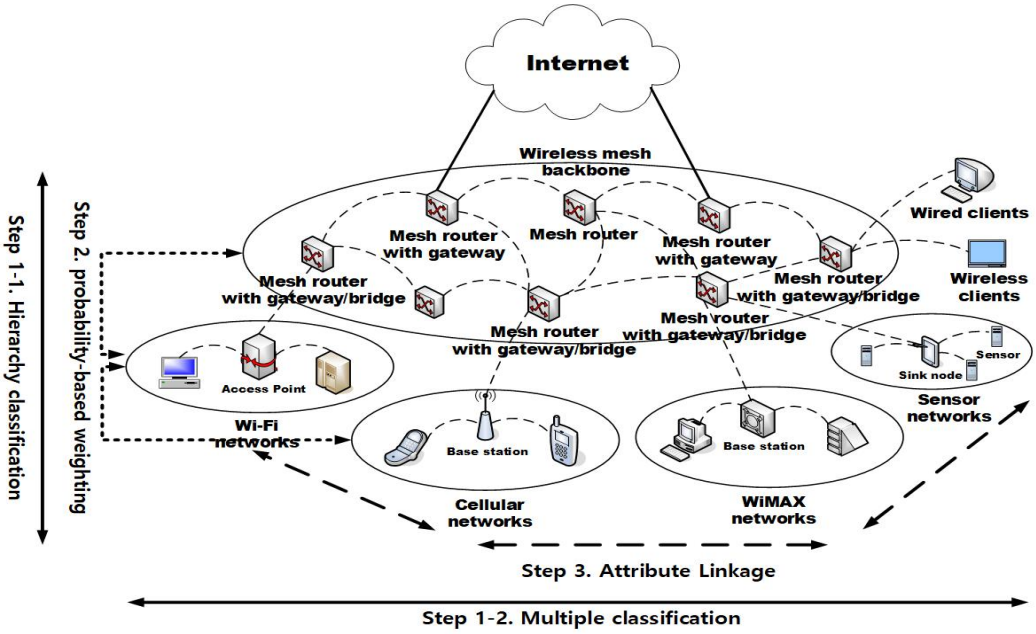

Fig. 2. Hierachical Proposed Model usign IoT

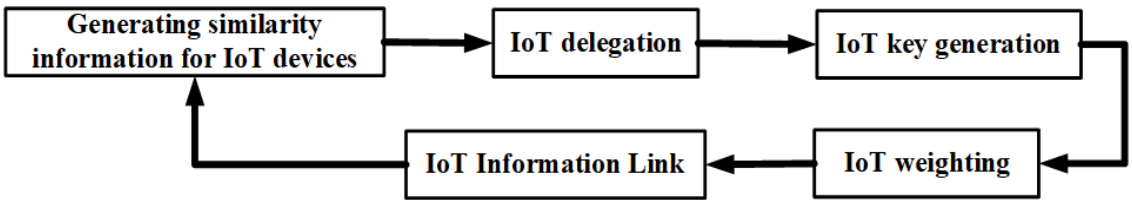

Fig. 3. Process of IoT Access based on multigroup

3.2 IoT 장치의 유사도 정보생성

IoT 장치의 유사도를 검증하기 위한 정보는 Table 1과 같다. 제안 모델에서는 IoT 장치의 조건과 동작에 따라 유사 정보가 부여되기 때문에 유사도 검증이 효율적이다. 제안 모델은 IoT 장치의 상태와 동작에 따라 빅데이터를 처리하는 IoT 장치의 불법 접근을 판별한다.

Table 1. Information on similarity of IoT devices

Information	
Status	Data sharer
	Purpose
	Obligation
	Mandate
	Location
	Time
	Sensor
	Status
Action	

제안 모델은 IoT 장치의 중요 정보를 안전하게 전달할 때, 계층적 구조로 구성된 IoT 장치의 무결성을 효율적으로 검증하기 위해서 N-1차의 다항식을 쌍대 비교에 적용한다. 이것은 IoT 장치의 중요정보를 중첩하여 분산 처리함으로써 IoT 장치의 중요정보를 안전하게 복원하기 위해서이다.

3.3 IoT 위임 및 키 생성

이 절에서는 송신지 IoT 장치의 중요정보에 대한 권한을 대리로 위임받아 수신지 IoT 장치에 전달하기 위한 방법을 기술한다. 제안 모델은 위임장 m_i를 식 (1)을 통해 인증서를 생성한다.

$$Sig = (01)^{d_2} \cdot e^{d_1} \cdot H(m_i, T) \mod N \quad (1)$$

IoT 장치의 서명은 식 (2) 와 (3)의 개인키와 공개키를 이용하여 암·복호한 후 IoT 장치의 중요정보를 전달한다.

$$x_i^{n[i]} = \begin{cases} x_i^0, \text{if } n[i]=0 \\ x_i^1, \text{if } n[i]=1 \end{cases} \quad (2)$$

$$PK_{i+1}^{n} = h(x_{i+1}^{n[i]}) = \begin{cases} PK_{i+1}^{n[i]} = h(x_{i+1}^{n[i]}), \text{if } n[i]=0 \\ PK_{i+1}^{n[i]} = h(x_{i+1}^{n[i]}), \text{if } n[i]=1 \end{cases} \quad (3)$$

제안 모델은 IoT 장치의 중요 정보에 대한 무결성을 검증하도록 식 (2)를 이진 값으로 비밀 값을 나타내도록 함으로써 IoT 장치의 중요정보를 제3자로부터 안전하게 보호하여 무결성을 보장받는다.

3.4 IoT 중요 정보 처리 과정

제안 모델은 소사이어티 5.0 환경에서 이기종의 IoT 정보를 다음과 같은 3가지 과정을 통해 안전하게 처리한다.

첫째, 제안 모델은 가상 환경을 통해 다중 그룹으로 분류된 IoT 정보를 계층적으로 관리한다.

둘째, IoT 장치의 정보는 가중치를 부여하여 확률적으로 가중치 정보를 누적 처리한다.

셋째, 제안 모델은 개별 IoT 장치에 부여된 속성 정보를 연계 처리하도록 IoT 장치를 세분화한다.

제안 모델은 가상 환경에 존재하는 IoT 허브 장치를 통해 IoT 허브 장치와 서버 간 송·수신되는 IoT 정보를 분석한 뒤 그 결과를 주기적으로 피드백하여 IoT 정보 수집에 반영한다. 제안 모델은 다중으로 IoT 정보를 복제하여 IoT 장치와 IoT 허브 장치, IoT 허브 장치와 서

버간 IoT 장치 정보를 가상 환경에서 동시에 수행하기 때문에 IoT 장치의 인증서를 이용하여 복제키를 백그라운드에서 실행한다.

4. 평가

4.1 환경 설정

제안 모델은 Fig. 4과 같은 장비를 이용하여 IoT 정보를 송・수신하도록 하였다. Fig. 4에서 IoT 장치로부터 수집된 데이터는 서버가 실시간으로 분석하여 분석된 결과를 모니터링하는 구조로 실험하였다. 성능평가의 비교분석은 [15]를 기반으로 Table 2처럼 평가를 수행하였다.

Table 2. Environment Setup

Parameter	Value
The transmit/receive power of the users	0.2W / 0.1W
The network coverage radius	1000m
The static circuit power	0.05W
The pathloss exponent	4
The available bandwidth for β_x/β_y	20MHz / 10MHz
The power of noise	-174dBm/Hz
Input data size	5kbits/s
Delay threshold	15s
Computation worload/intensity	18000 CPU cycles/bit
Computation energy efficiency coefficient of the processor's chip in the APs/users	10^{-26}
Computational capability of the Aps	10-100 GHz CPU cycles/s
Computational capability of the users	1-10 GHz CPU cycles/s
The unit price of energy	0.1 Token/J

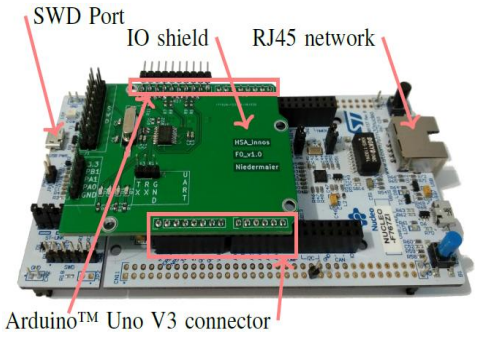

Fig 4. IoT Device used for Performance Evaluation

4.3 성능 평가

4.3.1 효율성

소사이어티 5.0을 기반으로 한 IoT 장치의 효율성은 IoT 네트워크에서 IoT 정보를 송・신하기 위한 서버의 효율성에 대한 성능평가를 수행하였다. Table 3의 효율성 평가 결과처럼 제안 모델은 IoT 장치 수와 IoT 허브 장치 수에 따라 IoT 장치의 효율성이 기존 모델보다 평균 5.6% 향상되었다. 이 같은 결과는 소사이어티 5.0이 IoT 네트워크 환경에 적합하도록 네트워크가 구축되었으며, IoT 장치의 접근 권한에 따른 처리 방법이 효과적이기 때문에 나타난 결과이다.

Table 3. Efficient using IoT devices

units : ms

Number of IoT Device	Previous Model	Proposed Model
10	70.216	76.542
25	70.685	75.859
50	70.985	76.128
75	71.458	75.898
100	71.125	77.102
125	72.859	74.639
150	71.912	76.201
200	72.107	75.878

4.2.2 정확도

Fig. 5는 서버가 실시간으로 IoT 정보를 수집 및 처리할 경우에 발생하는 서버의 데이터 분석 정확도를 평가하였다. 평가 결과, 제안 모델은 정보 수집 및 처리에 따른 정확도가 평균 15.9% 향상되었다. 제안 모델이 IoT 네트워크에 최적화된 네트워크 구조에 적합한 IoT 장치의 인증서와 암・복호키를 사용하였기 때문이다.

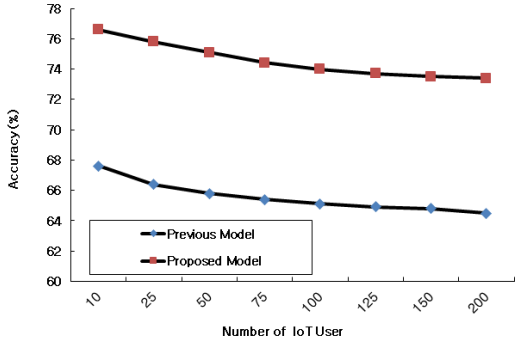

Fig 5. Accuracy using IoT devices

4.2.3 보안 분석

제안 모델은 소사이어티 5.0 환경을 기반으로 IoT 장치에서 수집된 정보를 안전하게 송・수신하기 위한 무결성 검증을 암・복호키 생성과 유사정보처리을 통해서 해결하고 있다. 제안 모델은 네트워크 구조를 계층적 형태로 처리되도록 IoT 장치의 유사정보를 이용하고 있다. 제안 모델은 IoT 장치의 다중 접근을 안정적으로 처리하기 위해서 서명키를 이용한 암・복호키 $x_i^{n[j]}$ 와 PK_{i+1}^n을 생성하여 접근 권한이 없는 IoT 장치나 제3자가 불법적으로 접근 시도를 예방하였다. 제안 모델은 IoT 네트워크에 접속하는 수 많은 IoT 장치가 사용하는 암・복호키를 다단계 접근 방식으로 관리한다. 제안 모델은 IoT 장치간 안전한 통신을 보장하도록 위임장 m_i과 타임스탬프 T을 주기적으로 갱신하여 사용함으로써 무결성과 최신성을 제공하고 있다.

5. 결론

인더스트리 4.0과 함께 소사이어티 5.0이 최근 IoT 기술과 함께 대두되면서 IoT 관련 분야가 확대되고 있다. 특히, IoT 장치가 적용된 휴대폰, 의료서비스 등을 중심으로 활발한 활동이 이루어지고 있다. 본 논문에서는 소사이어티 5.0 기반의 IoT 사용자에 대한 다중 접근방식의 프라이버시 접근 모델을 제안하였다. 제안 모델은 가상 환경에 연동 가능한 IoT 장치의 중요 정보를 서로 동기화하는 다중 접근 방식을 사용하였다. 성능평가 결과, IoT 장치 수와 IoT 허브장치 수에 따라 IoT 장치의 효율성이 평균 5.6% 향상되었다. 정확도는 정보 수집 및 처리에 따른 정확도가 평균 15.9% 향상되었다. 향후 연구에서는 기존 연구를 기반으로 소사이어티 5.0의 다양한 환경에 연구 결과를 적용할 계획이다.

REFERENCES

[1] Y. S. Jeong, D. R. Kim & S. S. Shin. (2019). Efficient Mutual Authentication Protocol between Hospital Internet of Things Devices Using Probabilistic Attribute Information. *sustainability*, *11(24),* 7214.

[2] A. Iera, G. Morabito & L. Atzori. (2016). The internet of things moves into the cloud. *Proceedings of the 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW)*, 191.

[3] H. N. Saha, A. Mandal & A. Sinha. (2017). Recent trends in the internet of things. *Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, 1-4.

[4] J. S. KIm. (2019). Specialized on HPC Convergence Technology. *Communications of the Korean Institute of Information Scientists and Engineers*, *37(10)*, 3.

[5] Y. Wu, X. Xiong, X. Gang, & T. R. Nyberg. (2013). Study on intelligent port under the construction of smart city. *2013 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Dongguan*, 175-179.

[6] A. Belfkih, C. Duvallet & B. Sadeg. (2017). The Internet of Things for Smart Ports: Application to the Port of Le Havre. *Proceedings of the International Conference on Intelligent Platform for Smart Port (IPaSPort 2017)*, 1-2.

[7] A. Valsamis, K. Tserpes, D. Zissis, D. Anagnostopoulos & T. Varvarigou. (2017). Employing traditional machine learning algorithms for big data streams analysis: The case of object trajectory prediction. *J. Syst. Softw.*, *127*, 249-257.

[8] A. Celesti, D. Mulfari, M. Fazio, M. Villari & A. Puliafito. (2016). Exploring container virtualization in iot clouds. *Proceedings of the 2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, 1-6.

[9] K. S. Dar, A. Taherkordi & F. Eliassen. (2016). Enhancing dependability of cloud-based iot services through virtualization. *Proceedings of the 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 106-116.

[10] Y. S. Jeong. (2015) An Efficiency Management Scheme using Big Data of Healthcare Patients using Puzzy AHP. *Journal of Digital Convergence*, *13(4),* 227-233.
DOI : 10.14400/JDC.2015.13.4.227

[11] Y. S. Jeong. (2016). An Efficient IoT Healthcare Service Management Model of Location Tracking Sensor. *Journal of Digital Convergence*, *14(3)*, 261-267.
DOI : 10.14400/JDC.2016.14.3.261

[12] Y. S. Jeong. (2016). Measuring and Analyzing WiMAX Security adopt to Wireless Environment of U-Healthcare. *Journal of Digital Convergence*,

11(3), 279-284.
DOI : 10.14400/JDPM.2013.11.3.279

[13] D. S. Zois. (2016). Sequential decision-making in healthcare IoT: Real-time health monitoring treatments and interventions. *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on. IEEE*, 24-29.

[14] N. Gonzalez., C. Miers., F. Redigolo., T. Carvalho., M. Simplicio., M. Naslund & M. Pourzandi. (2011). A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. *2011 IEEE Third International Conference on Cloud Computing Technology and Science*, 231-238.

[15] Y. S. Jeong. (2014). Tracking Analysis of User Privacy Damage using Smartphone. *Journal of Convergence Society for SMB, 4(4)*, 13-18.

[16] Y. S. Jeong, D. B. Yoon & S. S. Shin. (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

정 윤 수(Yoon-Su Jeong) [정회원]

· 1998년 2월 : 청주대학교 전자계산학과 학사
· 2000년 2월 : 충북대학교 전자계산학과 석사
· 2008년 2월 : 충북대학교 전자계산학과 박사
· 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수
· 관심분야 : 유·무선 통신 보안, 정보보호, 바이오인포매틱, 헬스케어, 빅데이터, 클라우드 컴퓨팅
· E-mail : bukmunro@gmail.com

연 용 호(Yong-Ho Yon) [정회원]

· 1988년 2월 : 충북대학교 수학과 학사
· 1990년 2월 : 충북대학교 수학과 석사
· 1997년 8월 : 충북대학교 수학과 박사
· 2011년 3월 ~ 현재 : 목원대학교 교양교육원 조교수
· 관심분야 : 격자론, 수리논리, 함의대수
· E-mail : yhyon@mokwon.ac.kr