

중소기업 환경에 적합한 해쉬 체인 기반의 IoT 인증 기법

정윤수, 연용호, 구진희*
목원대학교 정보통신융합공학부

Hash-chain-based IoT authentication scheme suitable for small and medium enterprises

Yoon-Su Jeong, Yong-Ho Yon, Jin-Hee Ku*

Dept. of information Communication Convergence Engineering, Mokwon University

요약 4차 산업 혁명이 대두되면서 IoT 기술을 제조 공정에 적용하여 제품을 출시하려는 시도가 증가하고 있다. 본 논문에서는 우리나라 중소기업 중 제조업을 중심으로 IoT 장치를 손쉽게 적용하여 사용할 수 있는 해쉬 체인 기반의 IoT 인증 기법을 제안한다. 제안 기법에서는 제조업 환경에 적합한 IoT 장치를 설치한 업체를 선별하여 전체 제조 공정 중 제품 정보와 출시 정보를 효율적으로 수집·보관·관리·처리 할 수 있도록 IoT 장치 간 연계를 유지하는 것을 목적으로 한다. 또한, 제안 기법은 IoT 장치의 인증 정보를 해쉬 체인을 기반으로 구축하였기 때문에 추가적인 암호·복호 암호 알고리즘이 필요없는 것이 특징이다. 성능평가 결과, 제안 기법은 IoT 장치를 적용 유·무에 따라 제조 프로세스의 효율성이 18.5% 향상되었고, IoT 장치를 부착한 제조 공정의 업무 처리가 평균 20.1% 단축되었다. 또한, 제조 공정에 투입된 인력 감축 비용이 평균 30.7% 감소되는 것으로 나타났다.

키워드 : 중소기업, 사물인터넷, 인증, 서비스 모델, 업무 처리, 해쉬체인

Abstract With the emergence of the fourth industrial revolution, more and more attempts have been made to apply IoT technology to the manufacturing process and launch the product. In this paper, we propose IoT authentication scheme based on hash chain which can easily apply IoT device to small and medium enterprises in Korea. In the proposed method, the companies that installed IoT devices suitable for the manufacturing environment are selected to maintain the linkage between IoT devices so that product information and release information can be efficiently collected and managed during the entire manufacturing process. In addition, the proposed scheme is characterized in that it does not require an additional encryption / decryption algorithm because the authentication information of the IoT device is constructed based on a hash chain. As a result of the performance evaluation, the efficiency of the manufacturing process was improved by 18.5% and the processing of the manufacturing process with the IoT device was shortened by 20.1% on the average according to the application of the IoT device. In addition, the labor cost reduction costs in the manufacturing process decreased by an average of 30.7%.

Key Words : Small Business, IoT, Authentication, Service Model, Work Process, Hash Chain

1. 서론

최근 중소기업에서는 고령화에 따른 숙련공들의 축소

로 인하여 생산 차질이 우려되기 때문에 이에 대응하는 해결책으로 스마트공장이 새로운 방안으로 부상하고 있

다. 스마트공장이란 전통 제조 산업에 ICT를 융합하여 공장 내 설비와 센서(IoT)가 실시간으로 데이터를 수집, 분석되어 공장 내 모든 상황들을 목적된 바에 따라 스스로 제어되는 공장을 의미한다[1].

중소기업에서는 기존 제조 공장을 스마트공장으로 변경할 경우 수많은 데이터를 기반으로 각 공장의 프로세스를 분석하고, 의사결정 할 수 있기 때문에 생산현장에서 발생할 수 있는 다양한 문제들의 상관관계를 파악할 수 있다[2-6]. 예를 들어, 돌발 상황이 발생했는지 모니터링을 통해서 확인한 후 비숙련자들에게 대응 방안을 가이드할 수 있고, MES, ERP 등과 같은 시스템과 연동되어 자동 주문 접수가 가능하고 경영영상의 경영 판단이 결정되면 최적의 생산체제 하에서 운영할 수 있다[7-10].

본 논문에서는 우리나라 중소기업에서 운영하고 있는 제조 공정 시스템에 IoT 기술이 융합된 장치를 대상으로 제조 공정상 발생하는 실시간 정보를 수집·보관·관리·처리 등을 손쉽게 처리하기 위한 해쉬 체인 기반의 IoT 인증 기법을 제안한다. 제안 기법에서는 제조업 환경에 적합한 IoT 장치를 설치한 업체를 선별하여 전체 제조 공정 중 제품 관련 정보를 효율적으로 수집·보관·관리·처리 할 수 있도록 IoT 장치 간 연계를 유지하는 것을 목적으로 한다. 제안 기법은 기존 시스템의 생산 효율성과 비용 절감 효과를 얻기 위해서 다음과 같은 기능을 수행한다. 첫째, 제안 기법에서는 IoT 장치를 통해 제조공정에서 생산되는 제품의 정보를 추적, 모니터링하여 제어할 수 있다. 둘째, 기존 제조 시스템과의 연계 방안을 통해 제조업 프로세스를 확장할 수 있다. 셋째, 제안 기법은 IoT 장치의 인증 정보를 해쉬 체인을 기반으로 구축하였기 때문에 추가적인 암호·복호 암호 알고리즘이 필요 없다.

이 논문의 구성은 다음과 같다. 2장에서는 IoT 기술을 적용한 중소기업의 스마트 공장에 대해서 설명한다. 3장에서는 중소기업 제조업 생산 현장에서 활용 가능한 해쉬 체인 기반의 IoT 인증 기법을 제시하고, 4장에서는 제안 기법에 대한 평가를 분석한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

2. 관련 연구

스마트공장이란 전통 제조 산업에 ICT를 결합하여 공

장 내 설비와 센서(IoT)가 실시간으로 데이터를 수집, 분석하여 스스로 제어되는 생산체제를 의미한다[1]. Fig. 1은 스마트공장의 전체 프로세스를 파악할 수 있는 전체 개요를 보여주고 있다.

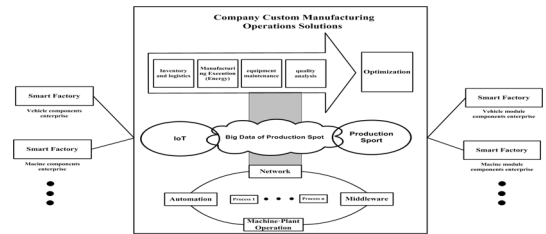


Fig. 1. Overview of Smart Factory

Fig. 1처럼 스마트공장은 기업별 제조수준·환경을 고려하여 기업의 역량을 강화하고, 기업 간 가치사슬 역량을 강화하는 것을 목적으로 한다. 중소기업에서는 전통적으로 운영하던 전문분야를 하드웨어와 소프트웨어의 다양한 영역으로 신규 비즈니스 영역을 접목하고 있다 [11-13]. 그러나, 우리나라는 대기업을 중심으로 ICT를 적용하여 제조현장을 혁신시키려는 시도를 진행하고 있으나, 대부분 외국 솔루션에 의존하고 있으며 국내 기술의 한계로 민간투자는 시작단계에 머무르고 있다.

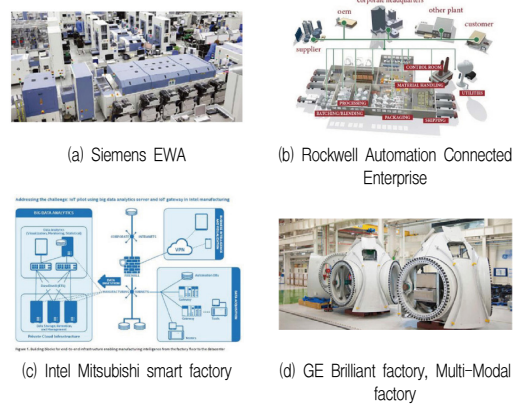


Fig. 2. Smart factory of overseas major companies

Fig. 2는 최근 해외 주요기업의 스마트 공장 현황을 보여주고 있다. 해외 주요기업들은 지능형 공장을 구현하여 생산설비, 제어시스템 및 산업용 소프트웨어를 공정 자동화 솔루션에 적용하고 있으며, 공장시설과 산업인터넷을 통해 실시간 정보 공유뿐만 아니라 품질 유지 및 돌발 상황을 예방할 수 있는 최적화된 생산 유지를 진행하

고 있다[14-16].

3. 해쉬체인 기반 IoT 장비 인증 기법

3.1 개요

4차 산업 혁명이 대두되면서 정부는 중소기업의 생산 현장을 자동화 기술을 이용하여 스마트 공장을 만들도록 유도하고 있다[17,18]. 그러나, 중소기업의 경영 문제로 인하여 모든 생산 공정 대신 부분적 생산 공정을 스마트 공정으로 만들고 있다[2,6,12]. 본 논문에서는 스마트 제조현장에서 IoT 장치를 설치한 장비의 정보를 수집 관리하기 위해서 Fig. 3과 같은 처리 과정을 갖도록 프로세스를 정의하였다.

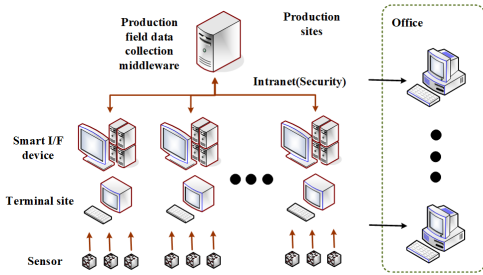


Fig. 3. Product Factory Process of Proposed Model

Fig. 3처럼 중소기업 제조 현장을 구축할 경우 생산 효율성 향상, 생산 비용 절감 및 인력 비용 절감 등의 효과가 나타난다. 반면, 제조 장비의 IoT 구축 비용 및 유지보수에 대한 비용은 증가할 수 있다. 그러나, 장기적으로 Fig. 3처럼 제조 공정을 관리할 경우 중소기업 경쟁력 향상 및 비용 절감에 대한 효과를 얻을 수 있는 효과가 있다. 또한, 제안 기법에서는 기존 제조 현장의 문제점(산업용 IoT 구현/활용, 실시간 모니터링, 제조 이력관리, 품질문제 대응, 맞춤형 클라우드 서비스 등)을 해결할 수 있는 장점이 있다.

3.2 제조 현장 내 IoT 장치 정보 수집 과정

제안 기법에서는 제조 장비수 만큼 $h^n()$ 형태로 해쉬 체인으로 IoT 장치 정보를 묶어 정보를 수집 관리하기 때문에 추가적인 암호 알고리즘 없이 수집 정보를 관리할 수 있다.

제안 기법에서는 제조 현장 내 IoT 장치 정보를 수집

하여 관리하기 위한 정보를 식 (1)과 같이 생성한다.

$$f_i^k = p(X_i^k=x|A_i^k=a) = \begin{cases} 1, & a = ID(x) \\ 0, & Otherwise \end{cases} \quad (1)$$

여기서, i 는 IoT 장치가 부착된 제조 장비 수를 의미하고, k 는 제조 장비에 부착된 IoT 장비 수를 의미한다. x 는 IoT 장비 정보를 의미하고, a 는 IoT 장비의 속성 정보를 의미한다. f_i^k 는 IoT 장치가 부착된 제조 장비에서 수집된 정보 요소(Factor)를 의미한다. A_i^k 는 IoT 장비 속성의 코드워드를 의미하고, X_i^k 는 IoT 장비의 코드워드(Codeword)를 의미한다.

식 (1)처럼 수집된 IoT 장치 정보는 연계 정보로 암호화하여 서버로 전달하여 통합 관리하게 된다. 이때, 서버에서 관리하는 수집 정보는 제조 공정에서 출시되는 실제 제품의 실시간 상태 정보를 융합하여 제조 공정에 활용한다.

3.3 IoT 장치를 위한 키 설정 과정

이 절에서는 제조 현장에서 제품을 생산하는 제조 장비 중 IoT 장치를 설치한 제조 장비 간 연계를 수행하기 위한 키를 설정하는 과정을 다음과 같이 5단계로 나타내고 있다.

- 1단계 : 제조 공장 내 IoT 장치가 부착된 장비들 간 제조 공정 중 생성되는 정보를 인증하기 위한 적절한 키를 생성하기 위해서 제안 기법에서는 제조 설비에 사용되는 전체 장치 중 IoT 장치가 설치된 장비 수로 $n-bit$ 블록 형태로 나눈다.
- 2단계 : 서버는 제조 장비의 익명 파라미터 ID 를 입력받아 키 생성 함수에 식 (2)처럼 적용한다.

$$keygen[\pi] \rightarrow \lambda \quad (2)$$

- 3단계 : 서버는 제조 현장의 장비를 체크하여 IoT 장치가 설치된 장비가 $n-bit$ 블록 형태로 정상적으로 나누어졌는지 체크한다. 체크 결과가 정상적인 결과라면 서버는 제조 장비 간 연계 정보 λ 를 각 $n-bit$ 블록이 적용하여 대칭 암호 알고리즘을 실행하고, 비정상적인 결과가 나타나면 서버는 제조 장비 간 연계 정보 λ 를 생성하기 위해서 IoT 장치가 설치된 장비 수를 이용하여 다시 $l-bit$ 블록으로

나눈다. 제조 장비 간 연계 키를 생성하는 위 과정에 대한 키 설정 알고리즘은 Table 1과 같다.

Table 1. Key Setup Algorithm for IoT Device

Algorithm 1 Key Setup Algorithm for IoT Device
Input The number of manufacturing equipment and anonymity of manufacturing equipment due to the establishment of IoT device
Output Linkage λ between manufacturing equipment
1: Procedure: Key Setup
2: The entire device used in the manufacturing facility is divided into blocks using the number of IoT devices installed.
3: The server receives an anonymous parameter ID of the manufacturing equipment and applies it to the key generation function as $keygen[\pi] \rightarrow \lambda$.
4: if The IoT device has already been divided into $n-bit$ blocks with the number of installed devices then
5: The server executes the symmetric encryption algorithm by applying the association information λ between the manufacturing equipments to each $n-bit$ block.
6: else
7: In order to generate the linkage information λ between the manufacturing equipments, the server divides the IoT devices into $l-bit$ blocks using the number of equipments installed.
8: end if
9: end procedure

3.4 IoT 장치 인증 과정

이 절에서는 IoT 장치가 부착된 장비의 인증 과정을 수행하기 위한 과정으로써 다음과 같이 4단계로 나타내고 있다.

- 1단계 : 인증 서버는 인증 핸들 정보 η 를 얻기 위해서 식 (3)과 같은 과정을 수행한다.

$$encode(\tilde{K};\lambda)[\pi] \rightarrow (\tilde{K},\eta) \quad (3)$$

- 2단계 : 인증 서버는 인증 핸들 정보 η 를 통해 제조 장비의 인증 정보 AI 와 각 IoT 장치의 코드 값 c 를 추출한다.
- 3단계 : 인증 서버가 $challenge(AI,c)$ 를 제조 장비에게 전달하면 제조 장비는 $response(ID) \rightarrow r$ 을 수행한다.
- 4단계 : 인증 서버는 $challenge(AI,c)$ 에 응답한 $response(ID) \rightarrow r$ 가 무결(Valid)한지를 체크한다. 체크 결과 이상이 없다면 Boolean 변수를 1로 설정

정하고 그렇지 않다면 0으로 설정한다.

IoT 장치의 인증 과정에 대한 인증 처리 알고리즘은 Table 2와 같다.

Table 2. Authentication Process for IoT Device

Algorithm 2 Authentication Algorithm for IoT Device
Input Linkage information λ between equipment installed at the manufacturing site
Output The authentication information AI of the manufacturing equipment to be stored in the server and the code value c of the IoT device.
1: Procedure: IoT Device Authentication Process
2: The authentication server performs $encode(\tilde{K};\lambda)[\pi] \rightarrow (\tilde{K},\eta)$ to obtain authentication handle information η .
3: The authentication server extracts the authentication information AI of the manufacturing equipment and the code value c of each IoT device through the authentication handle information η .
4: When the authentication server delivers the $challenge(AI,c)$ to the manufacturing equipment, the manufacturing equipment performs $response(ID) \rightarrow r$.
5: if The authentication server receives the request r then
6: Authentication server checks r valid or not
7: if value r is valid then
8: Authentication server outputs the Boolean variable '1'
9: else
10: Authentication server outputs the Boolean variable '0'
11: end if
12: else
13: $CT \leftarrow CT+1$
14: if $CT < i$ then
15: The authentication server performs the $response(ID) \rightarrow r$ and sends it back to the manufacturing equipment.
16: else
17: Authentication server outputs the Boolean variable '0'
18: end if
19: end if
20: end procedure

4. 평가

제안 기법은 우리나라 전체 중소기업의 제조 공장 중 IoT 장치를 제조 프로세스에 적용한 50개 업체를 대상으로 설문 조사한 결과를 바탕으로 평가 분석하였다. 분석 결과를 바탕으로 제안 기법은 IoT 기술을 중소기업 제조업 환경에 적용한 업체를 대상으로 전체 제조 공정 중 제품 정보와 출시 정보를 효율적으로 수집·관리할 수 있도록 IoT 장치 간 인증 정보를 연계한 제조 프로세스의 효율성, IoT 장치를 부착한 제조 공정의 업무 처리, 제조

공정에 투입된 인력 감축 비용 등을 평가하였다.

4.1 제조 공정 프로세스에 따른 효율성 분석

Fig. 4는 IoT 기술을 제조 공정에 적용하여 전체 제조 공정 프로세스에 따른 효율성 분석을 보여주고 있다. 분석 결과, 제조 공정 수(1~10개)와 IoT 장치 적용 유·무에 따라 제조 공정 프로세스의 효율성은 IoT 장치를 적용하지 않았을 때보다 18.5% 향상되었다. 이 같은 결과는 수작업으로 제조 공정을 처리했을 때보다 IoT 장치를 적용한 제조 공정이 생산 라인에서 발생할 수 있는 불량률 발생 비율이 낮아졌기 때문에 나타난 결과이다. 또한, 실시간으로 처리되는 공정별 작업 지연이 줄어들었기 때문에 나타난 결과이다.

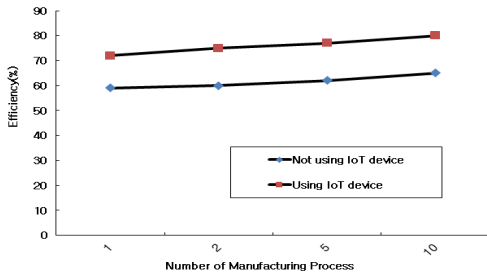


Fig. 4. Analysis of efficiency according to manufacturing process

4.2 제조 공정의 업무처리 분석

Fig. 5는 IoT 장치를 부착한 장비 수에 따른 제조 공정의 업무 처리 시간을 보여주고 있다. Fig. 5의 분석 결과, IoT 장치를 부착한 제조 공정의 업무 처리가 평균 20.1% 단축되었다. 이 같은 결과는 IoT를 이용한 제조 공정에서 수작업으로 이루어졌던 업무 과정을 자동/반자동화로 변경하였기 때문에 나타난 결과이다.

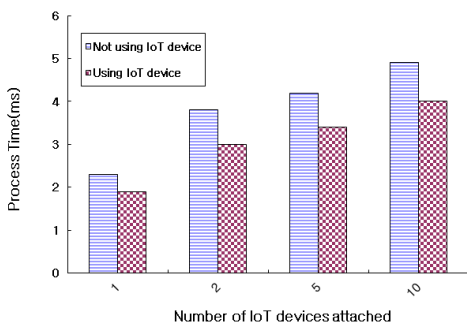


Fig. 5. Business process analysis of manufacturing process

4.3 IoT 기술 기반의 인력 비용 분석

Fig. 6은 IoT 기술을 제조 공정에 반영하여 제조 공장에서 근무하는 인력 비용을 분석하고 있다. 분석 결과, IoT 기술을 제조 공정에 반영하여 스마트 공장으로 운영하도록 만들면 제조 공정에 투입된 인력 감축 비용이 평균 30.7% 감소되는 것으로 나타났다. 이 같은 결과는 IoT 기술을 제조 장비에 얼마만큼 적용하여 사용하는가에 따라 달라질 수 있다. 최근 경기불황으로 인하여 중소기업은 IoT 기술을 제조 장비에 적용하는 것을 고심하고 있다. 그러나, 중소기업은 장기적으로 비용 절감 및 제품 생산에 대한 효율성 향상을 위해서 점진적으로 IoT 기술을 제조 장비에 적용하려는 시도를 하고 있다.

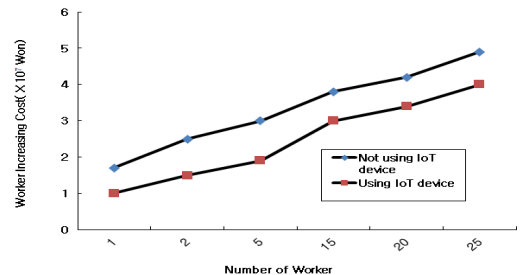


Fig. 6. Analysis of labor cost based on IoT technology

5. 결론

글로벌 경제의 저성장 기조와 생산성 하락으로 인해 신성장 동력이 필요한 가운데 주요국·기업들은 4차 산업혁명 대응 및 산업경쟁력 강화를 위한 산업인터넷·스마트 공장에 대한 관심이 증대하고 있다. 본 논문에서는 제조 공정상 발생하는 실시간 정보를 수집·보관·관리·처리 등을 손쉽게 처리하여 스마트공장을 구현할 수 있는 해쉬 체인 기반의 IoT 인증 기법을 제안한다. 제안 기법은 전체 제조 공정 중 제품 정보와 출시 정보를 효율적으로 수집·관리할 수 있도록 IoT 장치 간 연계를 유지한다. 또한, 제안 기법에서는 IoT 장치를 통해 제조공정에서 생산되는 제품의 정보를 추적, 모니터링하여 제어할 수 있다. 특히, 제안 기법은 기존 제조 시스템과의 연계 방안을 통해 제조업 프로세스를 확장뿐만 아니라 추가적인 암·복호 알고리즘이 필요 없는 것이 특징이다. 성능평가 결과, 제안 기법은 IoT 장치를 적용 유·무에 따라 제조 프로세스의 효율성이 18.5% 향상되었고, IoT

장치를 부착한 제조 공정의 업무 처리가 평균 20.1% 단축되었다. 또한, 제조 공정에 투입된 인력 감축 비용이 평균 30.7% 감소되는 것으로 나타났다. 향후 연구에서는 본 연구의 결과를 기반으로 중소기업 스마트 공장의 활성화 방안 연구를 수행할 계획이다.

ACKNOWLEDGMENTS

본 연구는 산업통상자원부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음.

REFERENCES

- [1] POSCOICT. (2016). *What is Smart Factory?*. POSCOICT. <http://smartfuture-poscoict.co.kr/306>
- [2] Y. S. Jeong. (2011). A User Privacy Protection Scheme based on Password through User Information Virtuality in Cloud Computing. *Journal of Convergence Society for SMB, 1(1)*, 29-37.
- [3] K. I. Kim. (2014). An Exploratory Study IMS Performance Modeling Using Information Systems Success Model. *Journal of Digital Convergence, 12(3)*, 127-140.
DOI : 10.14400/jdc.2014.12.3.127
- [4] K. I. Kim. (2015). The Effects on Improvement of IMS Through Corrective Actions. *Journal of the Convergence Society for SMB, 5(4)*, 1-4.
- [5] K. I. Kim. (2012). Causes Analysis of Increasing Revocation for IMS Certification in small and Medium-size Enterprises. *Journal of the Convergence Society for SMB, 2(2)*, 7-12.
- [6] N. J. Allen & J. P. Meyer. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. *Journal of Occupational and Organizational Psychology, 63(1)*, 1-18.
DOI : 10.1111/j.2044-8325.1990.tb00506.x
- [7] R. N. Kanungo. (1982). Measurement of job and work involvement. *Journal of Applied Psychology, 67(3)*, 341-349.
DOI : 10.1037//0021-9010.67.3.341
- [8] B. J. Babin & J. S. Boles. (1996). The effects of perceived co-worker involvement and supervisor support on service provider role stress, performance and job satisfaction. *Journal of retailing, 72(1)*, 57-75.
DOI : 10.1016/s0022-4359(96)90005-6
- [9] S. S. Shin, Y. S. Jeong & Y. J. An. (2015). A Study of Analysis and Response and Plan for National and International Security Practices using Fin-Tech Technologies. *Journal of Convergence Society for SMB, 5(3)*, 1-7.
- [10] Y. S. Jeong. (2016). A Study of An Efficient Clustering Processing Scheme of Patient Disease Information for Cloud Computing Environment. *Journal of Convergence Society for SMB, 6(1)*, 33-38.
DOI : 10.22156/cs4smb.2016.6.1.033
- [11] D. Ilic, S. Kamouskos, P. Silva & S. Detzler. (2014). A system for enabling facility management to achieve deterministic energy behaviour in the smart grid era. *International Conference on Smart Grids and Green IT systems* (pp. 170-178). Barcelona : Smart Greens.
DOI : 10.5220/0004861101700178
- [12] C. F. Lai, Y. X. Lai, L. T. Yang & H. C. Chao. (2012). *Integration of IoT Energy Management System with Appliance and Activity Recognition*. Besancon : 2012 IEEE International Conference on Green Computing and Communications (pp. 66-71). Besancon : IEEE.
DOI : 10.1109/greencom.2012.20
- [13] D. Ilic, S. Kamouskos & M. Wilhelm. (2013). A comparative analysis of smart metering data aggregation performance. *2013 11th IEEE International Conference on Industrial Informatics* (pp. 434-439). Bochum : IEEE.
DOI : 10.1109/indin.2013.6622924
- [14] Y. S. Jeong. (2010). An Efficiency Management Scheme using Big Data of Healthcare Patients using Puzzy AHP. *Journal of Digital Convergence, 13(4)*, 227-234.
DOI : 10.14400/jdc.2015.13.4.227
- [15] Y. S. Jeong. (2016). Design of Prevention Model according to a Dysfunctional of Corporate Information. *Journal of Convergence Society for SMB, 6(2)*, 11-17.
DOI : 10.22156/cs4smb.2016.6.2.011
- [16] L. Raymond. (1985). Organizational Characteristics and MIS success in the Context of Small Business. *MIS Quarterly, 9(1)*, 37-52.
DOI : 10.2307/249272
- [17] Y. S. Jeong. (2014). Tracking Analysis of User Privacy Damage using Smartphone. *Journal of Convergence Society for SMB, 4(4)*, 13-18.
- [18] Y. S. Jeong. (2012). Design of Security Model for Service of Company Information. *Journal of Convergence Society for SMB, 2(2)*, 43-49.

저 자 소 개

정 윤 수(Yoon-Su Jeong)

[중신회원]



- 1998년 2월 : 충북대학교 전자계산학과 학사
- 2000년 2월 : 충북대학교 전자계산학과 석사
- 2008년 2월 : 충북대학교 전자계산학과 박사

▪ 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수
<관심분야> : 유·무선 통신 보안, 정보보호, 헬스케어, 빅 데이터

연 용 호(Yong-Ho Yon)

[정회원]

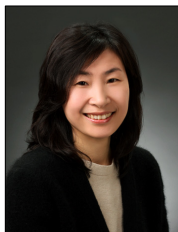


- 1988년 2월 : 충북대학교 수학과 학사
- 1990년 2월 : 충북대학교 수학과 석사
- 1997년 8월 : 충북대학교 수학과 박사

▪ 2011년 3월 ~ 현재 : 목원대학교 정보통신융합공학부 교수
<관심분야> : 격자론, 격자암호, 양자논리

구 진 희(Jin-Hee Ku)

[정회원]



- 2001년 2월 : 충남대학교 컴퓨터과학교육학과 교육학석사
- 2010년 2월 : 충남대학교 공업(컴퓨터)교육학과 교육학박사
- 2010년 9월 ~ 현재 : 목원대학교 정보통신융합공학부 교수

<관심분야> : 컴퓨터과학 교육, 빅데이터, 데이터마이닝, 클라우드 컴퓨팅