Journal of the Korea Convergence Society
Vol. 9. No. 4, pp. 9-14, 2018

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2018.9.4.009

# 클라우드 환경에서 이중 복제 키를 사용한 사용자 프라이버시 보호 기법

정윤수
목원대학교 정보통신융합공학부

# User Privacy Security Scheme using Double Replication Key in the Cloud Environment

**Yoon-Su Jeong**
**Dept. of information Communication & Convergence Engineering, Mokwon University**

요 약 최근 인터넷 속도가 빨라지면서 클라우드 환경에서는 서비스 수신 장치가 일반 PC에서 휴대폰 또는 태블릿 PC 등의 소형 장치로 변화되고 있는 추세이다. 휴대폰 또는 태브릿 PC 등과 같은 소형 장치들은 유선보다는 무선에서 사용되는 경우가 많기 때문에 제3자로부터 악의적으로 개인 정보가 노출될 수 있는 문제점이 많다. 본 논문에서는 다양한 무선 매체를 통해서 서비스되고 있는 클라우드 서비스 중에서 사용자의 프라이버시를 제3자로부터 안전하게 보호할 수 있는 이중 복제키 생성 과정을 통한 사용자 프라이버시 보호 기법을 제안한다. 제안 기법은 복제된 키를 서버와 중간 장치의 동기화를 위해서 사용되며, 사용자의 프라이버시를 보호하는 인증 처리 과정의 시간을 단축하는 것을 목표로 한다. 이 때, 제안 기법은 서버와 중간 장치의 동기화에 $Interleave()$함수와 랜덤수를 사용하기 때문에 제3자의 악의적인 공격을 안전하게 예방할 수 있다.

주제어 : 클라우드 서비스, 이중 복제 키, 사용자 프라이버시, 보안, 인증

**Abstract** Recently, as the internet speed is getting faster, in the cloud environment, the service receiving device is changing from a general PC to a compact device such as a mobile phone or a tablet PC. Since handheld devices such as mobile phones or tablet PCs are often used in wireless rather than wired, there are many problems that personal information may be exposed maliciously from a third party. In this paper, we propose a user privacy protection scheme through a duplicate duplicate key generation process which can safely protect user 's privacy from third party among cloud services being served through various wireless media. The proposed scheme is used to synchronize the duplicated key between the server and the intermediary device, and aims at shortening the time of the authentication process protecting the user 's privacy. In this case, the proposed scheme uses $Interleave()$ function and random number to synchronize the server and the intermediary device, so it can safely prevent the malicious attack of the third party.

**Key Words :** Cloud Service, Double Replication Key, User Privacy, Security, Authentication

## 1. 서론

최근 IoT 및 컴퓨팅 자원을 기반으로 서비스를 제공하는 클라우드 컴퓨팅이 큰 관심을 받고 있다[1]. 그러나, 클라우드 환경에서 동작되는 IoT 장치의 보안요구 사항에 대한 필요성이 대두되고 있지만 특별한 대책 마련은 못하고 있는 실정이다.

대부분의 클라우드 서비스는 PC 뿐만 아니라 모바일

*Corresponding Author : Yoon-Su Jeong (bukmunro@gmail.com)
Received February 13, 2018 Revised March 29, 2018
Accepted April 20, 2018 Published April 28, 2018

단말기를 모두 지원하고 있어 다양한 네트워크 방식을 통해 접근하기 때문에 사용자가 원하는 원활한 서비스를 제공받기 위해서는 모바일 장치에 맞는 서비스를 개발업체가 각각 만들어야 한다[2,3].

클라우드 컴퓨팅 환경에서는 송·수신되는 데이터를 보호하기 위해서 다양한 암호 알고리즘 및 키 생성 방법을 사용하고 있다. 그러나, 클라우드 컴퓨팅 시스템에 저장되는 데이터는 암호화한 후 저장되어도 기밀 정보가 제3자에게 유출될 수 있는 문제점이 존재한다[4].

본 논문에서는 클라우드 환경에서 사용자가 다양한 매체를 통해서 클라우드 서비스를 제공받고 있는 상황에서 사용자가 모르는 사이에 사용자의 프라이버시가 노출되어 악용되는 것을 예방하고자 사용자가 사용하는 키를 이중 복제 하여 사용자의 프라이버시를 보호하는 기법을 제안한다. 제안 기법의 목적은 클라우드 환경을 구성하는 장치의 부하를 줄이면서 제3자로부터 사용자의 프라이버시를 효율적으로 예방하는 것이다. 제안 기법은 사용자의 키를 이중으로 복제하여 사용자와 서버, 사용자와 중간 게이트웨이 장치간 사용자의 인증을 동시에 수행한다. 제안 기법에서는 인증 처리 시간을 줄이기 위해서 중간 게이트웨이 장치에 사용자의 복제키를 저장하여 서버가 사용자의 인증을 요청할 경우 사용자가 소유하고 있는 키 대신 복재 키를 사용하여 서버와이 인증을 백그라우드로 실행한다. 이때, 제안 기법은 사용자와 서버, 중간게이트웨이와 서버 간 동기화가 이루어지게 하기 위해서 $Interleave()$함수를 사용한다. $Interleave()$함수는 중간 게이트웨이 역할을 수행하는 장치와 인증서버에서 생성한 랜덤수를 적용하기 때문에 제3자의 악의적인 공격을 예방하여 사용자의 프라이버시를 보호할 수 있다.

이 논문의 구성은 다음과 같다. 2장에서는 클라우드 환경에서 사용자의 프라이버시를 보호하는 기존연구에 대해서 알아본다. 3장에서는 클라우드 환경에서 이중 키를 사용한 사용자 프라이버시 보호 기법을 제안하고, 4장에서는 제안 기법의 안전성 측면에서 기존에 제신된 보안 항목에 대해서 평가하고 마지막으로 5장에서 결론을 맺는다.

## 2. 관련연구

스토리지 그룹화, 보안 문제, 프로세스 및 메모리 보안 문제, 클라우드 시스템으 IoT 노드 등에 대한 클라우드 컴퓨팅에 대한 많은 연구가 현재까지 진행되고 있다.

클라우드 컴퓨팅은 인터넷을 통해 많은 양의 가상 스토리지를 사용하여 값 비싼 대규모 컴퓨팅 인프라를 구축할 수 있는 장점은 있지만 로컬 컴퓨팅에 대한 변경으로 많은 보안 문제가 발생할 수 있는 문제점을 가지고 있다.

Singh et al. 은 클라우드 컴퓨팅의 기본, 클라우드 환경과 관련된 보안 문제 및 Focusses 클라우드 보안과 관련된 다양한 보안 이슈들에 대해서 제시하였다[5].

Singh et al.은 클라우드 컴퓨팅과 관련된 보안 문제에 대해서 3계층 보안 아키텍처를 제안했다[6]. Zhang et al. 은 다른 알고리즘을 사용하여 체계적으로 클라우드 환경의 보안 문제를 분석하였으며 태클 이 외에도 다양한 150여개의 기사들을 토론하였다[7]. Varadharajan et al. 은 유연한 보안 서비스를 위해서 CSP가 수행하는 보안 서비스 일부를 개인이 제공하도록 하고 있다[8].

클라우드 시스템에서 IoT의 마이그레이션이 된 이후에 Iera et al.은 클라우드에서 IoT를 지원하는 특정 솔루션을 제안하였다[9]. 이 솔루션은 기존의 IoT 클라우드 서비스는 물론 다양한 장·단점을 제시하고 있다. Saha et al.은 클라우드 컴퓨팅, 자율제어, IoT 뿐만 아니라 인터넷, 무선 센서 및 액추에이터의 동기화 방법에 대해서 언급하고 있다[10]. Celesti et al. 은 경량화 될 수 있는 하이퍼 바이저 기반 접근 방식의 대안으로 IoT 클라우드 서비스를 향상시킬 수 있는 장치를 구현하였다[11]. Dar et al. 은 SicthSense 클라우드 플랫폼을 사용하여 수요에 따른 가용성 및 확률을 얻기 위한측정 항목을 선택하여 가상화 프레임워크를 제안하였다[12].

## 3. 이중 복제 키를 이용한 사용자 프라이버시 보호 기법

이 논문에서는 클라우드 환경에서 사용자의 프라이버시를 보호하기 위해서 사용자가 사용하는 키를 복제하여 사용자의 프라이버시를 보호하고 있으며, 사용자와 서버, 사용자와 중간 게이트웨이 장치로 구분하여 사용자의 프라이버시를 2중으로 보호하는 기법을 제안한다.

### 3.1 개요

클라우드 환경에서 서비스를 이용하는 수많은 사용자

들은 서비스 종류에 따라 사용자를 그룹으로 묶어 서비스를 제공받는다. 그러나, 현재 운영되고 있는 대부분의 클라우드 서비스는 사용자의 접근 권한에 대한 특별한 정책 변경 없이도 서비스를 제공받을 수 있어 제3자가 불법적으로 사용자의 프라이버시 정보를 이용할 수 있다[13-17]. 제안 기법에서는 이러한 문제점을 해결하기 위해서 사용자 그룹에 대한 정보를 그룹 인덱스 정보로 표현하여 중간 장치에서 사용자의 정보와 그룹 인덱스 정보를 해쉬한다. 중간 장치는 사용자 정보와 그룹 인덱스 정보를 캐쉬하여 제3자가 악의적으로 사용자의 프라이버시 정보를 이용하지 못하도록 서버의 인증 수행을 최소화하도록 한다.

제안 기법은 효율성과 안정성을 극대화하기 위해서 사용자 그룹을 생성할 때 $n$개의 그룹을 만들어 사용자의 프라이버시 정보를 계층적 분산형태로 배치될 수 있도록 해쉬한 후 중간 장치에게 전달한다. 중간 장치의 역할은 크게 2가지 목적이 있다. 첫째, 중간 장치는 사용자가 클라우드 서비스를 안전하게 제공받을 수 있는 복제키($K_1$과 $K_2$)를 생성하여 사용자의 프라이버시를 제3자가 불법적으로 사용하지 못하도록 한다. 둘째, 사용자가 생성한 랜덤키 $ur$과 중간 장치가 생성한 랜덤 키 $gr$를 해쉬함수에 적용하여 사용자를 효율적으로 인증함으로써 사용자와 그룹이 효율적으로 클라우드 서비스를 제공받을 있도록 한다.

제안 기법에서 전체적으로 동작되는 과정은 그림1과 같다. 그림 1처럼 제안 기법은 사용자의 프라이버시 정보를 $H_U$: {0,1} → $Z_N$으로 표현한 후 그룹 정보를 $H_P$:{0,1}$^*$×$Z_N$→$Z_P$ 와 같이 나타내어 중간 장치간 인터리브하도록 해쉬 체인으로 묶어 연결한다. 중간 장치는 식 (1)처럼 연결 정도값을 행렬로 나타내어 계층적 구조를 나타낼 있도록 구성한다.

$$CI_k = \begin{pmatrix} x_{00} \cdots x_{0j} \\ \cdots \ \cdots \ \cdots \\ x_{i0} \cdots x_{ij} \end{pmatrix}, \ k=1,2,.., \ n \qquad \text{식 (1)}$$

여기서, $i$는 사용자의 프라이버시 정보를 나타내는 행의 순서를 의미하며 범위는 $i$=1,2,.., $n$처럼 나타낸다. $j$는 중간 장치간 인터리브할 수 있도록 연결한 해쉬 체인 정도값을 의미하며 범위는 ,$j$=1,2,..,$n$처럼 나타낸다.

## 3.2 용어 정의

표 1은 제안 기법에서 사용한 용어를 대한 설명이다.

Table 1. Notations

| Notation | Definition |
|---|---|
| $SK_i$ | Shared key |
| $q$ | The private key selected between [2, $n$-2] |
| $Q$ | The public key computed via $q \times P$ |
| $ak_i$ | Auxiliary key |
| $sk_i$ | Session key |
| $H()$ | Hash function |
| $ur$, $gr$ | Random key |
| $T$ | Time stamp |

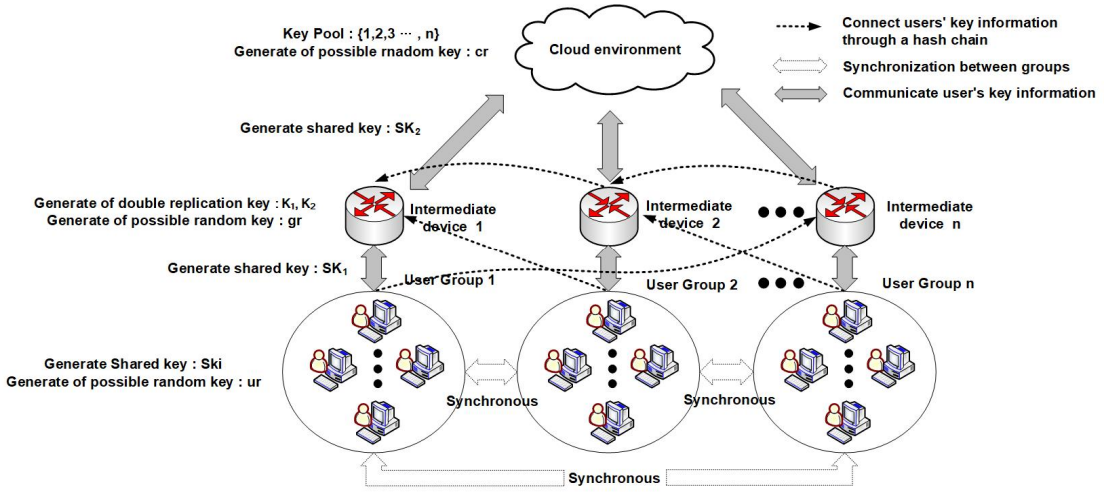



Fig. 1. Architecture overview

### 3.3 사용자 프라이버시를 위한 키 생성 및 초기화

이 절에서는 클라우드 환경에서 사용되는 사용자의 프라이버시 정보를 제3자가 불법적으로 악용하는 것을 예방할 수 있도록 중간 장치가 이중 복제키를 생성하여 사용자를 인증할 수 있도록 한다. 클라우드 서비스를 이용하는 사용자가 사용자의 프라이버시 정보를 안전하게 서버에 등록하기 위해서는 다음과 같은 키 생성 및 초기화 과정이 필요하다.

● 단계 1 : 사용자의 프라이버시 정보 생성

이 단계에서는 사용자의 프라이버시 정보 $\vec{p}$와 를 식 (2)처럼 생성한다. 여기서, $n$은 사용자의 중요 정보 수를 의미한다.

$$\vec{p} = (a_1, a_2, \cdot \cdot \cdot, a_n) \quad (2)$$

● 단계 2 : 사용자의 프라이버시 전달

단계 1에서 생성된 사용자의 프라이버시 정보 $\vec{p}$는 사용자의 인식자 정보 $UI_i$와 랜덤키 $ur$를 공유키 $SK_i$로 암호화하여 중간 장치에게 전달한다. 여기서, 공유키 $SK_i$는 안전한 경로를 통해 사전에 공유된 키를 의미한다.

$$Transfer \ E_{SK_i}(\vec{p}, UI_i, ur) \quad (3)$$

● 단계 3 : 이중 복제 키 생성

중간 장치는 사용자로부터 전달된 $E_{SK_i}(\vec{p}, UI_i, ur)$를 사전 공유된 공유키 $SK_i$를 이용하여 복호화한 후 사용자의 인식자 정보 $UI_i$와 호환할 수 있는 랜덤 키 $gr$를 식 (4)과 같이 생성한다.

$$Generate \quad gr \in Z_q^* \quad (4)$$

중간 장치는 사용자의 프라이버시 정보를 사용자와 서버간 중간 역할을 수행하기 위해서 식 (5) ~ 식 (6) 과 같은 과정을 통해 이중 복제 키 $sk_i$를 생성한다.

$$ak_i = (q^{x+at_1}, q^{t_1}, q^{t_2}) \quad (5)$$

$$sk_i = H(UI_i \| \vec{p} \| ak_i) \ \| \ T \ \| \ SEN \quad (6)$$

여기서, $sk_i$는 공유키($ur$, $sr$) 이외에 사용자의 프라이버시를 제3자에게 악의적으로 도용하는 것을 막는 동시에 중간 장치의 성능 개선을 위해 사용되는 캐쉬 기능의 세션키를 의미한다. $T$는 세션키 $sk_i$가 사용될 수 있는 타임스탬프를 의미한다.

● 단계 4 : 해쉬 정보 $HI_i$ 생성

이 단계는 중간 장치가 사용자의 그룹 인덱스 정보 $DII_i$를 생성한다. 중간 장치는 사용자의 그룹 블록 $B_i$과 사용자의 프라이버시 정보 $\vec{p_i}$을 이용하여 식 (7)과 같은 해쉬 정보 $HI_i$를 생성한 후 식 (8)과 같은 그룹 인덱스 정보 $DII_i$를 생성한다.

$$HI_i = H(B_i, \vec{p_i}), \quad 1 \le i \le n \quad (7)$$

$$DII_i = H(B_i) \in L, \quad 1 \le i \le n \quad (8)$$

여기서, $L$는 그룹 인덱스 정보 $DII_i$와 함께 사용자 프라이버시 정보 추출에 사용 해쉬 길이 값이 된다.

● 단계 5 : 이중 복제 키 $sk_i$와 룹 인덱스 정보 $DII_i$를 서버에 등록

이 단계는 중간 장치가 사용자의 프라이버시 보호에 사용되는 이중 복제 키 $sk_i$와 그룹 인덱스 정보 $DII_i$를 공유키 $gr$을 이용하여 식 (9)처럼 암호화하여 서버에 전달한다.

$$Transfer \ E_{gr}(sk_i, DII_i) \quad (9)$$

## 4. 평가

### 4.1 보안공격에 따른 분석

#### 4.1.1 다단계 서비스 접근인증에 따른 공격

제안 기법은 $ak_i = (q^{x+at_1}, q^{t_1}, q^{t_2})$와 $sk_i = H(UI_i \| \vec{p} \| ak_i)$ 같은 이중 복제 키를 중간 장치가 생성함으로써 권한이 없는 중간 장치나 제3자의 불법적인 접근을 허용하지 않는다. 제안 기법은 단계별로 장치 인증에 사용하는 세션키를 이중으로 사용하기 때문에 다단계 서비스 접근 인증 공격에 안전하다.

4.1.2 사용자 프라이버시 공격

제안 기법은 클라우드 서비스를 제공받는 사용자의 프라이버시를 보호하기 위해서 사용자와 중간 장치가 생성한 랜덤 수를 Interleave()함수에 적용하여 사전에 동의한 공유키로 암호화하여 송•수신하기 때문에 사용자의 프라이버시 정보를 보호할 수 있다. 이 같은 방법은 클라우드 서비스를 제공받는 수많은 사용자 그룹을 손쉽게 관리할 수 있기 때문에 사용자 프라이버시에 대한 가용성을 보장받을 수 있다.

4.1.3 Blackhole/Sinkhole 공격에 따른 보안

제안 기법은 클라우드를 구성하는 중간 장치의 동작 과정에서 발생할 수 있는 Blackhole/Sinkhole 공격을 예방하기 위해서 세션키 $sk_i$를 생성할 때 타임스탬프 $T$와 연속번호 $SEQ$를 사용한다. 타임스탬프 $T$와 연속번호 $SEQ$을 사용하는 이유는 불법적인 통신을 원하는 제3자가 플로딩 기반의 프로토콜을 사용하는 통신 사이에서 패킷 패싱과 같은 공격을 예방하기 위해서이다. 또한, 제안 기법은 타임스탬프 $T$와 연속번호 $SEQ$ 이외에 중간 장치가 랜덤 키 $gr$를 주기적으로 갱신 및 체크하기 때문에 Blackhole/Sinkhole 공격을 예방할 수있다.

4.1.4 Hello 플로우 공격에 따른 보안

제안 기법은 클라우드 환경에서 흔하게 발생할 수 있는 Hello 플로우 공격을 예방하기 위해서 해쉬 정보 $HI_i$와 그룹 인덱스 정보 $DII_i$, 그리고 랜덤 값($ur$, $gr$)등을 생성하기 때문에 사용자와 중간 장치간 안전한 통신을 보장한다. 또한, 제안 기법은 세션키 $sk_i$와 함께 전달되는 타임스탬프 $T$와 연속번호 $SEQ$, 랜덤 값($ur$, $gr$)은 주기적으로 변경하여 무결성 및 최신성을 제공한다.

4.1.5 웜홀 공격에 따른 보안

제안 기법에서는 사용자의 프라이버시 정보를 수집하기 위해서 네트워크의 팻킷(또는 비트) 정보를 기록 및 추적하여 사용자와 직접 터널링을 맺는 웜홀(Wormhole) 공격이 발생할 수 있다. 그러나, 제안 기법에서는 $Interleave()$함수를 사용하기 때문에 웜홀 공격을 예방할 수 있다. 또한, 제안 기법은 사용자와 중간 장치가 생성한 랜덤수($ur$, $gr$)와 해쉬 정보 $HI_i$ 및 그룹 인덱스 정보 $DII_i$,를 사용하기 때문에 웜홀 공격에 안전하다.

4.2 개선사항

제안 기법은 클라우드 환경에서 이중 복제 키를 이용하여 사용자의 프라이버시를 제공하고 있지만 이중 복제키를 생성하는 중간 장치가 확실히 감염되지 않고 사용자가 무분별하게 이중 복제키를 생성하기 위해 필요한 정보를 노출시키지 말아야 하는 문제점이 있다. 또한, 공격자가 중간 장치에 물리적으로 직접 접근하거나 그렇지 않은 공격자에 의해 완벽하게 랜덤 키를 원천적으로 보호하지는 못하기 때문에 안전성을 향상시키기 위한 추가 연구가 필요하다.

## 5. 결론

클라우드 환경에서 사용자의 프라이버시를 안전하게 보호하기 위한 연구가 최근 증가하고 있다. 클라우드 환경은 수 많은 사용자들이 접속하여 서비스를 제공받기 때문에 기존 보안 문제이외에 추가로 발생되는 보안 문제들이 존재한다. 클라우드 환경에서는 보안 문제를 해결하기 위한 해결책이 현재로써는 완벽하게 제공되고 있지 않기 때문에 이러한 부분을 해결하기 위한 연구가 필요하다. 본 논문에서는 다양한 무선 매체를 통해서 서비스되고 있는 클라우드 서비스 중에서 사용자의 프라이버시를 제3자로부터 안전하게 보호할 수 있는 이중 복제키 생성 기법을 제안하였다. 제안 기법은 사용자의 프라이버시를 보호하는 인증 처리 과정에서 복제된 키를 사용함으로써 클라우드 환경에서 발생할 수 있는 보안 문제를 해결하고 있다. 또한, 사용자와 중장 장치, 사용자가 소속된 그룹과 다른 그룹간 동기화를 이루기 위해서 $Interleave()$함수와 랜덤수를 사용하였다. 이러한 기능을 사용하는 이유는 제3자로부터 악의적인 공격을 안전하게 예방하기 위해서이다. 향후 연구에서는 본 연구의 결과를 기반으로 클라우드 컴퓨팅 환경에서 사용자의 속성을 다계층의 권한 기능을 적용하여 기존기법과 비교 평가할 계획이다.

## REFERENCES

[1] J. G. Choi & B. N. Noh. (2011). Security Technology Research in Cloud Computing Environment. *Journal of Security Engineering, 8(3),* 371-384.

[2] 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.

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

[4] Y. S. Jeong. (2016). Measuring and Analyzing WiMAX Security adopt to Wireless Environment of U-Healthcare. *Journal of Digital Convergence, 11(3),* pp. 279-284.

[5] A. Singh & K. Chatterjee. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79, 88 - 115.

[6] S. Singh, Y.-S. Jeong & J. H. Park. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, 75, 200 - 222.

[7] J. Zhang, H. Huang & X. Wang. (2016). Resource provision algorithms in cloud computing: A survey. *Journal of Network and Computer Applications, 64,* 23 - 42.

[8] V. Varadharajan & U. Tupakula. (2014). Security as a service model for cloud environment. *IEEE Transactions on Network and Service Management, 11(1),* 60 - 75.

[9] 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 - 191.

[10] 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.

[11] 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.

[12] 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.

[13] Y. S. Jeong & S. H. Lee. (2015). Personal Information Leakage Prevention Scheme of Smartphone Users in the Mobile Office Environment. *Journal of Digital Convergence, 13(5),* 205-211.

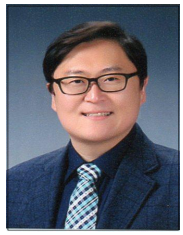
[14] B. Anggorojati, N. R. Prasad & R. Prasad. (2014). Secure capability-based access control in the m2m local cloud platform. *Proceedings of the 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE),* 1 - 5.

[15] A. Ouaddah, H. Mousannif, A. A. Elkalam & A. A. Ouahman. (2017). Access control in the internet of things: Big challenges and new opportunities. *Computer Networks, 112,* 237 - 262.

[16] R. S. Sandhu & P. Samarati. (1994). Access control: Principle and practice. *Comm. Mag., 32(9),* 40 - 48.

[17] A. Ouaddah, A. A. Elkalam & A. A. Ouahman. (2017). Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. *Cham: Springer International Publishing,* 523 - 533.

정 윤 수(Yoon-Su Jeong) [정회원]



- 2000년 2월 : 충북대학교 전자계산학과 이학석사
- 2008년 2월 : 충북대학교 전자계산학과 이학박사
- 2009년 8월 ~ 2012년 2월 : 한남대학교 산업기술연구소 전임연구원
- 2012년 3월 ~ 현재 : 목원대학교 정보통신융합공학부 조교수
- 관심분야 : 유·무선 통신 보안, 정보보호, 빅 데이터, 헬스케어 서비스
- E-mail : bukmunro@gmail.com