Journal of the Korea Convergence Society
Vol. 9. No. 4, pp. 57-63, 2018

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2018.9.4.057

클라우드 환경에서 서로 다른 IoT 장치간 효율적인 접근제어 기법

정윤수[1], 한군희[2*]
[1]목원대학교 정보통신융합공학부
[2]백석대학교 정보통신공학과

An efficient access control techniques between different IoT devices in a cloud environment

Yoon-Su Jeong[1], Kun-Hee Han[2*]
[1]Dept. of information Communication & Convergence Engineering, Mokwon University
[2]Dept. of Information Communication & Engineeringe, Mokwon University

요 약 IoT 장치는 클라우드 환경에서 다양한 역할과 기능을 수행할 수 있도록 여러 분야에서 사용되고 있다. 그러나, IoT 장치를 안정적으로 제어할 수 있는 접근제어에 대한 방안은 아직 구체적으로 제시되고 있지 않은 상황이다. 본 논문에서는 클라우드 환경에서 사용되고 있는 IoT 장치의 안정적인 접근을 수행할 수 있는 계층적 기반의 다단계 속성 접근제어 기법을 제안한다. 제안 방법은 IoT 장치의 원활한 접근을 돕기 위해서 IoT Hub을 두어 IoT 장치에 고유한 ID 키(보안 토큰)를 제공할 뿐만 아니라 수 있도록 하는 X.509 인증서 및 개인 키를 IoT Hub에서 인증하도록 하여 IoT 장치의 개인키를 IoT 장치 외부에서 알 수 없도록 하였다. 성능평가 결과, 제안방법은 기존 기법보다 인증 정확도가 평균 10.5% 향상되었으며 처리 시간도 14.3% 낮은 결과를 얻었다. IoT 속성 수에 따른 IoT Hub의 오버헤드는 기존 기법보다 9.1% 낮은 결과를 얻었다.

주제어 : 사물인터넷, 접근제어, 보안, 클라우드, 속성 정보, 인증키

Abstract IoT devices are used in many areas to perform various roles and functions in a cloud environment. However, a method of access control that can stably control the IoT device has not been proposed yet. In this paper, we propose a hierarchical multi-level property access control scheme that can perform stable access of IoT devices used in a cluster environment. In order to facilitate the access of the IoT device, the proposed method not only provides the ID key (security token) unique to the IoT device by providing the IoT Hub, but also allows the IoT Hub to authenticate the X.509 certificate and the private key, So that the private key of the IoT device can not be seen outside the IoT device. As a result of the performance evaluation, the proposed method improved the authentication accuracy by 10.5% on average and the processing time by 14.3%. The overhead of IoT Hub according to the number of IoT attributes was 9.1% lower than the conventional method.

Key Words : IoT, Access Control, Security, Cloud, Attribute Information, Authentication Key

1. 서론

최근 4G에서 5G로 이동통신 속도가 향상되는 변화기에서 클라우드 환경에서 동작되는 IoT 장치의 보안요구사항에 대한 필요성이 대두되고 있다. 그러나, IoT 보안과 관련하여 정부의 특별한 대책 마련은 현재까지 마련되어 있지 못하고 있는 것이 현실이다.

기존 IoT 장치와 관련해서는 클라우드 환경에서 IoT

*Corresponding Author : Kun-Hee Han (hankh@buk.ac.kr)
Received February 28, 2018 Revised April 2, 2018
Accepted April 20, 2018 Published April 28, 2018

장치가 권한 없이 서버에 접근하여 불법적으로 민감한 데이터를 수집할 수 없도록 접근 권한을 두고 있다[1-3]. 또한, IoT 장치에 속성 기반의 암호화 (ABE) 방법을 사용하여 서버 접근 정책을 지원하는 방법도 있다. 이 방법은 IoT 장치의 속성 집합과 연동하여 암호문의 비밀 키에 액세스하는 정책을 사용한다.

접근제어는 인증, 권한, 감사 등 3가지 구성요소로 구성된다. 이러한 구성요소들은 시스템을 안전하게 유지할 수 있는 중요한 구성요소이다. 그러나, 권한은 접근 규칙을 강화할 책임이 있기 때문에 특별한 주의가 요구된다. 접근 권한과 관련하여 잘 알려진 전통적인 기법들은 XACML, OAuth, UMA 등이 있다. 그러나. 이 기법들은 IoT 접근제어의 특징(확장성, 의존성등)을 기본적으로 제공하지 못하는 문제점이 있다[4-6].

최근 연구에서는 IoT에 적합한 접근제어를 제공하기 위해서 블록체인(Blockchain)을 적용하는 연구도 있다[7]. 그러나, 블록체인을 사용할 경우 토큰 기반 권한과 자원 소유자만이 접근을 해야만 하는 조건이 있기 때문에 안전성 측면에서 접근 제어 보장이 완벽하지 않은 문제점이 있다. IoT 장치의 확장성 및 협력성 등을 고려한다면 접근제어의 퍼미션(Permission)을 통한 높은 시간 비용(High time cost)과 토큰 만기(token expiration) 그리고 자원에 대한 추가 접근(new access)에 대찬 추가 연구가 필요하다.

본 논문에서는 클라우드 환경에서 IoT 장치의 효율적인 접근을 제어하기 위해서 계층적으로 분산 배치되어 있는 IoT 장치를 n개 그룹으로 구분하여 속성정보를 비트형태로 나타내는 접근제어 기법을 제안한다. 제안 기법은 크게 다음과 같은 2가지 목적을 가진다. 첫째, IoT 장치에 대해 IoT Hub와 통신하는 데 사용할 수 있는 고유한 ID 키(보안 토큰)를 생성한다. 둘째, IoT 장치의 X.509 인증서 및 개인 키를 IoT Hub 장치를 인증하는 수단으로 사용한다. 제안 기법은 분산 배치된 IoT 장치의 부하 및 처리율을 낮추기 위해서 IoT 장치의 속성정보 $PI=\{pi_1, pi_2,...,pi_n\}$ 중 일부에서 k개의 속성값이 선택되도록 $pi_k \in PI(1 \le k \le n)$ 속성 정보를 일정한 규칙에 따라 인터리브하게 순서를 교체 분산 배치하는 것이 특징이다.

이 논문의 구성은 다음과 같다. 2장에서는 접근 제어와 관련된 기존 연구에 대해서 알아본다. 3장에서는 클라우드 환경에서 속성 기반의 접근제어 방법을 제안하고, 4장에서는 제안 기법과 기존 기법과 비교 평가하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

IoT 접근제어와 관련하여 기존 연구된 기법은 FairAccess[7], XACML[8], OAuth[9] 그리고 UMA[10] 등이 있다.

FairAccess 기법은 블록체인을 사용하여 토큰을 분산 제어하는 방법을 사용한다. 그러나, 이 방법은 블록체인이 표준화되어 있지 않아 기존 알고 있는 문제점 이외에 추가적으로 발생할 수 있는 보안 문제점이 존재할 수 있다는 문제점이 있다.

XACML 기법은 속성기반 접근제어 정책 언어를 표준으로 사용하고 있다. 그런, 정책간 애플리케이션을 강화하기 위해서 PEP(Police Enforcement Point)와 PDP (Police Decision Point)를 사용해야 하는 단점이 있다.

OAuth 기법은 토큰 기반의 권한을 부여하는 기법으로써 제3자가 자원 접근을 요청할 경우 자원 소유자가 접근을 허락해준다. 그러나. 이 기법은 자원 소유자의 토큰을 제3가 획득할 경우 자원 소유자의 보든 자원을 접근할 수 있는 단점이 있다.

UMA 기법은 자원 보유자의 속성 단일화하여 자원 이용 권한을 제어한다. 그러나 이 기법은 자원 소유자, 자원 서버, 인증 서버, 클라이언트 간 접근이 토큰을 통해서 제어해야만 하는 단점이 있다.

클라우드 환경에서 서로 다른 그룹내 동작되는 IoT 장치의 인증 연구는 꾸준히 발전되고 있다[11]. IoT 장치 인증을 위해 가장 대표적으로 연구되는 기법은 랜덤 키 사전 분배 방법을 키 설정에 사용한 기법[12], 클러스터 환경을 t 그룹으로 구분하여 공유키를 설정하는 기법[13], 게이트웨이 역할을 수행하는 중간 노드가 인증을 수행하는 기법[14], 공개키와 개인키를 이용한 ID 기반의 암호화 기법[15] 등이 있다.

그러나, 위 기법들은 다음과 같은 문제점을 가지고 있다[16]. 첫째, 랜덤 키 사전 분배 방법은 확률적으로 키를 랜덤하게 분배하여 키를 찾기 때문에 키 검색에 많은 시간이 소비되는 단점을 가지고 있다. 둘째, 클러스터 환경을 t 그룹으로 나누어 공유키를 설정하는 기법은 메모리 낭비로 인하여 통신 비용이 높은 것이 단점이다. 셋째, 게

이트웨이 역할을 수행하는 중간 노드가 인증을 수행하는 기법은 모든 노드가 공유키를 사전에 알고 있어야 하는 문제점이 있다. 넷째, 공개키와 개인키를 이용한 ID 기반의 암호화 기법은 주변 노드로부터 임계 계수만큼 개인키를 획득할 경우 중간자 공격에 취약한 문제점을 가지고 있다.

3. 계층적 속성 기반의 다단계 접근 제어 방법

이 논문에서 제안하고 있는 접근 제어 방법은 계층적 속성을 기반으로 하고 있으며, 사용자와 서버, 사용자와 사용자간 n개 그룹으로 구분하여 접근 제어를 제공하는 방법을 제안한다.

3.1 개요

IoT는 최근 IT업계를 중심으로 뜨거운 관심과 개발 응용부분(휴대폰, 테블릿)까지 다양한 성과를 내고 있다[17-19]. 특히, 주변의 이동기기나 클라우드 기반 정보를 이용한 IoT 장치는 이동 통신 기술 및 빅 데이터 분야에서 각광을 받고 있다. 그러나, IoT 장치는 다양한 환경에서 서로 다른 역할을 수행하는 IoT 장치간 동기화 및 인터페이스를 위한 효율적이고 안전적인 대안이 많지 않은 상황이다[20,21].

제안 기법에서는 이질적인 환경에서 서로 다른 역할을 수행하는 IoT 장치간 효율적인 접근을 수행하기 위해서 IoT 장치를 n개 그룹으로 구분하여 속성값을 n 비트 형태로 나타낸 후 계층적 분산 배치 방법을 사용하여 IoT 장치에 접근할 수 있는 방법을 제안한다. 제안 기법은 효율성과 안전성을 극대화하기 위해서 게이트웨이 역할을 수행하는 IoT Hub를 사용하여 다음과 같은 2가지 목적을 가진다. 첫째, IoT 장치에 대해 IoT Hub와 통신하는 데 사용할 수 있는 고유한 ID 키(보안 토큰) 제공한다. 둘째, IoT 장치의 X.509 인증서 및 개인 키를 IoT Hub에 장치를 인증하는 수단으로 사용 이 인증 방법은 장치의 개인 키를 장치 외부에서 항상 알 수 없도록 하여 더 높은 수준의 보안을 유지한다.

Fig. 1은 제안 기법의 전체 구조를 나타내고 있다. Fig. 1에서 동작되는 IoT 장치는 계층적으로 구성되며 IoT 장치의 속성 정보를 $PI=\{pi_1, pi_2,...,pi_n\}$ 중 k개의 속성이 선택되도록 $pi_k \in PI(1 \le k \le n)$처럼 속성 정보를 선택하도록 설정한다. 이 때, IoT 장치는 k번째 속성정보 pi_k 가 사전에 정의된 속성들로 구성되었는지 확인한 후 IoT 장치 간 인터리브하도록 연결한다. 여기서, 인터리브는 IoT 장치를 관리하는 서버가 IoT 장치의 속성값을 n 비트로 표현할 수 있는 속성 수의 비율을 의미한다.

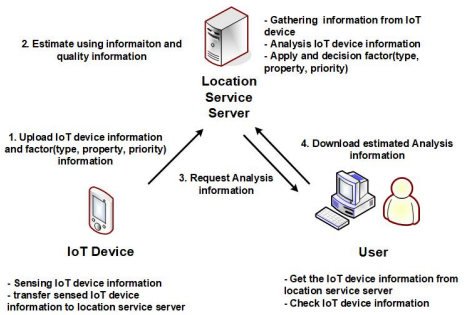

Fig. 1. Architecture overview

3.2 용어 정의

Table 1은 제안 방법에서 사용한 용어를 대한 설명이다.

Table 1. Notation Definition

Notation	Definition
pi_k	Property information
q	The private key selected between [2, n-2]
Q	The public key computed via $q \times P$
SID	Unique identifier
s_i	Bit sequence
h_i	Hash chain
idx	IoT devicer index value
M_i	Important attribute information among attribute information pi_k

3.3 다중 계층에서 사용되는 IoT 장치의 속성 지정

클라우드 환경에서 IoT 장치의 효율적인 서비스를 제공하기 위해서 IoT Hub를 사용하여 IoT 장치의 속성 정보를 ID 키(보안 토큰)를 사용하여 보호함으로써 외부 공격에 안전성을 보장하는 속성 지정 방법을 제안한다.

3.3.1 속성 부여 과정

IoT Hub는 클라우드 환경의 서로 다른 계층에서 동작되는 IoT 장치에 속성 정보를 부여하기 위해서 임의의 비트 수열(0과 1로 구성된 수열)을 n비트 형태로 나타내

기 위해서 식 (1)과 같은 상관관계 행렬을 사용한다.

$$pi_k = \{0,1\}^* \rightarrow \{0,1\}^N = \begin{Bmatrix} 0 & \lambda_{12} & \cdots & \lambda_{1k} \\ \lambda_{21} & 0 & \cdots & \lambda_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{k1} & \lambda_{k2} & \cdots & 0 \end{Bmatrix} \quad (1)$$

식 (1)에서 k는 클라우드 환경에서 계층적으로 서로 다른 역할을 수행하는 IoT 장치의 속성수를 의미하고, λ_{ij}는 속성 정보간 상관 정보를 의미한다.

3.3.2 고유한 ID 키 생성 과정

IoT Hub는 식 (1)에서 생성한 임의의 비트 속성 정보 pi_k를 해쉬체인 h_i으로 생성한 후 식 (2)처럼 무작위로 비트 수열 s_i을 선택한다.

$$\{h_i | s_i,\ i \in N\} \quad (2)$$

IoT Hub는 무작위로 선택된 비트 수열 생성된 해쉬체인 h_i과 IoT 장치의 인덱스 값 idx을 함께 식 (3)처럼 XOR하여 생성된 고유한 ID 키 SID 를 데이터베이스에 저장한다.

$$SID = h_i \oplus idx \quad (3)$$

3.3.3 IoT 속성 정보 접근제어 단계

IoT Hub는 IoT 장치가 가지고 있는 고유한 ID 키 SID가 정상적인지 검증한 후, IoT 장치의 속성 정보 pi_k를 식 (4)처럼 수집한다.

$$Gathering\ pi_k = (pi_1, pi_2, ..., pi_n) = \bigvee_{i=1}^{n} pi_n \quad (4)$$

$$M_l = \{M_l | M_l \in pi_k,\ 1 \le l,\ k \le L\} \quad \text{식 (5)}$$

IoT Hub는 IoT 장치의 속성정보 수집이 완료되면 계층적 구조를 갖는 IoT 장치의 속성정보를 구성하도록 식 (5)처럼 IoT 장치의 속성 정보 pi_k 중 중요 속성 정보 M_l를 추출한다.

여기서 M은 다음과 같이 2가지 가정을 통해 분산된 IoT 장치의 총 개수 L을 갖도록 한다. 첫째, M은 $M_1 \cup M_2 \cup \cdots \cup M_L$이다. 둘째, $\oslash$은 $M_1 \cap M_2 \cap \cdots \cap M_L$ 이다.

3.3.4 IoT 인증 과정

이 과정은 IoT Uub에 접속하는 IoT 장치의 인증을 수행하는 과정이다. 이 과정에서 IoT Hub가 수락하는 IoT 장치 이외에 제3자가 불법적으로 사용하지 못하는 동시에 k개의 속성 $pi_k \in PI(1 \le k \le n)$을 통해 IoT 장치를 인증한다.

- 단계 1 : IoT 장치 인식자 전달

IoT 장치는 IoT Hub에게 공유키 SK(IoT Hub와 IoT 장치가 사전에 공유한 키)를 사용하여 IoT 장치 인식자 ID_U와 공개키/개인키(Q, q)를 암호화하여 IoT Hub에게 전달한다.

- 단계 2 : IoT 장치의 SID 값 생성

IoT Hub는 IoT 장치의 인식자 ID_U를 비교 검증한 후 IoT 장치의 인식자 ID_U가 정상적일 경우, IoT 장치의 속성 값 pi_k과 $\delta = h(ID_U, SK)$를 XOR 연산하여 SID를 생성한다.

- 단계 3 : SID 인증 수행

IoT 장치는 IoT Hub로부터 전달받은 SID 정보 중 $pi_k \oplus \delta$을 추출한 후 IoT 장치의 인식자 ID_U와 공개키/개인키(Q, q)을 사용하여 $\delta = h(ID_U, SK)$을 생성한다. 생성된 δ는 IoT Hub로부터 전달받은 정보와 비교하여 정상적이라면 인증을 수행하고 그렇지 않으면 인증을 종료한다.

4. 평가

4.1 환경설정

제안 기법을 수행하기 위해서 OPNet+ 시뮬레이터를 사용하였으며, Table 2와 같은 환경을 설정하였다.

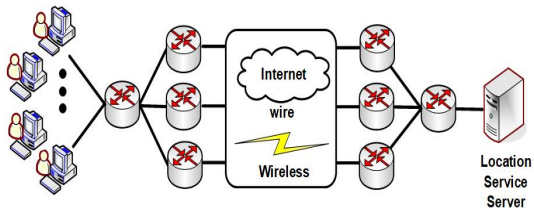

Fig. 2. Topology for experimental environment

Table 2. Simulation parameter

Parameter	Value
Network topology	Mesh topology
Number of server	1
Number of node	1-50
Number of relay nodes	5
Link capacity	1 Gbps
Link round trip delay	10ms
Internet Timeout Timer	500ms
Number of roads	50
Road length	rand(10,50) miles

4.2 접근제어 비교 평가

제안 기법과 기존 기법(XACML, OAuth, Fair Access)과의 접근제어를 호환성(Scalability), 결함 허용(Fault tolerant), 제3자 참여 없음(No third-parties), 새 권한 부여(New authorization), 권한 부여(Get authorization), 정수 관계(Integer relationship), 호환성(Compatibility), 낮은 객체 오버(Low object overhead) 등 8개 항목으로 비교 평가한 결과는 Table 2와 같다.

Table 3의 결과처럼 제안 기법은 기존기법에서 제공되지 않은 항목을 모두 지원하기 때문에 안전성 측면에서 접근제어를 효율적으로 처리할 수 있다. 특히,

제안 기법은 IoT 장치간 사용되는 공유키 SK구하기 위해서 타원 곡선(elliptic curve) 상에 사용자가 선택한 임의의 정수 $q \in [2, n-2]$를 공개키 $Q(=q \times P)$ 생성에 사용하기 때문에 q에 대한 정보를 알지 못하면 공유키 SK를 IoT 장치에 적용할 경우 새로운 권한 설정을 통해 제3자가 IoT 장치 권한에 접근하기가 어렵다. 또한, 타원 곡선 알고리즘을 사용하기 때문에 IoT 장치의 오버헤드 부담이 없어 IoT 장치간 효율적인 통신 및 확산이 가능하다.

4.2 효율성 평가

4.2.1 인증 정확도

Fig. 3은 IoT 장치에 부여된 속성들을 이용하여 사용자의 인증 정확도를 기존 기법들과 비교평가하고 있다. Fig. 3 결과에서, 제안 기법은 IoT 장치 수에 따른 속성정보를 계층적 형태로 단계적으로 속성을 부여함으로써 인증 정확도가 평균 10.5% 향상되었다. 이 같은 결과는 IoT 장치에 부여된 속성정보를 인터리브하게 연결하여 IoT 장치가 인증 서버에 접근하는 방법을 개선하였기 때문에 나타난 결과이다.

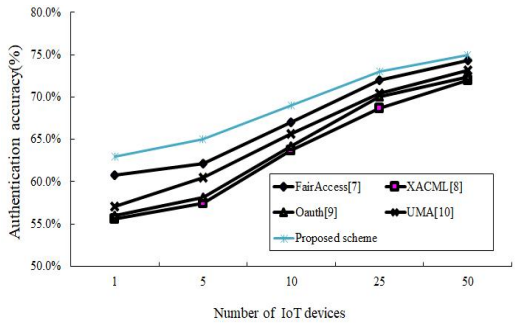

Fig. 3. Authentication accuracy

4.2.2 IoT 장치 인증 처리시간

Fig. 4는 계층적으로 구성되어 인증 서버에 접속하려는 IoT 장치의 인증 지연 시간을 기존기법과 비교평가하고 있다. Fig. 4의 결과처럼, 제안 기법은 IoT의 속성을 IoT 장치가 수행하는 역할에 따라 부여함으로써 IoT 장치 인증 지연시간을 평균 14.3% 향상시켰다. 이 같은 결과는 제안 기법이 IoT 장치에 부여된 속성 값에 해쉬 함수와 확률값을 토대로 IoT 장치 인증 정보를 함께 연계처리하였기 때문에 나타난 결과이다.

Table 3. Compare of Access Control Scheme

	FairAccess[7]	XACML[8]	OAuth[9]	UMA[10]	Proposed scheme
Scalability	+	−	−	−	+
Fault tolerant	△	−	−	−	+
No thrid-parties	+	−	−	−	+
New authorization	−	+	+	+	+
Get authorization	−(*)	+	+	+	+
Integer relationship	−	−	−	−	+
Compatibility	−	+	−	−	+
Low object overhead	+	+	+	+	+

(*) Exclusively dependent of the type of proof and dissemination speed of blocks

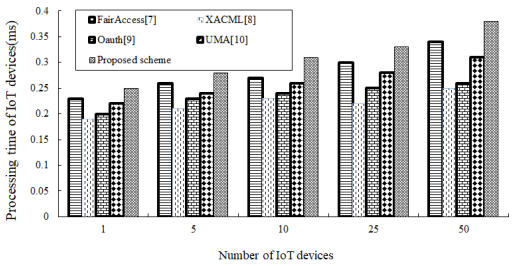

Fig. 4. Processing Time of IoT Devices

4.2.3 IoT Hub의 오버헤드

Fig. 5는 IoT 증가 수에 따른 IoT Hub의 오버헤드를 기존 기법과 비교평가하고 있다. Fig 5의 결과처럼, 제안 기법은 IoT Hub 에 IoT 장치의 속성 수를 증가하여 인증을 처리할 경우 IoT Hub의 오버헤드가 기존 기법보다 평균 9.1% 낮은 결과를 얻었다. 이 같은 결과는 제안 기법이 인증 수행을 위해 토근을 사용하지 않고 고유한 ID 키 *SID*와 공유키 *SK*만을 사용하였기 때문에 나타난 결과이다.

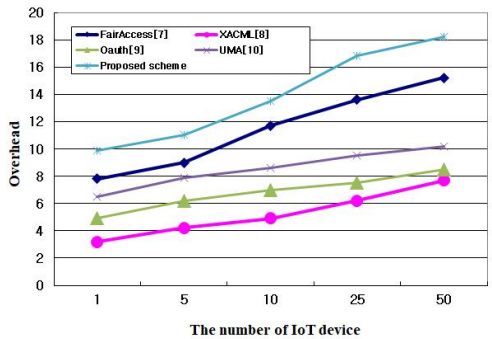

Fig. 5. Overhead of IoT Hub

5. 결론

클라우드 환경에서 서로 다른 종류의 IoT 장치간 효율적인 접근제어에 대한 연구가 최근 사회적으로 대두되고 있다. 본 논문에서는 클라우드 환경에서 제3자가 IoT 장치를 불접적으로 접근하여 악의적인 행동을 예방하기 위해서 계층적 기반의 다단계 속성 접근제어 기법을 제안하였다. 제안 방법은 n 비트의 IoT 장치 속성을 일정한 규칙에 따라 속성 값들을 계층적으로 분산 배치하여 IoT 장치의 효율성을 향상시켰다. 또한, 제안 기법은 IoT Hub을 중심으로 IoT 장치에 고유한 ID 키(보안 토큰)를 제공하여 X.509 인증서 및 개인키를 IoT Hub에서 인증하도록 하였다. 성능평가 결과, 제안방법은 기존 기법보다 인증 정확도가 평균 10.5% 향상되었으며 처리 시간도 14.3% 낮은 결과를 얻었다. IoT 속성 수에 따른 IoT Hub의 오버헤드는 기존 기법보다 9.1% 낮은 결과를 얻었다. 향후 연구에서는 본 연구의 결과를 기반으로 IoT 장치간 성능 향상을 위한 인터페이스 설계를 구현할 계획이다.

REFERENCES

[1] R. Neisse, I. N. Fovino, G. Baldini, V. Stavroulaki, P. Vlacheas & R. Giaffreda. (2014). A model-based security toolkit for the internet of things. *Proceedings of the 2014 Ninth International Conference on Availability, Reliability and Security*, 78 - 87.

[2] J. Park & R. Sandhu. (2004). The uconabc usage control model. *ACM Trans. Inf. Syst. Secur., 7(1),* 128 - 174.

[3] 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, Proceedings of the Information Theory and Aerospace Electronic Systems (VITAE),* 1 - 5.

[4] 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.

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

[6] O. J. A. Pinno, A. R. A. Gregio & L. C. E. De Bona. (2017). ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. *Proceedings of the 2017 IEEE Global Communications Conference,* 1-6.

[7] 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.

[8] A. A. A. El-Aziz & A. Kannan. (2013). A comprehensive presentation to xacml. *Proceedings of the Third International Conference on Computational Intelligence and Information Technology (CIIT 2013),* 155 - 161.

[9] D. Hardt. (2012). The oauth 2.0 authorization framework, Internet Requests for Comments. *RFC Editor*, RFC

6749.

[10] Kantara Initiative, Inc.. (2017). User-managed access (uma). https://kantarainitiative.org/confluence/display/uma/Home.

[11] L. Eschenauer & V. D. Gligor. (2012). A key-management scheme for distributed sensor networks. *Proceedings of the 9th ACM conference on Computer and communications security,* 41 - 47.

[12] L. Echenauer & V. D. Gligor. (2002). A Key-Management scheme for Distributed sensor networks. *Proceedings of the 9th ACM conference on Computer and communications security,* 41-47.

[13] H. Chan, A. Perrig & D. Song. (2003). Random key predistribution schemes for Sensor networks. *Proceedings of the 2003 IEEE Symposium on Security and Privacy,* 197-213.

[14] S. Zhu, S. Setia & S. Jajodia. (2002). *A distributed group key managemet protocol for ad hoc networks.* Doctoral dissertation., George Mason University, USA.

[15] A. Khalili, J. Katz & W. A. Arbaugh. (2003). Toward Secure key Distribution in Truly Ad-Hoc Networks. *Proceedings of the 2003 Symposium on Applications and the Internet Workshops(SAINT'03 Workshops),* 342-346.

[16] S. Haller, S. Karnouskos & C. Schroth. (2009). The Internet of Things in an Enterprise Context. *Future Internet - FIS 2008 Lecture Notes in Computer Science, 5468,* 14-28.

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

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

[19] Y. S. Jeong, Y. T. Kim & G. C. Park. (2017). A hierarchical property-based multi-level approach method for improves user access control in a cloud environment. *Journal of the Korea Convergence Society, 8(11),* 7-13.

[20] Y. S. Jeong. (2017). User Authentication Key Establishment Scheme based on Color Model for Healthcare Environment. *Journal of the Korea Convergence Society. 8(3),* 115-121.

[21] Y. S. Jeong. (2016). A Study of An Efficient Clustering Processing Scheme of Patient Disease Information for Cloud Computing Environment. *Journal of Convergence for Information Technology, 6(1),* 33-38.

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

한 군 희(Kun Hee Han) [정회원]

- 2000년 2월 : 충북대학교 컴퓨터공학과(공학박사)
- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 멀티미디어, 정보보호
- E-Mail : hankh@buk.ac.kr