# IOT 체계의 계정 및 권한관리 방법에 대한 연구

김민휘* · 김영길**

*(유)한국아이비엠테크니컬솔루션 · **아주대학교

# A Study on account and authority management method of IOT system

Min-Hwi Kim* · Young-kil Kim**

*IBM KOREA Technical Solution Co., Ltd. · **Ajou University

E-mail : sjmhkim@kr.ibm.com, ykkim@ajou.ac.kr

## 요 약

본 논문은 IOT 체계에서 우리 실생활에 밀접하게 관련되어 있는 전자기기,헬스케어,스마트카,스마트홈,원격검침,원격진료 같은 실효성이 있는 시스템 사용이 증가함에 따라, 점차적으로 IOT 체계시스템을 다루기 위해서는 사용자가 어느 시점에 얼마의 기간 동안 어떠한 용도로 시스템에 접근하여 사용했는지에 대한 확인 및 관리 필요에 수요가 증가함에 따라 이러한 문제를 해결 할 수 있는 방법인 IOT 통합계정솔루션이 필요하다. 각 사물인터넷에 endpoint 시스템에 대한 통신 알고리즘, IOT 시스템 관리권한정책, 사용자 정보 등을 구성하며, IOT시스템 스마트카, 스마트홈에 어떻게 적용할 것인지를 제안한다.

## ABSTRACT

In this paper, we propose a methodology to deal with the IOT system gradually as the use of effective systems such as electronic devices, healthcare, smart cars, smart home, remote meter reading and telemedicine closely related to our real life in the IOT system An IOT integrated account solution is needed as a way to address these needs as the demand grows for the need to identify and manage how users access and use the system for what period of time and at what point in time. We propose the communication algorithms for endpoint system, IOT system management rights policy, user information, and how to apply them to IOT system smart car and smart home on each object internet.

사물인터넷, 계정관리, 스마트카, 스마트홈

Internet of things, Identify management, smart car, smart home

## Ⅰ. 서 론

클라우딩컴퓨팅 서비스가 상용화되어 이에 따라 다양한 사업자들이 저비용으로도 고효율의 인프라를 구축하여 endpoint 단에 사물인터넷장치 서비스를 개발하여 서비스 하고 있다. 다양한 사용자에게 서비스를 제공함에 따라 IOT장치는 차세대 IT서비스로 주목받고 있다.

IOT장치는 엘리베이터와 같은 공용사용자가 존재하는 물체에 대해서도 서비스하고 있으며, 특히 사용자에 맞는 권한을 부여하는 것이 중요하다. 특권권한을 필요로 하지 않는 사용자에게 너무 많은 권한이 부여되어 사고발생 시 책임소재 규명이 어렵다는 점에서 미리 알맞은 권한을 부여할 수 있는 보안관리 서비스 제공이 필요하다. 이와 관련하여 ISO27001 사용자별, 그룹별 별도의 계정권한을 적용해야하며, 안전한 패스워드를 사용하는지에 따른 정합성과 시스템 접속에 따른 관련 연결시간에 관해 정의하고 있다. 2장 본론 가에서는 계정관리시스템 설계와 실제로 IOT장치에 구현에 대해서 정의한다. 2장 본론 나에서는 ISO27001 관련 계정에 대한 기본권한 특권권한 공유권한에 대해 정의한다. 2장 본론 다 에서는 IOT장치와 클라우딩컴퓨팅기반의 인프라 위에서 응용 될 수 있는 계정관리시스템간에 통신프로토콜에 대해 설계한다. 2장 본론 라에서는 IOT체계에서의 사용자 정보 관리방안에 대해서 보안통제를 정의한다. 2장 본론 마에서는 IOT장치 계정관

리시스템을 적용할 수 있는 환경과 적용하여 응용 할 수 있는 범위에 대해서 제안한다. 3장은 결론을 맺는다.

## II. 본 론

### 가. 계정관리시스템 설계 및 구현

클라우딩컴퓨팅 기반에 IOT체계시스템과 Legacy 시스템에 대한 계정관리시스템설계를 위해서는 Application Programming Interface기반에 다양한 서비스프로파일 구현이 필요하다. 사용자 편의를 위해 Single-Sign on 인증방식을 통하여 사용자가 웹페이지에 로그인하고 사용자에 맞는 권한을 Identity Access Management방식을 통하여 얻게 된다. SSO인증방식과 IAM계정권한정책관리를 관리할 수 있는 IOT Security Identity Management솔루션을 설계하여 모든 사용자의 정보를 제어하며 Endpoint단에 모든 시스템들을 관리할 수 있으며 인증절차를 자동화하여 보안적 측면에서 내부통제 강화와 효율적인 통제의 계정관리를 가능하도록 구현할 수 있다.

### 나. 계정에 대한 권한정책

시스템에 접근하기 위해서는 사용자에게 맞는 권한을 부여하는 시스템이 필요하다. [1]IAM방식을 이용하여 SSO방식으로 인증받은 사용자에 한하여 표1과 같이 선정한 권한을 부여한다. 일반사용자일 경우 Users그룹, 특권사용자일 경우 Super Users그룹, 공유사용자일 경우 Shared Users 그룹으로 나뉜다. 공유사용자는 IOT체계에서 공유해서 사용하는 스마트 자동차에 대한 권한정책이다. 여러 사용자가 임대하여 사용할 수 있도록 공유사용자 그룹에 사용자들을 지정하여 A라는 사용자가 사용할 경우 A라는 사용자에 대한 CICO(Check-In Check-Out) 개념을 통해 언제 시스템을 사용할 수 있게 Check-In하였고, 다른사용자 B가 이용하기 위해서는 A라는 사용자가 Check-Out 하기 전 까지는 B사용자가 시스템에 접근할 수 없다. 사용한 뒤에 Check-Out했는지에 대한 정보를 시스템에 저장함으로써 공유하는 IOT시스템에 대한 접근통제가 가능하다.

| 구분 | 그룹 | 비고 |
|---|---|---|
| 일반사용자 | Users | |
| 특권사용자 | Super Users | |
| 공유사용자 | Shared Users | |

표 1. 계정인증사용자 권한정책 그룹

[2] 클라우딩컴퓨팅 계정관리정책에 요구되는 요소는 표 2와 같다. 접근통제에 대한 절차와 원격접근 방식으로 사용자가 접속하여 접근권한을 어떻게 배정할 것인지에 대한 올바르고 최소한의 권한부여가 필요하다. 또한 패스워드를 여러 번 시도하여 지속적으로 틀렸을 경우 계정을 불용처리 할 수 있게 처리해야하며 한 사용자가 세션을 여러 개를 갖지 않게 세션을 통제하거나 세션을 Lock하는 기능이 필요하다. 또한 휴대용 모바일 장치 중 인가되지 않는 장치에서는 로그인 할 수 없도록 하는 접근통제로 등록된 장치만 사용할 수 있도록 함으로써 안정성을 보장한다. 또한 사용자가 로그인에 성공할 경우 접근 가능한 콘텐츠만 부여할 수 있도록 하는 기능이 있다.

| 요구사항 번호 | 구분 |
|---|---|
| CS-AC-1 | 접근통제 정책 및 절차(Control Policy and Procedures) |
| CS-AC-2 | 원격접근 정책과 절차(Remote Access Poliy and Procedures) |
| CS-AC-3 | 계정관리(Account Management) |
| CS-AC-4 | 접근권한 배정(Access Enforcement) |
| CS-AC-5 | 정보 흐름 권한 배정(Information Flow Enforcement) |
| CS-AC-6 | 권한분리(Separation of Duties) |
| CS-AC-7 | 최소권한(Least Privilege) |
| CS-AC-8 | 잘못된 로그인 시도(Unsuccessful Login Atternpts) |
| CS-AC-9 | 사전로그인 통지(Previous Logon Notification) |
| CS-AC-10 | 세션 공존 통제(Concurrent Session Control) |
| CS-AC-11 | 세션잠금(Session Lock) |
| CS-AC-12 | 원격 세션 종료(Remote Session Termination) |
| CS-AC-13 | 인증 및 권한 없이 허가된 행동(Permitted Action without Identification or Authentication) |
| CS-AC-14 | 원격 통제(remote Access) |
| CS-AC-15 | 무선 접속 제한Wireless Access Restrictions) |
| CS-AC-16 | 휴대용 모바일 장치에 대한 접근 통제(Access Control for Portable and Mobile Devies) |
| CS-AC-17 | 외부 정보통제시스템 사용(Use of Extrnal Information Control Systems) |
| CS-AC-18 | 접속제한 통제 시스템(Control System Access Restrictions) |
| CS-AC-19 | 접근 가능 공개 콘텐즈(publicly Accessible Content) |
| CS-AC-20 | 패스워드 설정(Password) |
| * CS: Cloud Compution Servce, AC: Access Control | |

표 2. 클라우딩컴퓨팅 서비스 계정관리정책

### 다. IOT(endpoint)와 서비스(Server)간의 통신 프로토콜

IOT체계시스템들은 스마트자동차, 드론, 스마트빌딩내의 엘리베이터와 같은 유동적인 사물에 적용된다. 계정인증관리 절차를 위해서 사용자가 실시간으로 인증하고 처리할 수 있는 IOT 통신프로토콜을 이용해야한다. IOT 보안통신규격인 대표적인 oneM2M방식을 이용하여 단말 시스템과 서비스간에 메시지를 주고받아 처리한다. [3]그림1과 같이 oneM2M방식에서 구성도 모듈은 크게 CSE와 ADN-AE 모듈로 나눌 수 있다. CSE모듈에는 Network Manager,Message handler, Resource Manager 모듈 로 구성되며 각각의 역할은 통신의 전체 운영을 관장하는 Network Manager 모듈, 단말시스템의 oneM2M메시지와 서비스(Server) HTTP메시지 간의 내용을 취합

하여 분석하는 Message Handler 모듈, 모든 통신정책을 가지고 있는 Resource Manager 모듈로 구성되어 있다.

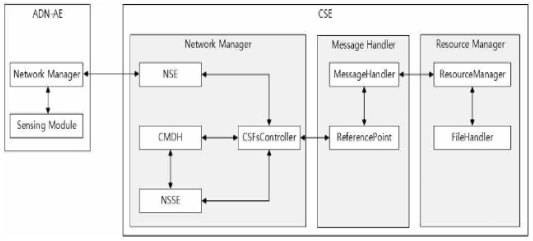


그림 2. IOT 통신프로토콜 구성도

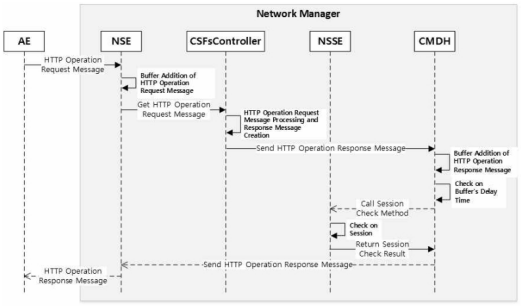


그림 3 Network Manager모듈 flow chart

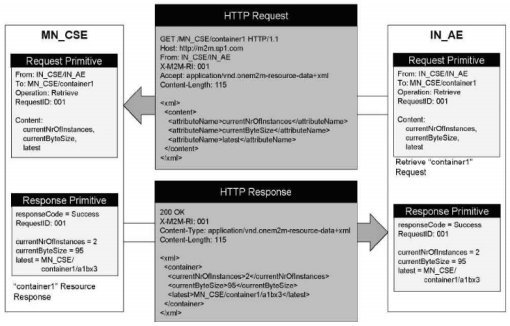


그림 4 Message Handler 모듈 flow chart

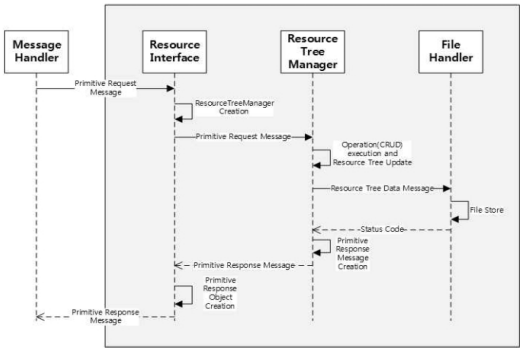


그림 5 Resource Manager모듈 flow chart

**라. 사용자 Human Resource 관리방안**

계정관리에서 가장 중요한 부분은 사용자의 존재 유/무 이다. [4] 그림 5와 같이 서비스를 이용하는 사용자가 탈퇴할 경우 외부에 있는 인사 Database서버의 정보를 실시간으로 Mirroring하여 가져와 존재하지 않을 경우 block처리하여 사용자의 모든계정을 불용처리후에 KISA ISMS (주요정보통신기반시설 보호대책)기관에서 권고하는 3일(72시간) 안에 삭제하는 구성이 필요하며 시스템과 시스템 간에 정보가 일치하는지에 대한 Reconcilication 방안이 필요하다. IOT Security Identity Management 솔루션일 경우 모든 서비스들에 대하여 인사DB를 통해 사용자들을 관리하며 서비스프로파일을 실시간으로 동기화함으로 계정관리가 가능하도록 설계한다.

| 구분 | 분류 | 설명 |
|---|---|---|
| 사용자 계정의 일반적 프로비저닝 | BR-300.1 | - 제안 시스템이 사용자와 목표 계정 도메인과 어떻게 인터페이스(사용자 생성, 수정, 잠금, 제거)하는지 방안 제시<br>- 사용자 관리 및 프로비저닝 절차에 대한 예시 제시<br>- 사용자 관리 및 프로비저닝 절차를 수정하는 방안 제시<br>* ISO27001 A.11.2.1. 사용자 등록<br>* 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2009.1.28) 제15조 2항 1. 개인정보처리시스템에 대한 접근 권한 부여, 변경, 말소 등에 관한 기준 수립 및 시행 |
| | BR-300.2 | 제안 시스템과 연결된 계정 도메인에서 사용자 특권을 포함하는 권한 정보를 실제 시스템과 제안 시스템 간에 일치(Reconciliation)시키는 방안 제시 |
| | BR-300.3 | - 제안 시스템의 패스워드 정책 기능 제시<br>- 프로비저닝 절차 중에 모든 목표 연결 시스템에 대해 패스워드 정책을 적용하는 방안 제시<br>* KISA ISMS 10.2.3. 사용자 패스워드 관리 |
| | BR-300.4 | 제안 시스템이 자동적으로 비소유(고아) 계정 탐지 및 이에 대한 관리 방안 제시<br>* KISA ISMS 10.2.4. 사용자의 접근 권한 검토 |
| | BR-300.5 | 계정 및 권한 신청 간 사용자 역할이나 직무에 따른 신청 가능한 계정 및 선택 가능한 권한 식별 및 표시 여부<br>* KISA ISMS 10.2.2. 특수 권한 관리<br>* ISO27001 A.11.2.2. 특권 관리 |
| | BR-300.6 | 인사 정보(예. HR 시스템 혹은 관련 정보를 담은 데이터베이스, 파일 등)를 기반으로 직무나 조직 변경 시, 자동화된 계정 및 권한 관리 방안 제시<br>* KISA ISMS 10.2.4. 사용자의 접근 권한 검토 |
| | BR-300.7 | 사용자 계정 및 권한에 주기적 검토를 통해 재승인 프로세스가 지원되어야 한다.<br>* KISA ISMS 10.2.4. 사용자의 접근 권한 검토<br>* ISO27001 A.11.2.4. 사용자 접근 권한 검토<br>* PCI DSS 8.5.4. 기간 만료 사용자에 대한 접근 권한 삭제 |

표 2. ISO 27001, KISA ISMS인증심사 기관에서 제시한 사용자 Human Resourse 관리 권한검토 표

**마. IOT 계정관리시스템 적용가능 범위**

중앙계정관리를 위해서 실시간으로 유동적인 물체에 대한 통신프로토콜 OneM2M을 이용하여 모든 IOT 객체에 대한 통신모듈을 이용한 관리가 가능하기 위해서는 더욱더 개선된 모듈이 필요하다. [5] 특히 치명적인영역에서는 더더욱 성능이 개선된 통신모듈이 필요하다. 또한 앞으로 사물인터넷과 관련된 기기들의 수가 2017년에서 2020

년 까지 연 평균 22%의 증가율을 보이고 있다. 스마트폰을 포함한다면 최대 500억 개의 기기가 보급될 것으로 보인다. 이러한 많은 사용자들에 대한 계정들을 관리하기 위해서는 보안적인 측면에서 계정관리에 대한 적용가능 범위는 증가 할 것으로 보인다. 사용자가 공유해서 사용하는 쉐어링카 서비스가 국내 뿐만 아니라 국외에서 우버 테크놀로지스에서는 승객에 대한 계정정보관리하며 전세계적으로 교통운수사업에 뛰어들고 있다. 또한 스마트빌딩에서 사용되는 엘리베이터를 이용하기 위해서는 사용자에게 부여되는 권한만을 이용해 해당 층을 사용할 수 있도록 통제 할 수 있는 Check-In Check-Out 서비스 또한 적용가능하다. 스마트폰, 스마트카, 스마트 빌딩 모든 전자기기통신을 이용한 M2M서비스에는 IOT Security Identity Management 솔루션을 제안할 수 있다.

## III. 결 론

이 논문에서는 클라우딩컴퓨팅 서비스를 이용한 ISIM(IOT Security Identity Solution)을 설계하여 그동안 대기업에서만 도입된 계정관리솔루션을 영세기업 뿐만 아니라 모든 사용자들도 쉽게 임대하여 사용할 수 있다. 현재 일부 IT보안 업무가 기술적으로 영세한 기업의 경우 사용자에 대한 개인정보 유출사건이 빈번하게 발생되고 있다.

그러나 본 논문에서의 ISIM 솔루션을 통해 개개인의 사업장에 계정관리솔루션을 도입할 필요 없이, 클라우딩서비스를 이용하여 각 사업자가 사업장에 필요한 스마트카 쉐어링 서비스, 운송업, 스마트 모빌리티 사업에 필요한 IOT를 이용한 사용자에 대한 정보를 안정적으로 구현할 수 있음을 재확인 하는 계기가 되었다.

## 참고문헌

[1] NIST, Guide for Assessing the Security Controls in Federal Information Systems, NIST Special Publication 800-53A, 2006

[2] 보안공학연구논문지(Journal of Security Engineering). 제 10권 제 3호 2013년 6월

[3] Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and SociologyVol.6, No.3, March(2016)41-49http://dx.doi.org/10.14257/AJMAHS.2016.03.14

[4] KISA(한국정보보호진흥원), 정보보호 관리체계 인증규격, 2002

[5]D. H. Shin, J. Y. Jeong and S. H. Kang, Korean Society for Internet Information. (2013), Vol.14, No.2, pp.32-46.