한국컴퓨터정보학회 동계학술대회 논문집 제25권 제1호 (2017. 1)

사물인터넷 플랫폼에서 권한 인증 모델

이세훈*, 문효재*, 이상민O, 고희창**
O*인하공업전문대학 컴퓨터시스템과,
**인하대학교
e-mail : seihoon@inhatc.ac.kr*, molybdan@icloud.com*, tricky094@gmail.comO, heechang.koh@inha.ac.kr**

Permission Authentication Model on IoT Platforms

Se-Hoon Lee*, Hyo-Jae Moon*, Sang-Min LeeO, Hee-Chang Koh**
O*Dept. of Computer Systems & Engineering, Inha Technical College
**Inha Unviersity

● 요 약 ●

현재 사물인터넷 시장이 커져감에 따라 사물인터넷 보안위협도 증가하고 있다. 시중의 가정이나, 회사 등에서 사용하는 사물인터넷 플랫폼은 사용자 개개인에 대해 각 장치의 제어권한을 설정할 수 없다. 이로 인해 보안사고, 자원낭비 등 여러 문제가 발생할 가능성이 높다. 본 논문에서는 관리자가 사용자 개개인에게 각 장치의 제어 권한을 설정하고, 인증을 거친 사용자가 장치를 쉽게 제어할 수 있는 사물인터넷 플랫폼에서 활용할 수 있는 권한 인증 모델을 제시한다.

키워드: 사물인터넷(IoT), 권한 설정(Permission Setting), 인증(Authentication)

I. Introduction

사물인터넷이라는 개념이 등장하면서 가정에 있는 조명이나 보일러와 같은 장치를 모바일로 제어하는 사용자가 많아지기 시작했다. 앞으로는 가정뿐만이 아니라 회사나 학교에서도 원격으로 장치를 제어하려는 사용자가 많아질 것이다[1]. 많은 구성원 간 장치 제어의 범위가 제한되지 않는다면 무질서한 사용으로 인한 자원낭비 혹은 보안문제를 초래할 수 있을 것이다. 이런 문제들을 해결하기 위해, 본 논문에서는 관리자가 각 구성원의 권한을 할당하고 인증하는 사물인터넷 플랫폼을 설계, 구현함으로서, 이러한 문제를 예방할 수 있도록 한다[2].

II. Permission Authentication

권한 인증은 크게 4가지로 구분하여 부여한다.

(1) 각 구성원에게 특정 장치를 제어할 권한 부여

구성원마다 제어할 수 있는 장치를 다르게 지정하는 방식으로 최고 관리자가 구성원의 장치 제어 권한을 추가하거나 삭제한다. 이를 테면 학교의 시설을 관리하는 관리자가 선생A에게는 교실1의

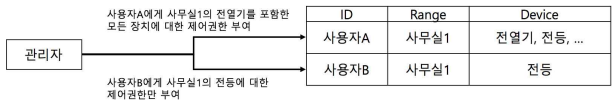

Fig. 1. Setting the Permission Each Member to Control the Specific Device

전열기를 포함한 모든 장치를 제어할 수 있는 권한을, 학생B에게는 교실1의 조명만 제어할 권한을 부여하는 방식이다. 관리자가 각 사용자에게 부여한 권한에 따라 제어 범위가 다른 것이다.

(2) 그룹별로 장치 제어 권한 부여

권한이 유사한 사용자를 그룹으로 묶고, 그룹별로 권한을 설정하여 관리자가 효율적으로 권한을 할당하는 방식이다.

Fig. 2. Setting Permissions to a Specified Group

(3) 일시적으로 장치 제어 권한 부여

관리자가 구성원에게 일시적으로 제어 권한을 부여하는 방식으로 크게 2가지가 있다.

관리자가 일정 기간에만 집단에 소속되는 사용자에게 기간을 설정하여 사용자에게 장치 제어의 권한을 부여하면 그 기간 동안만 장치를 제어를 할 수 있도록 하는 방식과, 관리자가 토큰을 발행하여, 이 토큰을 Guest가 받아 ID없이도 Guest에게 장치제어 권한을 부여하는 방식이 있다[3].

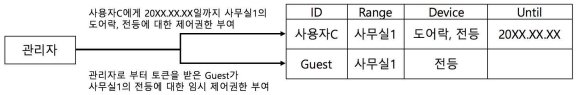

Fig. 3. Setting Device Control Permissions for a While

(4) 서버 접근 IP 주소 기반 제어 권한 부여

장치를 제어할 때 사용자가 접속한 IP 주소가 제어할 장치의 내부 IP주소가 아닐 경우 제어 권한을 설정하지 않는다. 쉽게 말해 회사 IP에서 접속하지 않은 사용자가 장치를 제어할 경우 권한을 제한해 불필요하게 작동하는 것을 막는 방식이다.

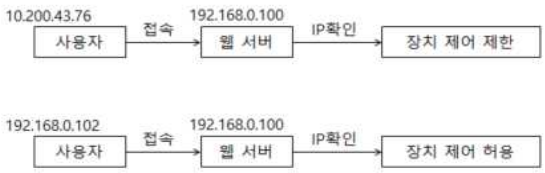

Fig. 4. Setting Device Control Permission based on Access IP Address

III. Design and Implementation

Fig.5는 권한 인증기반 사물인터넷 시스템의 전반적인 시스템 구조도이다. 이 시스템은 프로세싱과 UI를 담당하는 웹서버, 장치들에 대한 사용자 권한 정보를 저장하는 권한DB, IoT장치들과 이 장치를 인터넷과 연결할 IoT공유기로 구성되어있다.

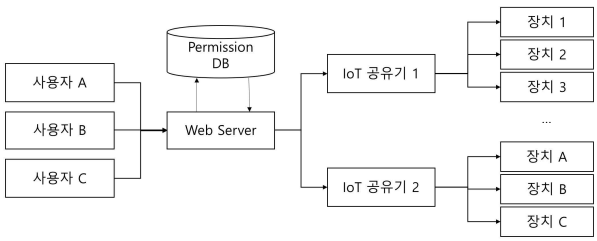

Fig. 5. System Architecture

Fig.6는 시스템의 전체 흐름도이다.

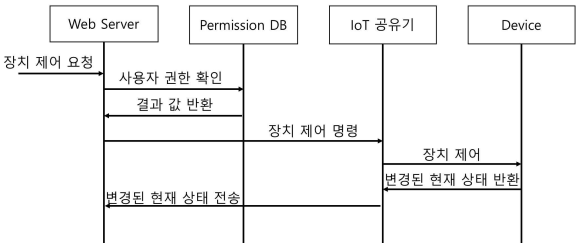

Fig. 6. Sequence Diagram

사용자가 웹에 접속하면 서버는 해당 사용자의 권한정보를 토대로 제어 가능한 장치를 화면에 출력한다. 사용자가 장치 제어 버튼을 클릭하면 웹 서버는 사용자가 해당 장치에 대한 권한을 검증한다. 인증된 사용자인 경우 웹 서버는 암호화된 소켓을 통해 선택된 장치를 사용자가 설정한 상태를 변경한 후, 결과를 웹 서버로 반환한다. 그 후 변경된 상태를 갱신하여 사용자에게 전달한다.

IV. Conclusions

본 논문에서 사물인터넷 플랫폼에 4가지의 권한 부여라는 방식을 추가해 그룹에서 컨트롤 할 수 있게 제시하였다. 이를 통해 각 구성원에게 IoT가 가지는 편의성을 제공하면서 동시에 권한의 차이로 인한 효율적인 장치 관리를 할 수 있게 하였다.

References

[1] Thingplus. "Introduction of Thingplus Platform" https://thingplus.net/platform/

[2] J.Y.Lee. "Development of the Web-based Participation IoT Service Brokering Platform", Master. Dissertation. Hanbat University, Daejeon, 2015

[3] B.K. Lee. "Design and Implementation of CL using a token based access control system in the Internet of Things environment". Master. Dissertation, Mokpo University, Mokpo, 2015