한국컴퓨터정보학회 동계학술대회 논문집 제25권 제1호 (2017. 1)

사물 인터넷을 위한 OAuth 기반 권한부여 기법에 대한 연구

강용혁O
O극동대학교 글로벌경영학과
e-mail:yhkang@kdu.ac.krO

Study of OAuth-based Authorization Mechanism for Internet of Things

Yong-Hyeog KangO
ODept. of Global Business Administration, Far East University

● 요 약 ●

IoT(Internet of Things)는 우리 일상생활에 깊숙이 관여하고 있어서 보안 문제는 중요해지고 있다. OAuth2.0은 웹기반 응용이나 REST 특성의 API를 안전하게 하는 권한부여(authorization) 프레임워크이다. 본 논문에서는 IoT에 OAuth2.0을 적용하여 효율적이고 효과적인 권한부여 기법을 제안한다. OAuth2.0 기술은 서버쪽 기술이지만, IoT에서도 웹을 이용할 수 있는 CoAP 기술이 있으므로 IoT 디바이스 쪽에 접근에 대한 권한부여 기법으로 적용할 수 있다. 제안기법은 권한 부여 서버와 자원 서버와의 키 분배와 해시 함수 및 암호화를 통해 권한부여 기법을 적용한다.

키워드: OAuth2.0, 사물인터넷(IoT), 권한부여(Authorization)

I. Introduction

IoT는 인터넷과 같은 구조로 수많은 자원 제약적인 디바이스들의 연결이다. IETF에서는 REST 특성의 제약적인 환경을 위해 M2M 응용을 위해 HTTP를 대신하는 프로토콜로 CoAP를 일반적인 웹 프로토콜로 정의하여 기존 웹과의 통합을 고려하였다[1].

OAuth2.0은 클라이언트로 하여금 서비스 상에서 보호된 자원에 대한 자원소유자를 대신하여 인가되 요청을 만들 수 있는 권한부여(Authorization)을 제공한다[2]. OAuth2.0의 장점은 API Security를 제공한다는 점이며[2], 통합 응용을 제공할 수 있으며, 서비스 통합과 권한부여 위임도 가능하며 연합 신분을 사용하여 여러 개의 다른 서비스를 이용할 수 있으며, 서비스 모니터링이 쉬어진다.

IoT에 OAuth2.0을 적용하려면 IoT 디바이스에서 서버로 접근하는 권한부여보다는 IoT 디바이스에 대한 권한부여를 고려해야 한다. 그러려면 IoT 디바이스에 WoT기술이나 CoAP 기술이 적용되어야 한다. 본 논문에서는 IoT 환경에 OAuth2.0을 적용하여 효율적이고 효과적인 권한 부여 프레임워크를 제안한다. 2장에서는 OAuth2.0에 대한 소개를 하며, 3장에서는 본 논문의 제안기법을 제시하고, 4장에서는 결론과 향후 연구 과제를 설명한다.

II. Preliminaries

OAuth2.0의 기본 구성요소는 클라이언트, 자원 소유자, 자원서버, 권한부여 서버이다. OAuthu2.0 부여 흐름도(grant flow)에는 네 가지 유형이 있지만, 가장 많이 쓰이는 흐름도는 권한부여 코드(Authorization code) 부여 흐름도로 웹서버 응용에 사용되며 흐름도는 다음 그림과 같다.

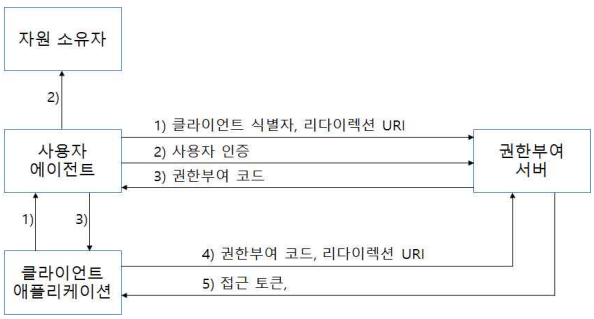

Fig. 1. Authorization Code Grant Flow

클라이언트가 보호된 자원에 접근하기 위해서 가장 먼저 해야 할 일은 접근토큰(access token)을 얻어야 한다. 이 토큰은 권한부여증명서로 사용되어 자원접근 시에 접근제어에 사용된다.

III. The Proposed Scheme

IoT 환경을 위한 OAuth2.0을 적용하기 위해서는 자원 서버, 자원 소유자, 권한부여 서버, 클라이언트를 정의해야 한다. 하지만, 그전에 자원에 대한 정의부터 해야 한다. 자원은 데이터일수도 있고 API일 수도 있다. 자원이 데이터인 경우에도 데이터를 읽거나 쓰는 API로 매핑할 경우 자원은 IoT 디바이스의 API로 정의할 수 있다. 따라서 요청은 API를 호출하는 것이고 OAuth2.0은 이러한 API에 대한 권한부여를 위한 프레임워크이다.

자원 소유자는 IoT 디바이스의 소유자로 볼수 있으며, 자원 서버는 웹을 지원하는 IoT 디바이스가 된다. 마지막으로 권한부여 서버는 무엇으로 할지를 정해야 한다. 권한부여 서버의 위치와 인증하는 방법과 권한부여 방법을 정해야 한다. 권한부여 서버는 자원서버에 위치할 수 있으며, 다른 서버에 위치할 수도 있다[2]. 또한, 하나의 권한부여 서버가 여러 개의 자원서버를 위해 사용할 수 있다. OAuth2.0 표준안에는 인증방법과 인증 권한부여 방법은 제시되어 있지 않으며, 자원 서버와 권한부여 서버와의 상호작용도 제시되어 있지 않다[3]. 인증 방법은 커버러스 기법이나 PKI 기법, 또는 패스워드 기법 등이 제시되고 있지만[4], 권한부여 방법과 자원 서버와 권한부여 서버와의 상호작용 방식에 대해서는 간단히 인증이 성공하면 접근 토큰을 부여하는 방식이다.

본 논문에서는 권한부여 서버와 자원 서버와의 상호과정 모델 제시하여 효율적이고 효과적인 권한부여 기법을 제안한다. 자원 서버와 인증부여 서버와의 통신을 효율적으로 하기 위해 인증부여 서버와 자원 서버와의 세션키를 미리 분배하거나 동적으로 분배한 후, 해시함수를 이용하여 접근 토큰 정보들을 부여한다. 접근 토큰을 구하는 방식은 다음과 같다.

$$AccessTokeni = h(Ek\_n(AccessTokeni-1))$$

AccessTokeni는 i번째 접근 토큰으로 i-1번째 접근 토큰을 이용하여 권한부여서버와 자원서버와의 비밀키를 통해 암호화하여 생성함으로써 API에 대한 접근 허가를 체크한다. 이 방식을 쓰면 인증부여서버와 자원서버와의 통신은 거의 발생하지 않아서 효율적이며 토큰의 재사용이 불가능하며, 유효한 토큰이 계속 생성되므로 접근 토큰의 취소 과정이 불필요하여 효과적이다. 또한, 권한부여서버와 여러 자원서버가 하나의 키를 공유한다면, 하나의 접근 토큰을 이용하여 여러 자원서버로의 접근도 가능하다. 물론 이 방식은 권한 부여서버와 자원서버와의 동기화가 필요하지만, 그렇게 많은 오버헤드를 발생하지 않은 것이다.

IV. Conclusions and Future Works

본 논문에서는 IoT 환경을 위한 효율적이고 효과적인 OAuth2.0 적용 기법을 제안하였다. 향후 연구과제로는 제안한 기법을 경량의 암호화 기법과 경량의 해시함수에 적용하여 자원제약적인 IoT 디바이스에 적합하도록 연구하는 것이다. 또한, 제안 기법이 보안 문제를 발생시키지 않는지도 검증할 것이다.

References

[1] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios," IEEE Sensors Journal, Vol. 15, No.2, 2015.

[2] M. Spasovski, "OAuth2.0 Identity and Access Management Patterns," Packt Publishing, 2013.

[3] D. Hardt, "The OAuth 2.0 Authorization Framework," rfc 6749, IETF, 2012.

[4] S. Emerson, Y-K Choi, D-Y Hwang, K-S Kim, and K-H Kim, "An OAuth based Authentication Mechanism for IoT Networks," (ICTC), 2015 International Conference on. IEEE, 2015.