이벤트 기반 IoT 디바이스 데이터 통신을 위한 OAuth 2.0

*육근웅 **임태범
전자부품연구원
*kunwoongyuk@keti.re.kr

OAuth 2.0 For Event-based IoT Device Data Communication

*Kun Woong Yuk **Lim Taebeom
Korea Electronics Technology Institute

요 약

웹 서비스에 주로 적용되어 왔던 OAuth 2.0 사용자 인증 기법을 이벤트 기반 IoT 디바이스 데이터 통신 처리에 이용할 수 있도록 확장한다. OAuth 2.0 사용자 인증 기법은 최소화된 인증 절차에 맞추어져 있지만, 이벤트 기반의 IoT 디바이스의 데이터를 응용하기에는 적합하지 않은 실정이다. OAuth 2.0 사용자 인증 기법을 이용하여 이벤트 기반의 IoT 디바이스 데이터 통신으로 동작하기 위한 구성방법, Data Format, 그리고 전송 구조를 제안한다.

1. 서론

최근 들어 사물인터넷(IoT) 가전 및 센서 통신 기술의 급격한 발전으로, 사물인터넷의 데이터를 이용한 복합 서비스의 필요성과 개발이 급속도로 증가하고 있다. 이에 따라 IoT 디바이스 데이터 이용에 대한 수요도 지속적으로 증가되고 있다. 따라서 효과적인 데이터 응용 및 통신 기법이 요구되고 있는 실정이다.

사물인터넷에서 OAuth 2.0 기법은 사용자에게 해당 디바이스의 접근 권한 부여를 위한 개방형 표준 기법으로 널리 알려져 있다. 그 중 Authorization Request 는 사용자의 IoT 디바이스 데이터 제어 및 접근 할 수 있는 승인 요청의 요소들을 만들어 승인 요청의 단계로 넘어가기 위한 설정이다.

일반적으로 사용자의 승인 요청을 하기 위하여 " application/x-www-form-urlencoded" 형식을 사용하는 권한 부여 종단점 URI 의 질의 구성 요소를 만드는 역할은 한다. response_type, client_id, redirect_uri(optional), scope(optional), state(optional)과 같은 매개 변수의 구성이다. OAuth 2.0 기법은 Client Side 의 간단한 구현으로 효과적인 사용자의 개인 정보의 공개 설정 및 IoT Device 의 Data 접근 및 제어의 역할을 수행할 수 있으므로 Google, Facebook, Twitter 등과 같은 다양한 웹 서비스와 Smartthings, NetAtmo Weatherstation, Fitbit 등 다양한 사물인터넷 서비스 분야에서 사용되고 있다. 일반적인 OAuth 2.0 Authorization Request[1]의 parameters 구성의 범위를 response_type, client_id, redirect_uri 에서 Event 기반의 IoT Device 의 Data 와 통신 할 수 있도록 매개 변수를 확장하는 방안을 제시하여 사물인터넷을 이용한 서비스를 더욱 효과적으로 향상시킬 수 있다.

현재 서비스 제공자가 이벤트 기반 IoT 디바이스 데이터를 실시간으로 얻기 위해서는 대부분 Polling 기법을 이용하거나 CronTap 기법 또는 Scheduling 기법을 이용해야 한다. 때문에 Event 기반의 실시간 처리가 필요한 IoT Device Data 를 이용한 서비스를 제공할 경우 짧은 주기의 Pooling 방식을 이용하는 것이 최선이다. 또한 이용자가 많아질수록 서버의 성능이나, DataBase 의 관리, 회선관리의 문제가 발생 할 수밖에 없다. 이러한 문제 때문에 분산 처리 시스템을 한다고 하여도 서버 구축에 필요한 비용이 발생하거나 시스템의 복잡도를 높이게 되므로 Event 기반 IoT Device 의 실시간 Data 처리에는 Polling 이나 crontap, Scheduling 은 적합하지 못하다. 본 논문에서는 위와같은 문제점을 해결하기 위한 구조를 제안한다. 구체적으로 OAuth 2.0 의 Redirect URI 기법을 이용하여 현재의 Event 기반 IoT Device 의 Data 통신을 구성하는 방안을 제안한다.

본 논문의 구성은 다음과 같다. 2 절에서는 이러한 OAuth 2.0 Authorization Request 기법을 확장하여 이벤트 기반 IoT 디바이스 데이터 통신 방안, 마지막으로 3 절에서는 본 논문에 대한 결론을 맺는다.

2. OAuth 2.0 Authorization Request 기법을 확장한 Event 기반 IoT Device Data 통신 방법

본 장에서는 OAuth 2.0 의 Authorization Request 기법을 확장하여 Event 기반의 IoT Device data 통신 방법을 제안한다. 먼저 현재의 일반적인 OAuth 2.0 Authorization Request 구성은 그림 1 과 같은 구성으로 인증 서버로부터 승인 서버로의 접근 정보의 수신 기능을 수행한다.

```
GET
/authorize?response_type=[code]&
client_id=[Request Client Id]&
state=[Session State]&
redirect_uri=[Redirect URI]
```

그림 1. OAuth 2.0 Authorization Request 의 예

OAuth 2.0 Authorization Request 문제점은 OAuth 2.0 인증 후 인증 받은 IoT 디바이스 데이터를 응용하여 새로운 서비스를 제공하려고 할 때 이다. 새로운 서비스로 IoT 디바이스 데이터를 응용 할 때, IoT 디바이스 제조사에서 인증 받은 데이터를 전송 받을 수 있는 시스템이 구축되어 있지 않다면, 서비스 사업자는 인증 받은 사용자의 Data 를 가져오기 위해서는 Pooling, Long Polling, CronTap 등의 방법을 이용한다. 이와 같은 구조는 클라이언트의 고성능의 Hardware 의 필요성을 요구할 뿐만 아니라, Web 표준을 준수하고 Web Data 를 고속으로 처리할 수 Softeware 가 요구 된다. 또한 Network 의 과부하를 불러올 수 있으며 Data 를 요청하고 실패하였을 경우를 위한 오류 처리 또한 고려해야 하므로 Softeware 개발의 복잡도를 높일 수 있다.

현재의 문제점을 해결하기 위한 방안으로 Authorization Request 기법에 인증 받은 사용자의 IoT 디바이스 데이터를 전송 받을 수 있도록 매개 변수를 확장하고 확장에 따른 보안의 문제점을 해결하기 위한 방법을 제시한다. OAuth 2.0 표준 인증 서버의 경우 Authorization Request 기법에 추가로 Customize 된 매개 변수를 정의 할 수 있다. 그림 2 와 같이 일반적인 Authorization Request 요청에 이벤트 데이터를 전송 받을 지에 대한 설정을 하는 매개 변수와 이벤트 데이터를 전송 받을 URI 를 설정하는 매개 변수, Event Data 전송 주기를 설정하는 매개 변수로 구성한다.

```
GET /authorize?response_type=[code]&
client_id=[ Request Client Id]&
state=[ Session State]&
redirect_uri=[ Redirect URI]&
event=[Enab le Option]&
event_uri=[ Event Data Receive URI]&
event_time=[Event Data Receive Time]
```

그림 2. OAuth 2.0 Authorization Request Event 매개변수 구성의 예

그림 2 와 같은 OAuth 2.0 Authorization Request 가 요청되었을 시 인증 서버는 인증을 요청한 사용자가 IoT Device 에서 Event 가 발생하였을 시 해당 Event 의 data 를 전송 받는 권한 또한 인증 하는 것으로 간주 하고 해당 인증 정보를 등록 한다. 등록된 인증 정보를 기반으로 사용자의 IoT Device Data 를 관리 하는 Data 관리 서버는 위와 같은 설정에 따라 인증 받은 IoT Device 의 Event 가 발생 할 때 마다 event_uri 로 event 가 발생한 data 를 그림 3 과 같은 data format 으로 전송한다.

```
POST
   PostBody{
   deviceId : exampleId,
   deviceType : exampleType,
   deviceValue : exampleValue
   }
httpPost(event_uri, PostBody);
```

그림 3. Event HTTP Post 전송의 예

그림 4 와 같은 Data 전송 구조를 구성함으로써 사용자는 인증 서비스 제공자가 인증 받은 사용자의 IoT 디바이스 데이터를 얻어 오기 위하여 불필요한 Pooling, Long Pooling, CronTop 등의 동작을 수행 할 필요가 없으며, IoT 디바이스 제조사가 제공하는 Resource Server 로부터 서비스 제공자는 httpPost 를 통해 Event 된 IoT 디바이스 데이터를 전송 받을 수 있다. 이러한 구조를 통해 최소한의 네트워크 자원의 사용과 Hardware 자원의 사용으로 서비스 이용자에게 빠른 처리 속도와 IoT Device 로부터 제공되는 데이터를 기반으로 한 사용자 상황/환경 정보에 적합한 서비스를 제공할 수 있다.

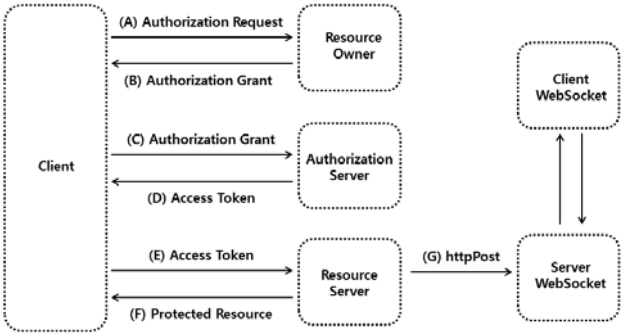

그림 4. Data 전송 구조의 예

3. 결론

본 논문에서는 OAuth 2.0 Authorization Request 기법을 확장한 이벤트 기반 IoT 디바이스 데이터 통신 구성 방법을 제안하였다. 특히 Authorization Request 매개변수의 확장을 이용한 구성 방법을 제안하였으며 이를 통하여 현재의 OAuth2.0 시스템 구조 및 이벤트 기반 IoT Data 응용 서버의 구조를 개선하여 이벤트 기반 IoT Device 또는 Non-Event 기반 IoT Device 를 이용한 응용 서비스의 개발 및 사용이 증가 할 것으로 기대한다.

Acknowlegement

본 연구는 미래창조과학부 및 정보통신기술진흥센터(IITP)의 산업융합원천기술개발사업(정보통신)의 일환으로 수행하였음. [과제번호(R0101-15-0159), 기기 정보뿐 아니라 사용자의 환경/감성/인지 정보에 적응적으로 반응하는 정보기기용 원격 UI 기술 개발]

참고 문헌

[1]E. Hammer-Lahav, Ed. Yahoo! D. Recordon Facebook D.Hardt Microsoft “The OAuth 2.0 Authorization Protocol draft-ietf-oauth-v2-17” Internet-Draft 5849 July 8, 2011.

[2]D. Hardt, Ed. Microsoft “The OAuth 2.0 Authorization Framework” IETF RFC 6749, October. 2012.