IoT 환경에서 역할 기반 접근제어를 적용한 Claim Token 인증 방식

김남호○, 홍충선*
경희대학교 컴퓨터공학과
{knm1471, cshong}@khu.ac.kr

Claim Token authentication method applying role-based access control in IoT environment

Namho Kim○, ChoongSeon Hong*
Department of Computer Science and Engineering, Kyung Hee University

요 약

최근 다양한 IoT 디바이스들이 등장함으로써 국내외 IoT 시장 규모가 증가함에 따라, 수많은 IoT 디바이스들로 구성된 IoT 데이터들에 대한 보안 솔루션이 필요하다. Token 기반 인증은 기존의 세션을 활용한 인증과는 달리 사용자별 Token을 발급하고 Token 인증을 통해 데이터에 접근할 수 있도록 하는 인증 기법이다. 기존의 Token 기반 인증은 OAuth와 Claim Token 인증을 꼽을 수 있다. 그러나 OAuth의 경우, 사용자 별 Token을 발행 시 사용자의 아이디와 패스워드 그리고 발행된 Token에 대한 정보가 저장되어야 하며 이는 수많은 사용자가 데이터를 접근하는 IoT 환경에서 데이터베이스 요구사항을 높이게 된다. 따라서 본 논문에서는 역할 기반 접근 제어를 적용한 Claim Token 기반 인증 기법을 제안한다. 본 논문에서 제안하는 인증 기법은 Management Server에서 사용자 별 Access Token과 Refresh Token을 생성 및 부여하고, 사용자는 특정 IoT 데이터에 대한 요청을 Access Token을 통해 Fog Node로 전달함으로써 인증 후 데이터에 접근할 수 있도록 한다.

1. 서 론

최근 다양한 IoT 디바이스들이 등장함에 따라, 국내외 IoT 시장 규모가 향후 10년 동안 최대 5배 이상 성장할 것으로 예상하고 있다.[1] 이렇듯 IoT 시장 규모의 성장과 수많은 IoT 디바이스들로 인하여 생성되는 정보들에 대한 솔루션이 필요하다. IoT 디바이스로부터 발생하는 데이터는 민감한 데이터를 처리하고 전송해야하는 경우가 많다. IoT 환경에서 이러한 데이터는 기밀성과 무결성이 보장되어야 한다.

따라서 본 논문에서는 역할 기반 접근 제어를 적용한 Token 인증 방식을 통해 IoT 데이터의 기밀성과 무결성을 보장하는 인증 방식을 제안한다. 본 논문에서 제안하는 인증 방식은 Claim Token 인증 방식을 사용하며 각각의 사용자에게 토큰 발행 시 역할 별 API 호출 권한을 상이하게 부여하는 정책(policy)을 적용하는 기법이다.

본 논문의 2장에서는 Token 인증 방식에 대해 설명하고, 3장에서는 본 논문에서 제안하는 시나리오와 시스템 구조를 명시한다. 그리고 4장에서는 본 논문에서 제안하는 인증 기법의 적합성을 확인한다. 5장에서는 본 논문에서 제안하는 인증 기법의 성능 평가를 기존 인증 기법과 비교하여 확인하고 끝으로 6장에서는 결론 및 향후 연구방향에 대하여 논한다.

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2015-0-00557, IoT 기기의 물리적 속성, 관계, 역할 기반 Resilient/Fault-Tolerant 자율 네트워킹 기술 연구) *Dr. CS Hong is the corresponding author

2. 관련연구

Token 기반 인증

Token 기반 인증은 토큰 기반의 HTTP 인증 체계를 의미한다. Token 기반 인증은 서버-클라이언트 구조에 적합하며[2], 이러한 인증 방식은 크게 OAuth와 Claim Token을 사용하는 JWT를 예로 들 수 있다.

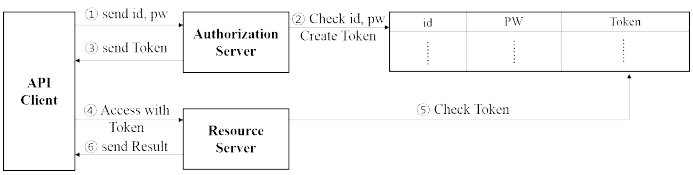

그림 1. Oauth 인증[3]

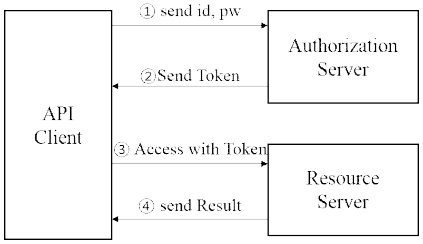

그림 2. JWT 인증[4]

그림 1과 2는 각각 OAuth 인증과 JWT 인증의 Flow를 보여준다. JWT 인증은 OAuth 인증과는 다르게 Token을 생성하여 저장하고 비교하는 부분이 없다는 것이 특징이다. 이는 Claim Token을 활용하기 때문인데, Claim Token을 활용할 경우 Token 자체 내부에 사용자 정보를 포함하기 때문에 추가적인 저장 및 인증 프로세스가 요구되지 않는다.

역할 기반 접근제어

역할 기반 접근 제어는 인증된 사용자에 대한 시스템 액세스를 제한하는 접근법이다. 이는 '역할'과 '권한'을 중심으로 정의된 정책을 활용하는 제어 메커니즘이다. 역할별 권한, 사용자별 역할, 등과 같은 구성 요소를 사용하여 사용자 별 권한 할당을 간단하게 수행할 수 있다.[5]

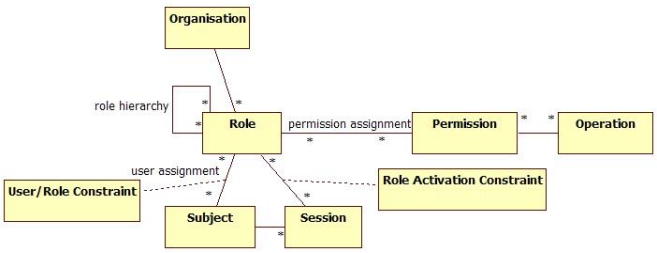

그림 3. RBAC(Role Based Access Control) 구성 요소

3. 시스템 구조 및 시나리오

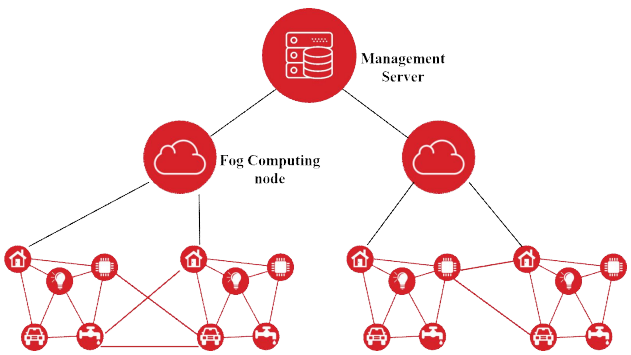

그림 4. 시스템 구조도

그림 4는 시스템 구조도를 나타낸다. 하나의 Management Server와 Fog 노드들 그리고 수많은 IoT 디바이스가 존재한다. 각각의 IoT 디바이스들은 Fog Node와 통신하며 자신의 데이터를 전송한다. 사용자는 Mobile application을 통해 IoT 디바이스의 데이터를 모니터링 할 수 있다. IoT 디바이스에서 생성되는 데이터는 개인 정보를 포함하거나 민감한 정보를 다룰 수 있으므로, 인증된 사용자에게만 데이터를 공개해야한다. 따라서 사용자는 인증 프로세스를 통해 데이터를 획득할 수 있다. 인증 프로세스는 다음과 같다.

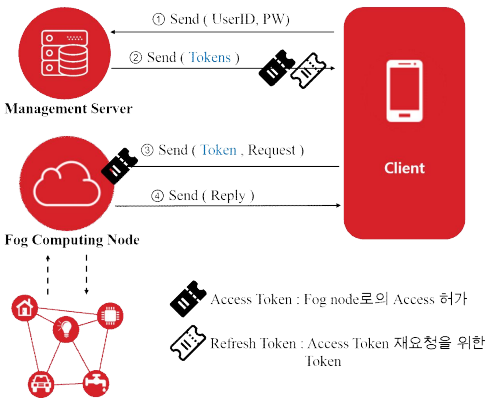

그림 5. 제안하는 인증 기법

여기서 사용자는 Management Server에 사전에 사용자 id와 비밀번호를 등록해두었다고 가정한다.

1) 사용자는 자신의 id와 비밀번호를 Management Server로 전달한다.
2) Management Server는 사용자의 id와 비밀번호를 확인하고 각 사용자별 접근제어 정책을 확인하여 Token을 생성한다. 이는 추후 내용에서 다루도록 한다.
3) Management Server는 Client에게 Access Token과 Refresh Token을 전달한다. 각각의 Token은 만료 시간 정보를 가지고 있다. Access Token은 Client가 Fog Node에 데이터를 요청할 때 사용한다. Refresh Token은 Access Token의 만료 시간이 지났을 때 Access Token을 갱신할 때 사용한다. 따라서 Refresh Toekn의 만료 시간은 Access Token보다는 길며, 만약 두 Token의 만료 시간이 지난 경우, 사용자는 다시 1)번의 과정을 통해 Token을 새로 발급받아야 한다.
4) Management Server로부터 전달받은 Access Token과 데이터 요청 Query문을 Fog Node로 전달한다.

5) Fog Node는 Token을 확인하고, 해당 API를 인증함으로써 Client가 해당 IoT 디바이스의 데이터를 가져갈 수 있도록 허가한다.

그림 5는 Token 발급 시 역할 기반 접근 제어 정책을 적용하여 Token을 생성하는 과정을 보여준다.

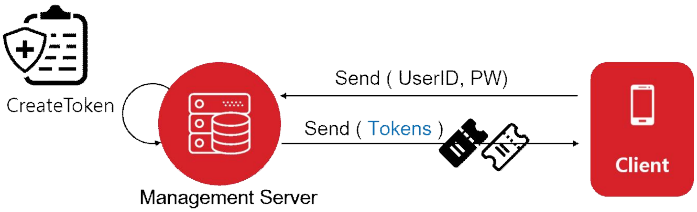

그림 5. 역할 기반 접근제어를 적용한 Token 발행

Client가 사용자의 id와 비밀번호를 전달하면 Management Server는 사전에 등록되어있던 사용자의 정보를 확인하여 사용자별 역할을 확인한다. 그리고 각 역할의 허가 권한을 확인하여 Token 생성 시 '역할'과 '권한'을 포함하는 Access Token을 생성한다.

4. 성능평가

기존의 인증 방식인 OAuth 2.0과 제안하는 역할 기반 접근제어를 적용한 인증 기법을 적용한 시스템을 구축하고 토큰을 저장하는 데이터베이스 공간 및 인증 수행 시간에 대해서 실험하였다. 그림 6은 실험 결과를 나타낸다.

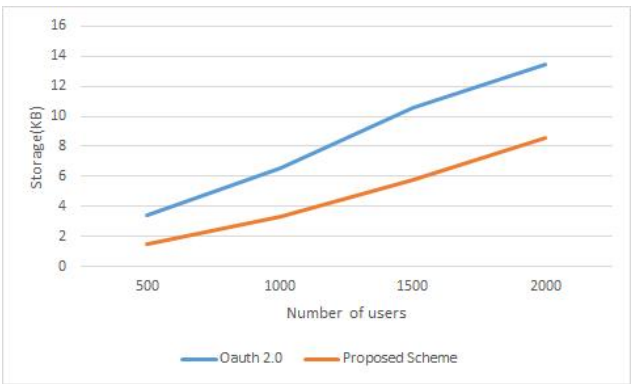

그림 6. 인증 기법 별 데이터베이스 요구사항

실험 결과를 나타낸 그림 6과 같이 기존의 OAuth 인증 방식 보다 제안하는 인증 기법이 데이터베이스 요구사항이 더 낮음을 확인 할 수 있었다. 또한, 제안하는 인증 기법은 Management Server에서 사용자 별로 토큰을 발급하고 Fog Node는 토큰을 확인하는 절차만을 수행하기 때문에 그림 7과 같이 인증 프로세스의 수행 시간 또한 낮음을 확인 할 수 있었다.

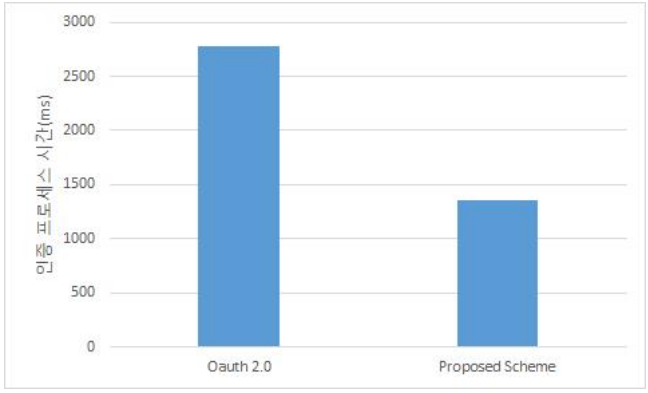

그림 7. 인증 기법 별 인증 수행 시간

5. 결론 및 향후 연구

본 논문에서는 역할 기반 접근제어를 적용한 Claim Token 기반 인증 기법을 제안한다. 본 논문에서 제안하는 인증 방법은 Session 인증 방식을 사용하지 않음으로써 자원 제약이 있는 IoT 디바이스와 사용자 Client간의 인증이 아닌 Fog Node와 Client간의 Token 인증을 통해 IoT 노드의 부하를 줄일 수 있다. 또한 Token은 Management Server에서 생성하기 때문에 기존의 OAuth 방법과는 달리 Fog Node의 데이터베이스 접근을 최소화함으로써 IoT 환경에 더 적합하다.

또한 역할 별로 권한이 허가되는 범위를 정의한 정책을 Token 생성 시 반영함으로써 민감한 데이터로의 접근을 차등적으로 관리할 수 있도록 함으로써 데이터의 기밀성과 무결성을 유지시킬 수 있다.

향후 연구로는 Token 생성 시 만료 시간을 포함시키는 과정에서 사용자 별 요청 횟수와 데이터 접근 시간 등을 확인하여 최적의 Token 만료 시간을 찾는 기법에 대해 연구할 것이다.

6. 참고문헌

[1] "IoT 현황 및 주요 이슈", 한국소프트웨어기술진흥협회
[2] TokenAuthentication, http://www.django-rest-framework.org/api-guide/authentication/#Tokenauthentication
[3] D.Hardt, "The OAuth 2.0 Authorization Framework", RFC 6749, Internet Engineering Task Force, Oct 2012
[4] Json Web Token, https://en.wikipedia.org/wiki/JSON_Web_Token
[5] Role based access control, https://en.wikipedia.org/wiki/Role-based_access_control