블록체인 기반 ThingsBoard의 엑세스 토큰 인증 강화

장성일, 김명호
숭실대학교 소프트웨어학과
e-mail:sungil@soongsil.ac.kr, kmh@ssu.ac.kr

ThingsBoard's Access Token Authentication Enhancement based Blockchain

Sung-Il Jang, Myung-Ho Kim
Dept. of Software, Soong-Sil University

요 약

ThingsBoard에서 사용되는 엑세스 토큰 인증 방식에 블록체인 메커니즘을 적용하여 디바이스의 무결성을 강화한다. 인증에 사용되는 데이터는 보호되어야 하고, 빠르게 제공되어야하기 때문에 제안 인증 방식에 퍼미션드 블록체인을 사용한다. 본 논문은 실험을 통해 블록체인 기반의 제안 인증 방식이 디바이스의 무결성을 강화하면서도 큰 성능저하를 발생시키지 않는 것을 검증한다.

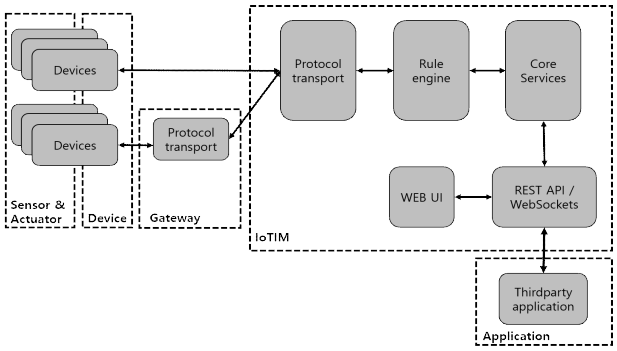
1. 서론

IoT 플랫폼의 인증 방식은 크게 엑세스 토큰 방식과 X.509 인증서 방식이 있다. 엑세스 토큰 방식은 자원이 제한적인 디바이스들도 지원이 가능하고, 적은 네트워크 오버헤드를 가진다. 하지만 암호화되지 않은 네트워크에서 취약하다는 단점이 있다. X.509 인증서 방식은 공개키 기반의 암호화된 네트워크 연결로 높은 수준의 보안을 보여준다. 하지만 이에 상응하는 큰 네트워크 오버헤드가 있다. IoT 오픈소스 플랫폼인 ThingsBoard는 두 가지 방식을 모두 지원한다[1]. 하지만 엑세스 토큰 방식은 보안성에 문제가 있어 테스트 용도로만 사용되고 있다. 본 논문은 블록체인을 기반으로 엑세스 토큰 인증 방식의 디바이스 무결성을 강화하여 서비스 운영에 사용할 수 있도록 한다.

2. ThingsBoard

ThingsBoard는 (그림 1)과 같은 아키텍처로 구성된다. IoTIM(IoT Integration Middleware)에 연결되는 클라이언트는 디바이스와 게이트웨이가 있다. 각 클라이언트는 IoTIM에 연결될 때 인증을 수행한다.

엑세스 토큰 인증 방식의 경우, ThingsBoard는 게이트웨이가 엑세스 토큰 인증에 성공하면 게이트웨이에 연결된 디바이스는 추가적인 인증을 거치지 않고 IoTIM에 연결된다. X.509 방식의 경우 모든 디바이스가 키 기반으로 통신하기 때문에 추가 인증을 하지 않아도 문제가 없지만 엑세스 토큰 방식의 경우는 디바이스를 증명할 수단이 없어 디바이스의 무결성을 보장하지 못하는 문제가 있다.



(그림 1) ThingsBoard 아키텍처

3. 블록체인

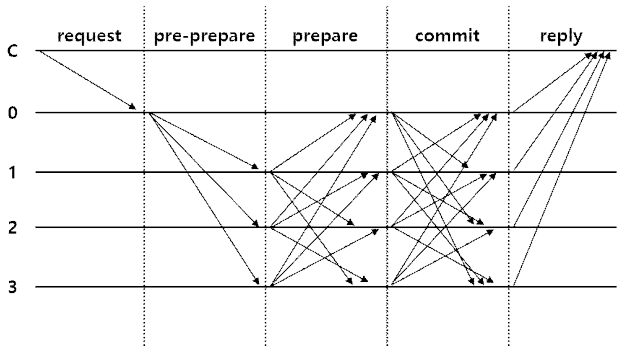
블록체인의 기본 개념은 트랜잭션 관리 단위인 블록을 체인 형태로 저장하고 블록의 내용을 공개함으로써, 누구나 블록을 만들거나 검증에 참여할 수 있다는 것이다. 블록체인 기술은 합의 알고리즘을 통해 블록들의 유효성을 보장한다. 각 블록체인은 합의 알고리즘에 따라 퍼미션리스 블록체인과 퍼미션드 블록체인으로 분류된다[2].

퍼미션리스 블록체인은 합의 알고리즘으로 작업증명 알고리즘이나 지분증명 알고리즘을 사용한다. 작업증명과 같은 합의 알고리즘은 암호 화폐 분야에 최적화된 합의 알고리즘이다. 하지만 기업들의 속도나 프라이버시에 대한 요구사항을 만족시키기는 어려운 합의 알고리즘이기 때문에 PBFT나 dPoS와 같은 합의 알고리즘을 사용하는 퍼미션드 블록체인들도 발전하고 있다. 퍼미션리스 블록체인은 주로 비트코인과 같은 암호 화폐들로 구성되어 있고, 퍼미션드 블록체인은 Hyperledger Fabric이나 Tendermint 등

이 있다[3,4,5].

본 논문은 블록체인 메커니즘을 엑세스 토큰 인증 방식에 적용한다. 기존 인증 방식은 PostgreSQL 등 데이터베이스를 사용하여 토큰을 관리한다. 제안 인증 방식은 블록체인을 통해 토큰을 관리하기 때문에 작업증명과 같이 데이터의 완전성을 즉각적으로 보장하기 힘든 합의 알고리즘을 사용하기에 적합하지 않다. 또한 인증 데이터를 블록체인에 저장하기 때문에 블록 데이터의 프라이버시가 보장되어야 한다.

따라서 본 제안 방식은 퍼미션드 블록체인을 사용한다. 그 중에서도 PBFT 기반의 Hyperledger Fabric을 사용한다[6,7]. PBFT 알고리즘은 크게 5단계의 과정을 커진다. 아래 그림은 PBFT 알고리즘의 합의 과정을 나타낸 그림이다.



(그림 1) PBFT 알고리즘의 합의 과정

PBFT 알고리즘을 블록체인 시스템에 적용하자면 아래와 같이 적용할 수 있다.

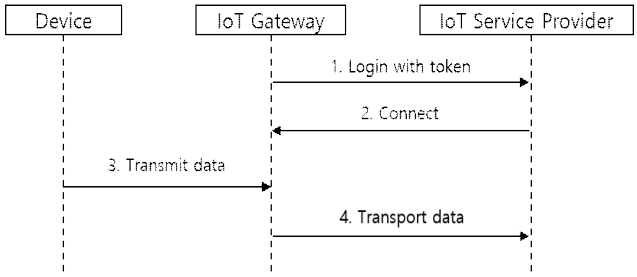
1. Request: 대표 노드는 클라이언트로부터 요청을 받아 해당 요청들을 수집한다.
2. Pre-prepare: 대표 노드는 수집한 요청들을 블록으로 만든 뒤, 합의 과정에 참여하는 노드들에게 전달한다.
3. Prepare: 각 노드들은 블록을 받았다는 사실을 다른 노드들에게 전파한다.
4. Commit: 각 노드는 다른 노드의 2/3 이상이 블록을 받았을 경우 해당 블록의 검증을 수행한다. 그리고 검증 결과를 다른 노드들에게 전파한다.
5. Reply: 각 노드들은 블록의 검증 결과를 수집하여 2/3 이상이 유효하다고 인정하면 블록체인에 해당 블록을 추가하고, 그렇지 않다면 삭제한다. 그리고 해당 결과를 클라이언트에게 반환한다.

또한, PBFT 알고리즘이 유효하려면 합의 네트워크에 최소 4개의 노드가 필요하다($n = 3f + 1$). PBFT 알고리즘은 n개의 노드가 존재할 때, f개의 악의적인 노드를 허용한다. PBFT 기반 블록체인에서는 블록을 추가할 때, 2f + 1개의 노드들의 동의를 얻어야 유효한 블록으로 인정된다[6].

4. 본론

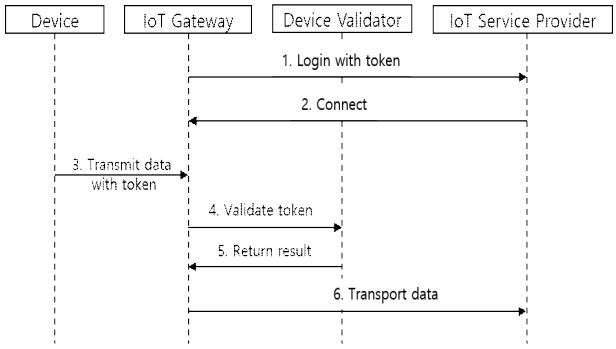
ThingsBoard의 엑세스 토큰 인증 방식은 로그인 시 토큰을 전달받아 인증한다. 플랫폼은 전달받은 엑세스 토큰을 데이터베이스의 저장된 토큰과 비교하여 로그인하려는 유저의 정보를 확인한다.

본 논문은 IoT 서비스제공자가 퍼미션드 블록체인 메커니즘을 적용하여 IoT 게이트웨이를 통해서도 토큰의 검증을 수행할 수 있도록 하는 시나리오를 구성하고 블록체인을 통한 엑세스 토큰 인증 방식의 성능을 검증한다. 아래 그림은 기존의 게이트웨이를 통한 디바이스 인증 시퀀스다.



(그림 2) 기존 방식의 시퀀스 다이어그램

IoT 디바이스는 IoT 게이트웨이의 토큰에 종속된 채 인증된다. 이는 IoT 특성 상 많은 디바이스의 연결을 감당하기 위한 조치로 보인다. 하지만 현 방식은 간단한 정보만 알면 게이트웨이를 통해 플랫폼에 접근하기 쉽다는 단점이 있어 디바이스의 무결성을 저하시킨다.



(그림 3) 제안 방식의 시퀀스 다이어그램

따라서 본 논문은 게이트웨이와 플랫폼이 노드로 참여하는 블록체인 네트워크를 구성한다. 그리고 Device Validator로 명명한 스마트 컨트랙트를 실행하여 IoT 게이트웨이가 디바이스에 대한 인증을 수행함으로써, 디바이스의 무결성을 강화한다.

5. 실험 및 평가

본 논문에서는 실험을 위해 Java 기반 사물인터넷 플랫폼인 ThingsBoard와 사물인터넷 게이트웨이인

ThingsBoard IoT Gateway를 사용한다. 또한 블록체인 시스템은 Go 기반 Hyperledger Fabric을 사용하였다.

본 논문에서는 기존 사물인터넷 게이트웨이와 제안 게이트웨이의 성능 비교를 위해 작업 처리시간을 측정한다. 실험에 사용된 디바이스의 개수는 아래 표와 같다.

<표 1> 실험에 사용된 디바이스 개수

구분	디바이스의 개수	전달한 총 메시지
Case 1	1 개	600 개
Case 2	10 대	6000 개
Case 3	25 개	15000 개
Case 4	50 개	30000 개
Case 5	100 개	60000 개

실험에서는 디바이스 개수별 작업 처리시간을 측정하여 비교한다. 디바이스의 개수는 <표 1>과 같이 5가지 경우로 구분하여 진행하였다. 각 디바이스는 50 KB의 문자열 데이터를 1초에 1개씩 전송하는 것으로 가정하고 작업 처리시간을 측정하였다. 디바이스 요청 메시지는 부하발생기에서 JMeter를 사용하여 발생시켰다.

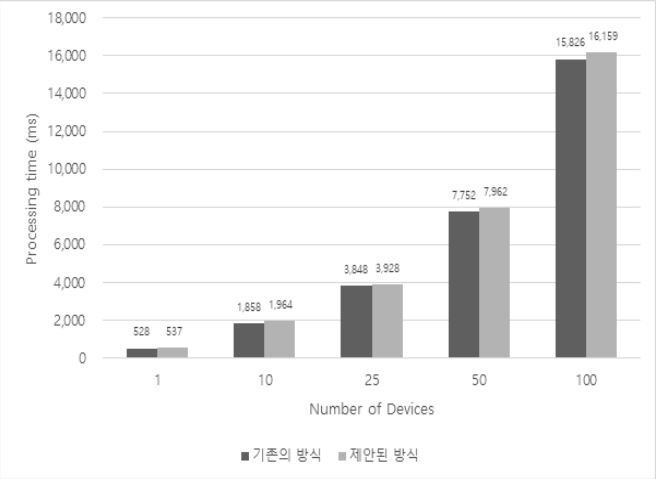
본 논문에서 측정한 작업시간은 부하 발생기에서 전송된 메시지를 IoT 게이트웨이가 처리할 때까지의 시간이다. 그리고 본 실험에 사용한 실험 환경은 다음 표와 같다.

<표 2> 실험 환경

구분	Hardware		EA
	CPU	RAM	
IoT 플랫폼	Intel Core i7 3.4GHz	16GB	1
IoT 게이트웨이	Intel Core i7 2.93GHz	8GB	2
블록체인 시스템	Intel Celeron G530 2.4GHz	8GB	1
	Intel Core i5 3.2GHz		1
부하 발생기	Intel Core i5 2.3GHz	16GB	1

(그림 4)는 실험의 각 케이스들을 가로축으로, 측정된 누적 작업처리시간을 세로축으로 그린 그래프다. 제안 게이트웨이는 디바이스의 인증을 추가로 수행하지만 전체 작업처리시간에 큰 영향을 주지 않는 것을 확인할 수 있다.

본 제안 방식은 퍼미션드 블록체인을 사용하여 게이트웨이 노드 내에 블록체인 데이터베이스가 존재한다. 따라서 엑세스 토큰 조회 시 외부로 요청을 보내지 않는다. 게이트웨이 내에서 인증 데이터의 처리하기 때문에 인증 시 발생하는 네트워크 오버헤드가 최소화되어 위와 같은 결과가 도출되었다.



(그림 4) 디바이스 수에 따른 누적 작업처리시간

6. 결론

본 논문은 퍼미션드 블록체인을 통해 TingsBoard의 엑세스 토큰 인증 방식에서 디바이스의 무결성을 강화할 수 있는 방식을 제안하였다. 제안 방식은 퍼미션드 블록체인 네트워크를 이용하여 인증 데이터를 공유하고 프라이버시를 확보하였다. 각 게이트웨이는 인증을 할 때마다 중앙 데이터베이스에 토큰 확인 요청을 보내지 않고 블록체인 데이터베이스를 통해 토큰을 확인할 수 있다. 블록체인 데이터베이스는 각 IoT 게이트웨이 노드 내에 존재하기 때문에 인증 시 데이터 요청에 의한 네트워크 오버헤드를 최소화한다. 따라서 제안 방식은 IoT 플랫폼에서 디바이스의 무결성을 강화하면서 큰 성능저하를 일으키지 않는다.

ACKNOWLEDGMENT

본 연구는 중소벤처기업부에서 지원하는 산학연협력기술개발사업(S2635358)의 연구수행으로 인한 결과물임을 밝힙니다.

참고문헌

[1] ThingsBoard device authentication options, https://thingsboard.io/docs/user-guide/device-credentials

[2] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, Huaimin Wang “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends” IEEE 6th International Congress on Big Data, 2017

[3] Satoshi Nakamoto “Bitcoin: A Peer-to-Peer Electronic Cash System” 2008

[4] Christian Cachin "Architecture of the Hyperledger

Blockchain Fabric" IBM Research, 2016
[5] Ethan Buchman, “Tendermint: Byzantine Fault Tolerance in the Age of Blockchains” 2006
[6] Miguel Castro, Barbara Liskov “Practical Byzantine Fault Tolerance” Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999
[7] Harish Sukhwani, Jos´e M. Mart´ınez, Xiaolin Chang, Kishor S. Trivedi, Andy Rindos "Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric)" IEEE 36th Symposium on Reliable Distributed Systems, 2017