블록체인 플랫폼과 IoT 클라우드 플랫폼 연동에 관한 연구

정한호, 오상봉*, 조욱**, 김호원***
부산대학교
hanho@islab.re.kr, *sangbong@islab.re.kr, **jouk@islab.re.kr, ***howonkim@gmail.com

A Study on the Link between blockchain platform and IoT cloud platform systems

Jeong Han Ho, Oh Sang Bong*, Jo Uk**, Kim Ho Won***
Pusan National Univ.

요 약

본 논문은 현재 다양한 분야에서 활용되고 있는 IoT 디바이스의 데이터 무결성 및 보안성에 관한 문제를 해결하기 위한 모델을 제안한다. IoT 디바이스는 일상생활의 편리성을 제공해 주지만, 해결해야 할 과제 또한 존재한다. 대부분의 IoT 장치는 저전력 장치에서 동작하므로 대부분의 보안성이 뛰어난 암호화 솔루션을 직접 적용할 수 없어 보안성 및 무결성에 대한 문제가 동반되며 한국정보통신기술협회에서 정의한 IoT 디바이스 보안 요구사항에도 데이터의 기밀성과 무결성 가용성, 인증/인가로 나누어 제시하고 있어 IoT 디바이스의 보안 문제는 오랜 기간 매우 중요하게 관리되고 있다. 본 논문에서 제시한 모델은 블록체인 플랫폼과 IoT 클라우드 플랫폼 간의 연동을 통해 IoT 디바이스의 데이터를 비공개/허가형 블록체인 네트워크에 저장하여 무결성과 기밀성을 보완하여 향후 IoT 디바이스의 보안 문제를 해결하기 위한 연구방향에 조금이나마 기여할 수 있을 것으로 기대한다.

Ⅰ. 서론

본 논문에서는 IoT 클라우드 플랫폼과 블록체인 플랫폼과의 연동 기술 모델을 보여준다. IoT 디바이스는 우리의 일상생활 모든 곳에 자리하고 있어 편리성을 제공해 주며 반도체, 제조, 금융, 식품 등 다양한 산업 분야에서 활용되면서 발전되고 있다. 하지만 사이버 보안 전문가들은 IoT 가 가장 취약한 기술 중 하나이며 데이터 도난, 물리적 파괴, DDoS공격, 랜섬웨어 등과 같은 신흥 인프라에 대한 더 많은 표적 공격에 대비해야 한다고 경고했다.[1] 해당 문제는 대부분의 IoT 디바이스가 저전력의 장치에서 동작하기 때문에 현재 상용되고 있는 강력한 암호화 솔루션을 적용할 수 없어 발생된다.[1] TTA 표준에서는 IoT 디바이스의 안전을 위한 보안 요구사항을 [표 1]과 같이 정의하고 있다.[2]

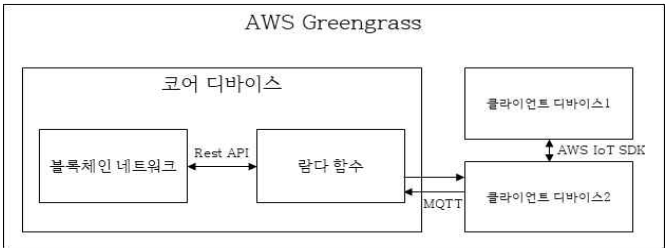
항목	요구사항
기밀성	메시지 암호화공격 탐지, 데이터 암호화, 부당 변경 방지, 외부 유출 방지
무결성	데이터 무결성 검증, 디바이스 무결성 검증, 시큐어 부팅 기능
가용성	로그 기능 제공, 기기 상태 정보 전송, 외부 공격 대응 기능, 보안 패치 기능, 정책 관리, 소프트웨어 안전성 확보
인증/인가	사용자 인증, 기기 인증, 주기적인 업데이트, 기기 간 상호 인증, 권한 제어, 접근 제어, 고유 식별 정보 검증 기능

〔표 1〕 IoT 보안 요구사항

본 논문에서는 IoT 보안 요구사항 중 기밀성, 무결성, 인증/인가 항목을 해결하는 것을 중점으로 연구를 진행하였고, 이에 따른 해결방안으로 AWS에서 제공하는 IoT 클라우드 플랫폼과 Hyperledger fabric 기반의 블록체인 네트워크를 구축해 IoT 클라우드 플랫폼과 블록체인 네트워크의 장점을 결합한 모델을 제안하였다. AWS Greengrass 플랫폼은 AWS에서 제공하는 IoT 클라우드 플랫폼으로 여러 IoT 디바이스들을 제어할 수 있는 sdk와 사용자 친화적인 대시보드를 제공해 주는 서비스이다. 또한 Hyperledger fabric은 비공개/허가형 블록체인 네트워크이며 누구나 네트워크에 참여하여 데이터를 열람하거나 거래가 가능한 비트코인과 같은 퍼블릭 블록체인과는 다르게 인증/허가된 사용자만 네트워크에 참여할 수 있는 네트워크 구조이다. 해당 블록체인 네트워크를 통해 디바이스 데이터가 블록체인의 특성인 불변성, 무결성, 부인방지 등의 성질을 가지게 되어 IoT 디바이스가 가지는 문제점을 해결할 수 있을 것이라 기대하며 본 논문에서는 제안된 모델의 구조 및 향후 연구 방향을 제시한다.

Ⅱ. 본론

본 논문에서는 AWS Greengrass 플랫폼을 이용해 IoT 디바이스들을 제어 및 연결, 디바이스 간 통신을 수행하고 그 결과 값을 블록체인 네트워크에 저장하는 모델을 제안하며, [그림 1]은 본 논문에서 제시한 모델의



〔그림 1〕 제안된 모델의 전체 구조

구조를 보여준다. 총 3개의 디바이스와 1개의 람다 함수, 블록체인 네트워크가 상호작용을 통해 블록체인 네트워크에 데이터를 저장하는 동작을 한다. 3개의 디바이스는 1개의 코어 디바이스와 2개의 클라이언트 디바이스로 나뉜다.

1. 코어 디바이스는 Greengrass에 속해있는 클라이언트 디바이스들과 AWS IoT 클라우드를 연결해 주는 중앙 관리 역할의 디바이스이다. 또한 코어 디바이스는 AWS에서 제공하는 IoT greengrass sdk를 이용하여 모든 장치와 장치 간 연결 및 통신을 제어할 수 있으며 람다 함수를 배포하여 서버 상태에 구애받지 않는 동작도 수행할 수 있다. 또한 본 연구에서 사용된 블록체인 네트워크도 코어 디바이스에 구축되어 있어 클라이언트 디바이스에서 전송되는 결과 값을 블록체인 네트워크에 저장한다.

2. 클라이언트 디바이스는 AWS에서 제공하는 IoT sdk를 이용하여 클라이언트 디바이스 간 통신이나 AWS IoT 클라우드에 Shadow 업데이트 요청을 보내는 등의 동작을 수행할 수 있다. Shadow는 AWS에서 JSON 형식으로 디바이스의 상태를 AWS 앱 및 기타 서비스에 연결할 수 있도록 데이터 스토어를 제공하는 서비스이다. 본 연구에서 클라이언트 디바이스들은 AWS IoT sdk에 작성된 MQTT 게시/구독 함수와 Shadow 업데이트 함수를 이용한다. 클라이언트 1은 클라이언트 2의 동작 제어만 기능하며 클라이언트 2는 센서와 같이 제어에 따른 실제 동작을 수행하도록 작성하였다.

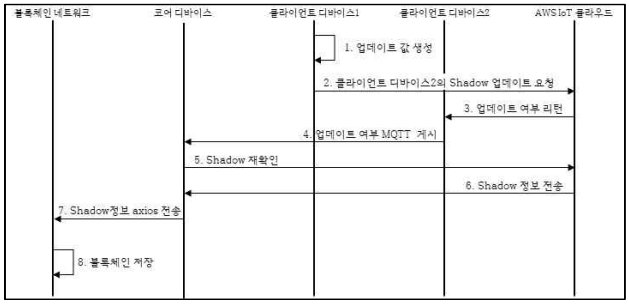
```
type GreengrassData struct {
        Doctype     string  `json:"doctype"`
        DeviceID    string  `json:"device_id"`
        State       string  `json:"State"`
        Payload     string  `json:"Payload"`
        Timestamp   string  `json:"timestamp"`
}
```

〔그림 2〕 go 언어로 작성된 본 모델의 스마트 컨트랙트 구조

3. Hyperledger fabric 기반 블록체인 네트워크는 chaincode라고 불리는 스마트 컨트랙트를 이용하여 데이터를 블록에 저장한다. 또한 Hyperledger fabric 기반 블록체인은 비공개/허가형 네트워크이기 때문에 인증/인가된 사용자만 네트워크에 참여할 수 있어 일반 사용자는 데이터 열람 및 접근할 수 없다. 이로인해 데이터의 기밀성을 가지게 되며 데이터의 저장 및 수정 또한 인증/인가된 사용자만 가능하므로 데이터의 무결성을 가지게 된다. [그림 2]는 본 모델에서 사용한 스마트 컨트랙트 토큰의 구조를 보여준다. 해당 토큰에서 Payload에 클라이언트 디바이스 2의 Shadow 값이 저장되며 Timestamp를 이용해 해당 트랜잭션이 올바른 트랜잭션인지 검사를 진행한다.

4. 람다 함수는 AWS에서 서비스하는 서버리스 함수로 AWS 서비스 전역에서 활용 가능한 함수를 사용자가 원하는 대로 작성할 수 있다. 본 모델에서는 코어 디바이스에 배포되어 클라이언트 디바이스 2가 자신의 Shadow값을 MQTT를 이용하여 특정 토픽에 게시하면 람다 함수는 해당 토픽을 구독하고 있다가 해당 내용을 블록체인 네트워크로 전송하는 역할을 하는데 이때, 블록체인 네트워크와 axios 통신을 이용하여 진행한다.

[그림 3]은 본 논문에서 제안한 모델의 전체 워크 플로우를 보여준다. 우선 클라이언트 디바이스 1 내부에서 특정 함수를 수행하여 생긴 결과 값을 이용하여 클라이언트 디바이스 2의 Shadow 값을 변경하라는 요청을 AWS IoT 클라우드에 전송한다. 그러면 IoT 클라우드는 클라이언트 디바이스 2의 Shadow를 업데이트한다. 이때, 클라이언트 디바이스 2는 자신의 Shadow 업데이트를 감지하면 MQTT를 이용하여 업데이트 여부를 사용자가 지정해놓은 특정 토픽에 게시한다. 람다 함수는 해당 토픽을



〔그림 3〕 제안된 모델의 워크 플로우

구독하고 있다가 게시물이 게시되면 클라이언트 디바이스 2의 Shadow 값을 다시 IoT 클라우드에 요청하여 Shadow 정보를 받은 뒤 해당 값을 axios를 통해 블록체인 네트워크에 전송한다. 그러면 마지막으로 코어 디바이스 내의 블록체인 네트워크에서 수신된 값을 블록체인에 저장함으로써 하나의 사이클이 종료된다.

Ⅲ. 결론

본 논문에서는 IoT 디바이스의 보안 문제에 따른 TTA에서 제시한 보안 요구사항 중 기밀성, 무결성, 인증/인가 항목 해결에 중점을 두었다. 우선 비공개/허가형 블록체인인 Hyperledger fabric기반 블록체인 네트워크를 이용하여 기밀성, 무결성, 인증/인가 항목을 해결하였고, AWS Greengrass를 사용하여 사용자 지정 함수 개발 및 IoT 디바이스 제어의 편의성을 보완하였다. 현재 블록체인 네트워크는 속도 및 컴퓨터 리소스 등의 문제를 해결하기 위한 많은 연구 및 개발이 진행되고 있다. 이에 맞춰 본 논문에서 제안한 모델의 연구를 통해 IoT 디바이스의 보안에 대한 문제 해결과 블록체인 기술의 발전에 기여할 수 있을 것이라 기대한다. 향후 해당 서비스 구조에서 클라이언트 디바이스 2의 값만이 아닌 클라이언트 디바이스 1의 값도 블록체인에 저장하고 람다 함수를 이용하여 일정시간 마다 블록체인 네트워크에 저장되어있는 데이터와 클라이언트 디바이스 2의 Shadow값을 비교하여 실시간 공격 감지 및 오류 수정 등의 기능을 추가하는 연구를 진행한다면 더욱 정교하고 안정성을 가진 IoT 클라우드 플랫폼을 구성할 수 있을 것이라 기대한다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 융합보안핵심인재양성사업의 연구 결과로 수행되었음 (IITP-2023-2022-0-01201)

참 고 문 헌

[1] Univ Plymouth. “A Concise Review on Internet of Things (IoT) - Problems, Challenges and Opportunities”, IEEE Xplore 2022.

[[2] 한국정보통신기술협회. “사물인터넷 기기 등급 분류 및 보안 요구사항”, TTA 2016.