스마트 컨트렉트를 사용한 IoT 서비스 접근제어 설계

김미선*, 서재현*
*국립목포대학교 정보보호학과
misun@mokpo.ac.kr, jhseo@mokpo.ac.kr

A Design of IoT Service Access Control using the Smart Contract

Mi-Sun Kim*, Jae-Hyun Seo*
*Dept of Information Security Engineering, Mokpo National University

요 약

IoT 서비스는 이기종의 다양한 IoT 장치들로부터 수집된 데이터를 목적에 맞게 가공, 저장, 처리하여 사용자에게 서비스를 제공한다. 본 연구에서는 이기종의 IoT 서비스에서 공유 가능한 접근 제어를 위해 스마트 컨트렉트를 사용하고자 한다.
이를 위해 IoT 데이터 공유를 위하여 탱글 네트워크 환경에서 실행되는 스마트 컨트렉트(Smart Contract)를 사용한 IoT 서비스 접근 제어를 설계하였다. 본 연구를 통해 이기종의 다양한 사물인터넷 서비스들이 탱글 네트워크를 통해 스마트 컨트렉트를 공유함으로써, 중앙 제어 없이 IoT 데이터 접근이 안전하게 이루어질 수 있다.

1. 서론

IoT 산업은 지속적으로 성장하여 더 많은 IoT 센서가 만들어지고, 다양한 분야에서 사용되고 있다. IoT 센서의 수가 증가함에 따라 해당 센서에서 생성된 데이터의 가치를 극대화하는 방법을 찾는 것이 점점 더 중요해지고 있다[1]. IoT 서비스는 다양한 IoT 장치들로부터 수집된 데이터를 목적에 맞게 가공, 저장, 처리하여 사용자에게 서비스를 제공한다. IoT 장치들로부터 수집된 데이터는 사물인터넷 서비스들에 의해 공유되어지며, 이 과정에서 보안 이슈가 발생할 수 있다.

기존 연구에서 사물 인터넷에 적합한 접근 제어를 위해 토큰을 이용하여 인증 및 권한 관리를 하고 모든 작업을 분산 원장 형태로 공유할 수 있는 기술을 제안하였으며[2,3], 본 연구에서는 이기종의 IoT 서비스에서 공유 가능한 접근 제어를 위해 스마트 컨트렉트(Smart Contract)를 사용하고자 한다.

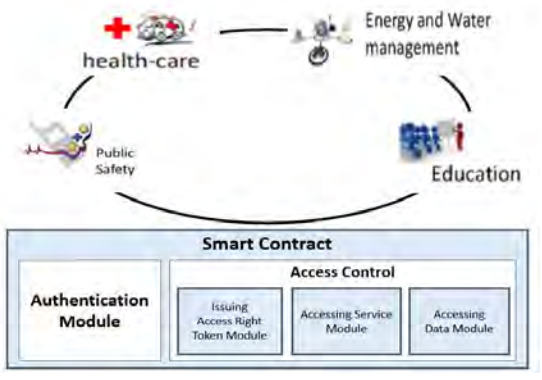
스마트 컨트렉트는 접근 권한 토큰 발급, 서비스 및 리소스 접근 수행을 위해 사용되며 탱글네트워크의 분산 원장에 트랜잭션으로 저장, 공유된다.

본 연구를 통해 이기종의 다양한 사물인터넷 서비스들이 탱글 네트워크를 통해 스마트 컨트렉트를 공유함으로써, 중앙 제어 없이 IoT 데이터 접근이 안전하게 이루어질 수 있다.

2. 스마트 컨트렉트를 사용한 IoT 서비스 접근 제어 설계

2.1 IoT 서비스 접근 제어 시스템 구성

본 논문에서는 IoT 서비스에 대하여 토큰 기반의 접근 제어를 수행하고 탱글 및 스마트 컨트랙트를 이용하여 분산화된 접근 제어를 수행하는 시스템을 제안하고자 한다. 이기종의 IoT 서비스에서 Smart Contract를 이용하여 접근 제어를 수행하는 시스템의 구성도는 (그림 1)과 같다.



(그림 1) 시스템 아키텍처

본 시스템은 IoT 서비스를 제공하기 위하여 다음과 같은 접근제어 과정을 수행한다.

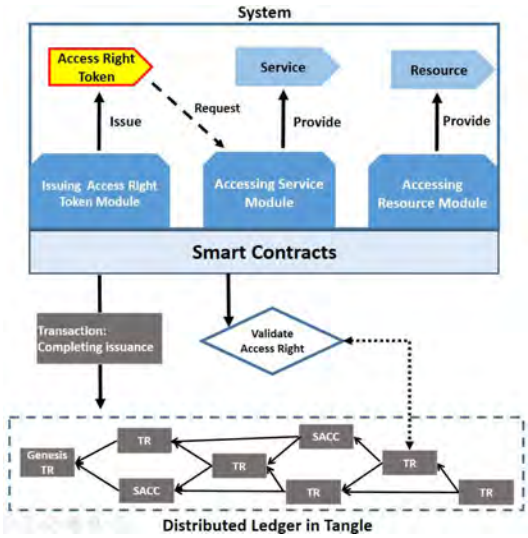
ⅰ. 접근 제어에 대한 정책을 스마트 컨트랙트로 정의한다.

ⅱ. 탱글의 분산 원장에 스마트 컨트랙트를 트랜잭션으로 저장하여 공유한다.

ⅲ. 공유한 스마트 컨트랙트를 기반으로 토큰을 발급함으로써 접근 권한을 부여하고 토큰에 대한 발급 사실을 원장으로 공유한다.

ⅳ. 발급한 토큰을 통하여 주체 기반의 접근 제어를 수행하여, 사물 인터넷 서비스에 대한 접근 제어를 수행한다.

접근 제어 수행을 위해 (그림 2)와 같이 모듈을 구성한다.



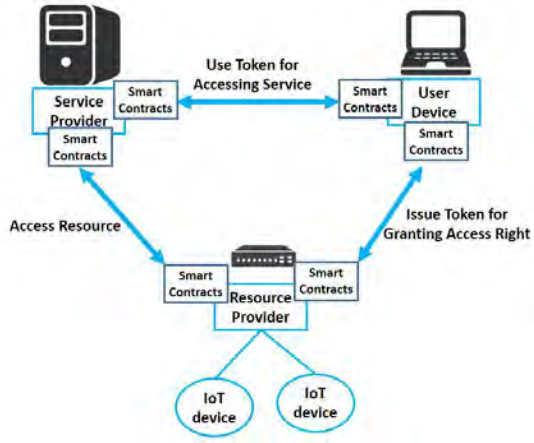
(그림 2) 시스템 모듈 구성도

접근 권한 토큰 발급 모듈에서는 스마트 컨트랙트를 이용하여 접근 권한 토큰을 발급함으로써 접근 권한을 부여한다.

서비스 및 리소스 접근 모듈에서는 스마트 컨트랙트를 이용하여 토큰에 대한 검증을 수행함으로써 서비스에 대한 접근 제어를 수행한다.

본 시스템에서는 토큰 발급에 대한 트랜잭션을 생성하여 발급 사실을 원장으로 공유한다. 원장으로 공유함으로써 다른 노드들은 토큰 검증을 위해 발급자에 요청을 수행하지 않고 토큰을 검증할 수 있다. 또한 한번 발급된 토큰을 재사용할 수 있으므로 반복적인 권한 부여 과정을 수행하지 않아 접근 제어 프로세스를 최소화 할 수 있다[2].

IoT 서비스 접근 제어 시스템은 (그림 3)와 같이 서비스 제공자, 리소스 제공자, IoT 디바이스, 유저 디바이스로 구성한다. IoT 디바이스를 제외한 나머지 노드들은 접근 권한 토큰에 대한 트랜잭션을 공유하며, 트랜잭션을 저장하기 위한 각자의 Wallet을 소유한다.

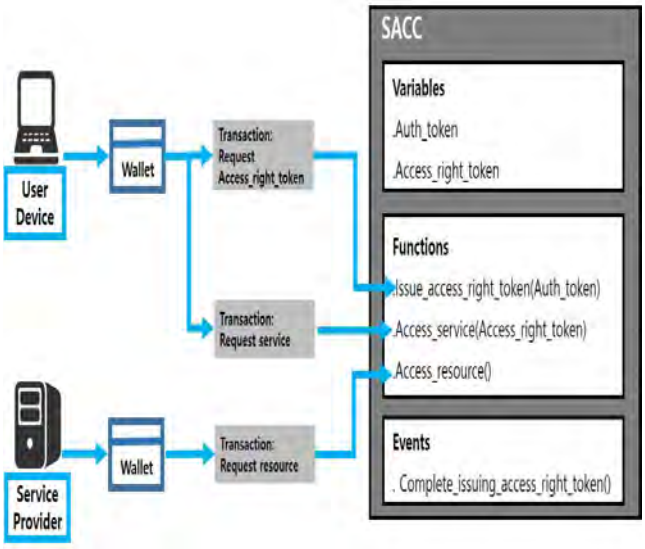


(그림 3) 서비스 구성도

2.2 서비스 접근 제어 컨트랙트(SACC, Service Access Control Contract)

본 논문에서 스마트 컨트랙트는 IoT 서비스를 이용하고자 하는 주체와 IoT 서비스 데이터를 제공하는 객체 사이에 접근제어를 수행하기 위해 인증 및 권한 부여를 위한 디지털 계약으로 정의하며, 서비스 접근 제어 컨트렉트(SACC, Service Access Control Contract)라고 명명하였다. SACC는 디지털 계약을 위한 함수들, 데이터, 각 스마트 컨트랙트간 메시지 전달을 위한 인터페이스 및 이벤트로 구성하였다.

본 논문에서 IoT 서비스 접근 제어를 위해 정의한 SACC의 구조는 (그림 4)와 같다.



(그림 4) SACC 구조

IoT 서비스 시스템에서 접근 제어를 위한 SACC의 주요 함수는 다음과 같다.

- Issue_access right_token() : 요청자의 인증 토큰을 파라미터로 입력받아 디바이스의 접근 권한 요청을 처리하여 접근 권한 토큰을 발행하는 함수이다. 인증 토큰에 대한 무결성 및 유효성을 검증하여 실패시 해당 요청을 거부하거나, 성고시 해당 유저 디바이스에게 접근 권한 토큰을 생성하여 송신한다.
- Access_service() : 요청자의 접근 권한 토큰을 파라미터로 입력받아 유저 디바이스의 서비스 요청을 처리하는 함수이다. 접근 권한 토큰의 생성자가 서비스에 대한 리소스를 소유하고 있는 리소스 제공자임을 확인하고 무결성을 확인한 다음, 원장에서 해당 토큰에 대한 발급 사실을 확인함으로서 유효성 검증을 수행한다. 검증이 실패하였을 경우, 해당 접근 요청을 거부한다. 검증이 성공하였을 경우에는 리소스 요청에 대한 트랜잭션을 생성하고 송신함으로써 Access data()를 호출한다. 인가된 유저 디바이스가 서비스를 요청했음을 전달하고 서비스에 필요한 리소스를 요청하여 수신한다. 또한 수신한 리소스를 이용하여 해당 유저 디바이스에게 서비스를 제공한다.
- Access_resource() : 서비스 제공자의 리소스 요청을 처리하는 함수이다. 요청을 수신한 리소스 제공자는 서비스에 필요한 리소스를 서비스 제공자로 송신한다.

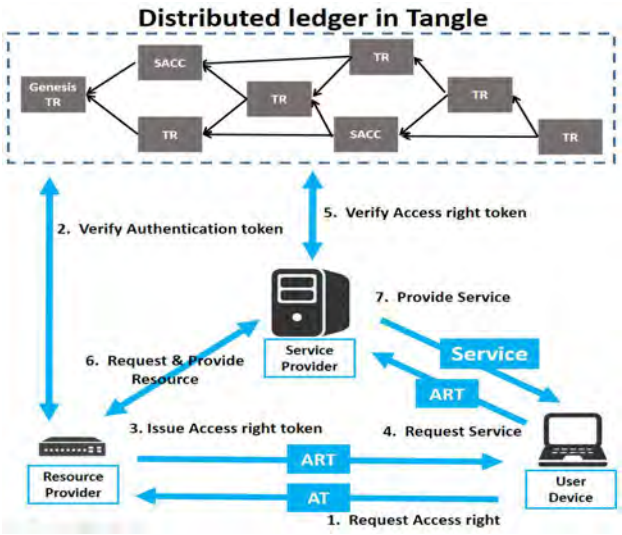
SACC는 컨트렉트의 수행 이후 발생 가능한 이벤트(Events)를 정의한다. SACC에서 이벤트는 컨트랙트의 함수를 수행한 다음, 함수 수행 결과에 대한 트랜잭션을 생성하여 다른 노드들에게 송신하는 기능을 갖는다.

SACC에서 정의한 이벤트는 다음과 같다.

- Complete_issuing_access_right_token() : 이 이벤트는 Issue_access_right_token()를 수행하여 접근 권한 토큰을 정상적으로 발급하였을 경우에 수행된다. 토큰 발급 완료에 대한 트랜잭션을 생성하여 시스템 노드들에게 송신함으로서 발급 사실을 노드들과 공유한다.

2.3 SACC를 사용한 IoT 서비스 접근 제어 프로세스

SACC를 사용하는 IoT 서비스 접근 제어의 전체적인 흐름도는 (그림 5)와 같다.



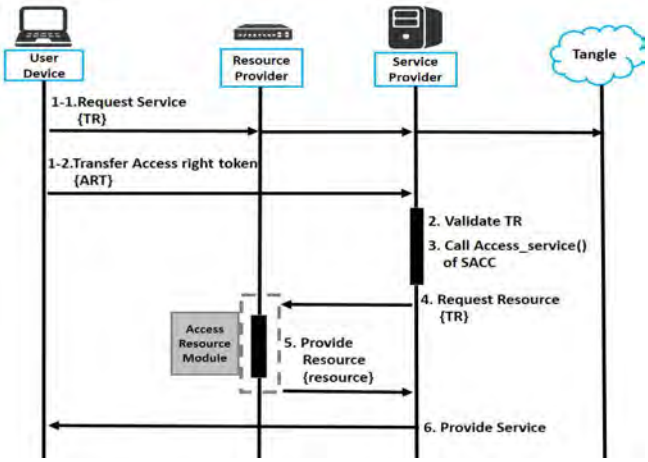
(그림 5) IoT 서비스 접근 제어 프로세스

본 논문에서는 IoT 서비스 접근 제어 시스템 모듈 중 서비스 접근 모듈에서 정의된 SACC를 사용하는 과정을 설명한다.

유저 디바이스는 서비스 제공자에게 소유하고 있는 리소스에 대한 접근 권한을 증명함으로서 서비스를 요청하여 이용할 수 있다. 서비스 요청 프로세스는 (그림 6)과 같다.

(그림 6) 서비스 요청 프로세스

유저 디바이스는 소유하고 있는 접근 권한 토큰을 이용하여 서비스 제공자에게 서비스를 요청할 수 있다. 서비스 요청 프로세스의 절차는 (그림 7)과 같다.



(그림 7) SACC를 사용한 서비스 요청 프로세스 절차

유저 디바이스는 서비스를 이용하기 위해 접근 권한 토큰 사용 요청에 대한 트랜잭션을 생성하여 시스템 노드들에게 송신한다. 또한 서비스 제공자에게 소유하고 있는 접근 권한 토큰을 송신함으로써 서비스 요청을 수행한다.

서비스 제공자는 수신한 트랜잭션에 대한 전자서명을 검증한다. 트랜잭션에 대한 검증이 완료되면, 서비스 제공자는 소유하고 있는 Wallet에서 SACC를 불러오고 서비스 접근에 대한 함수인 Access_service()를 호출한다.

Access_service()를 통해 수신한 접근 권한 토큰에 대한 전자서명을 검증하여 리소스 제공자가 발급했음을 확인한다. 소유하고 있는 원장에서 해당 접근 권한 토큰의 ID를 조회하여 비교함으로써 발급 사실 여부를 확인함으로써 검증을 수행한다. 검증이 실패하였을 경우 프로세스를 중단한다. 검증이 성공하였을 경우, 서비스 제공자는 서비스를 요청한 유저 디바이스에게 서비스를 제공함으로써 프로세스를 완료한다.

3. 결론

본 논문에서는 이기종 IoT 서비스의 접근제어를 위하여 스마트 컨트렉트를 이용하여, 접근 제어 토큰 발행 및 사용 관리 정보를 공유할 수 있는 시스템을 설계하였으며, 시스템 구성 및 SACC 구조를 정의하였다. 또한 IoT 서비스 접근 제어 시스템 모듈 중 서비스 접근 모듈에서 정의된 SACC를 사용하는 과정을 제시하였다.

추후 상세 아키텍처 설계 및 시스템 구현에 대한 연구를 진행하고자 한다.

Acknowledgement

본 논문(연구)은 교육부의 재원으로 이공분야기초연구사업의 지원을 받아 수행된 연구임

(No. NRF-2018R1D1A1B07051203).

참고문헌

〔1〕 Y.Zhang, S.Kasahara, Y.Shen, X.Jiang and J.Wan, "Smart Contract-Based Access Control for the Internet of Things", IEEE Internet of Things Journal, Vol. 6, No. 2, April, 2019.

〔2〕 Hwan Park, Mi-sun and Jae-hyun Seo, "Token-based IoT access control using distributed ledger", Journal of The Korea Institute of Information Security & Cryptology, Vol. 29, No. 2, pp.377-391, 2019.

〔3〕 Hwan Park, Mi-sun Kim and Jae-hyun Seo, "Token-based Righs Management Using IoT Blockchain", CISC-W'18, 2018.

〔4〕 I. Karamitsos, M. Papadaki, N. Baker Al Barghuthi, "Design of the Blockchain Smart Contract: A Use Case for Real Estate", Journal of Information Security, No. 9, pp. 177-190, 2018.