블록체인을 이용한 토큰 기반 IoT 접근제어 연구[1)]

김미선*, 박경우**, 서재현*
*목포대학교 정보보호학과
**목포대학교 융합소프트웨어학과
e-mail:misun@mokpo.ac.kr

A Study on Token based IoT Access Control using Blockchain

Mi-Sun Kim*, Kyung-Woo Park**, Jae-Hyun Seo*
*Dept of Information Security, Mokpo National University
**Dept of Software Convergence Engineering, Mokpo National University

요 약

IoT 환경은 다양한 장치들이 상호 통신을 통해 데이터를 발생하고 이에 대한 서비스를 제공한다. 이를 통해 많은 데이터와 객체 정보들이 네트워크를 통해 노출되어진다. 따라서, 신뢰할 수 있는 정보 접근 제어 서비스가 필요하다.

본 논문은 capability 토큰 기반의 IoT 접근제어 시스템에서 토큰의 생성, 위임, 폐기 과정에서 블록체인을 이용한 분산 트랜잭션 접근제어 모델을 제시한다.

1. 서론

IoT 환경은 다양한 장치들이 상호 통신을 통해 데이터를 발생하고 이에 대한 서비스를 제공한다. 이를 통해 많은 데이터와 객체 정보들이 네트워크를 통해 노출되어진다. 따라서, 신뢰할 수 있는 정보 접근 제어 서비스가 필요하다.

기존 연구[1]에서는 IoT 환경에서 접근제어를 수행하기 위하여 CapSG라는 게이트웨이를 통하여 중앙 집중적인 Capability 토큰의 발행 및 관리를 수행하였으며, Capabiltiy 토큰 기반의 접근제어의 효율성을 증명하였다. 그러나 토큰 발행에 있어서 중앙집중적인 관리가 이루어지고 있어, IoT 장치 및 사용자의 수가 증가함에 따라 이를 처리하기 위한 게이트웨이의 부하가 많아지고 게이트웨이가 발행하는 토큰에 대한 신뢰성에 대한 문제가 발생할 수 있다는 약점을 가지고 있다.

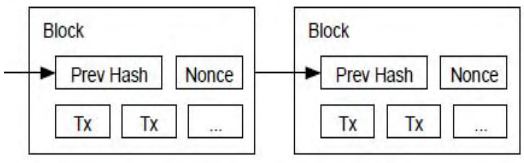
최근 블록체인 기술이 IoT를 위한 보안 이슈로 대두됨에 따라, IoT 환경에 블록체인을 통합하는 기술이 연구되고 있다[2].

따라서, 본 연구에서는 블록체인의 분산 트랜잭션 인증 기법을 적용하여 토큰의 발행, 위임, 폐기 과정에서 IoT 환경내 참여하는 기기간에 작업증명(Proof of work)을 통한 토큰에 대한 인증이 이루어지는 접근제어 모델을 제시하였다.

2. 블록체인을 이용한 토큰 기반 IoT 접근제어

2.1 블록체인의 작업증명(Proof of work)

블록체인은 가상화폐의 하나인 비트코인의 기반 기술로 사용되는 일종의 분산 공개 디지털 장부를 의미한다. 비트코인에서는 블록에 대해 다수의 사용자로부터 작업증명을 수행하고 이를 통해 거래내용에 대한 인증을 받는다. 블록의 위변조 여부를 판단하기 위해 트랜잭션이 모인 블록의 해시를 만들게 되며, 이 해시는 이전 블록의 해시를 포함하고 그림 1처럼 논리적으로 연결되어 있어 블록체인을 이룬다.



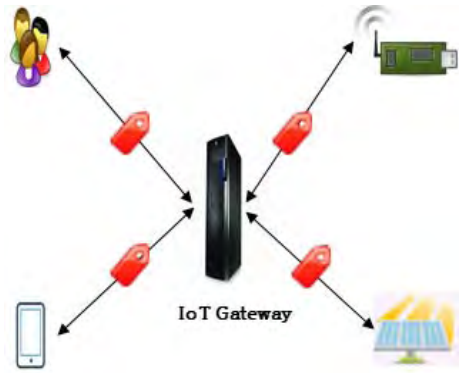
(그림 1) 블록체인 개념도[3]

비트코인에서 작업증명은 다수의 의사 결정을 통해 작업에 대한 인증을 수행하는데 하나의 장치(CPU)가 하나의 작업에 대해 한 번의 의사결정을 수행할 수 있도록 한다[3]. 이로 인해 다수의 장치를 가지거나, 다수의 의견을 모을 수 있는 누군가로 인한 위변조를 피할 수 없다는 문제를 갖기 때문에 충분히 많은 참여자를 포함한 분산 인프라에 적합하다.

1) 본 논문은 한국전력공사지원 스마트 에너지 캠퍼스 사업으로 지원된 연구임.

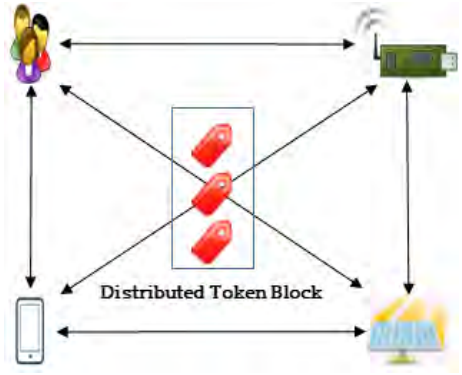
2.2 블록체인 기반 분산형 IoT 접근제어 시스템

IoT 보안 플랫폼 환경에서 접근제어는 그림 2와 같이 게이트웨이 또는 중앙 인증 서버를 통하여 중앙집중적인 접근제어 서비스가 수행되었다[1]. 이러한 시스템에서 사용자는 게이트웨이를 통해 토큰을 발행받고, 또한, 게이트웨이를 통해 리소스에 대한 서비스를 제공받았다. 이러한 환경에서는 장치가 많아질수록 게이트웨이가 발행하는 토큰의 수는 상대적으로 비례하며, 이에 대한 관리 기술 및 부하가 과도하게 발생할 수 있다.



(그림 2) Gateway 기반 중앙형 IoT 접근제어 시스템

본 연구에서는 그림 3과 같이 블록체인을 이용한 분산 토큰 블록을 구성하여 다수의 참여자의 인증을 통하여 토큰의 생성, 위임, 폐기 과정을 수행할 수 있는 블록체인 기반 분산형 IoT 접근제어 시스템을 제안하였다.



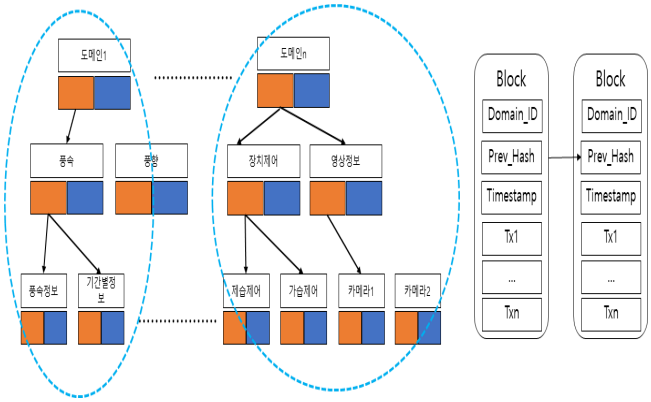
(그림 3) 블록체인 기반 분산형 IoT 접근제어 시스템

제안된 시스템에서 모든 장치, 사용자는 작업증명에 참여할 수 있는 주체가 될 수 있으며, 서비스를 제공하는 장치들은 리소스가 된다. 모든 참여자는 토큰의 작업증명 과정에 동일한 참여권을 갖을 수 있으며, 각 참여자는 블록을 저장할 수 있는 저장소를 유지하여야 한다. 토큰의 트랜잭션은 기존 IoT 접근제어 시스템의 토큰 생성, 위임, 폐기를 포함하며, 토큰은 리소스에 대한 접근권한을 포함한다.

기존의 블록체인이 가상화폐에 대한 트랜잭션 작업에 국한되어 있다면, 제안된 시스템에서 블록체인은 다양한 리소스에 대한 접근 권한을 포함하고 있기 때문에 단일 블록체인으로 모든 정보를 유지하는데에는 한계가 있을 수 있다. 또한, IoT 환경내의 장치는 대용량의 블록체인의 저장을 위한 공간 확보 및 처리에는 어려움이 있을 수 있어 본 연구에서는 멀티 블록체인을 구성하고자 한다.

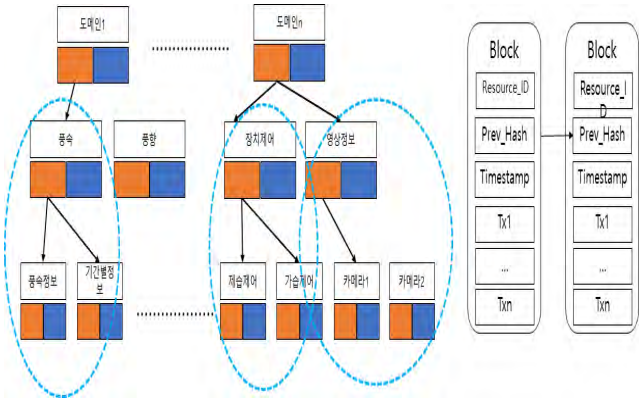
기존 연구[1]를 통하여 IoT 보안 플랫폼내 리소스들을 도메인으로 분류하였으며, 이를 이용하여 멀티 블록체인은 크게 두 가지 방법으로 구성할 수 있다.

첫 번째는 그림 4와 같이 IoT 환경내의 리소스에 대해 도메인별 분류를 하고 도메인별로 블록체인을 구성하는 방법이다. 이 방법에서 블록들은 도메인 식별자 (Domain _ID)를 갖으며, 도메인 내 토큰에 대한 트랜잭션들로 구성될 수 있다. 이 방법은 어떤 리소스들을 하나의 도메인으로 관리할 것인가의 문제를 포함하고 있어, 중앙집중형과 분산형의 결합된 방법으로 처리될 수 있다.



(그림 4) 도메인 기반 블록체인 구성

두 번째는 그림 5와 같이 IoT 환경내의 리소스별로 블록체인을 구성하는 방법이다. 이 방법에서 블록들은 리소스 식별자 (Resource _ID)를 갖으며, 리소스에 대한 토큰에 대한 트랜잭션들로 구성될 수 있다. 이 방법은 완전히 분산된 접근제어 방식이나, 리소스가 많을수록 체인의 수가 많아질 수 있으며, 이에 대한 리소스의 저장공간의 처리를 어떻게 할 것인가의 문제를 해결할 수 있어야 한다.



(그림 5) 리소스 기반 블록체인 구성

리소스 기반 블록체인 구성방법은 도메인내의 리소스들만으로 작업증명을 수행하는 방법으로 저장공간의 문제를 해결할 수 있을 것으로 보인다.

3. 결론

본 연구에서는 블록체인의 분산 트랜잭션 인증 기법을 적용하여 토큰의 발행, 위임, 폐기 과정에서 IoT 환경내 참여 기기간에 인증이 이루어지는 접근제어 모델을 제시하였다.

이를 위하여 도메인 기반 블록체인 구성 방법과 리소스 기반 블록체인 구성 방법을 제안하였으며, 추후 상세 아키텍쳐 설계 및 시스템 구현에 대한 연구를 진행하여 시스템의 보안성을 평가할 것이다.

참고문헌

[1] Jin-Bo Kim, Deresa Jang, Mi-Sun Kim and Jae-Hyun Seo, "The Access Control platform of the IoT Service using the CapSG",KIPS Tr.Software and Data Eng., Vo1 4, No 9, pp. 337-346, 2015.

[2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, bitcoin.org, 2009.

[3] A. Ouaddah, A. Abou Elkalam and A. Ait Ouahman, “FairAccess: a new Blockchain-based access control framework for the Internet of Things”, Security and Communication Networks, pp. 5943-5964, 2017.