다중 도메인 IoT 환경에서 블록체인 기반 접근제어 토큰 보안 강화를 위한 시스템

서아영, 허가빈, 도인실
이화여자대학교

ayg0418@ewhain.net, gjrkqls@ewhain.net, isdoh1@ewha.ac.kr

Enhancing Security of Blockchain-Based Access Control Token in Multi-Domain IoT Environment

Ahyoung Seo, Gabin Heo, Inshil Doh
Ewha Womans Univ.

요 약

한정된 자원을 가진 IoT 기기들이 다중 도메인 환경에서 작동하고, 서로 다른 도메인 간 상호 의존성이 늘어나면서 다중 도메인 IoT 환경에서 데이터 공유 시 적용할 수 있는 접근제어 시스템의 필요성이 대두되었다. 이에 대응하여 접근제어 토큰을 이용하여 다중 도메인 환경에서 자동적인 접근제어를 수행하는 IoT 기기를 위한 컨소시엄 블록체인 기반 접근제어 시스템이 제안되었으나, 여전히 토큰을 이용한 공격과 프라이버시 문제의 가능성이 존재한다. 본 연구에서는 다중 도메인 IoT 환경에서 동작하는 블록체인 기반 접근제어 토큰의 보안 강화를 위한 시스템을 제안한다. 제안 시스템은 IPFS(InterPlanetary File System)와 관리자 블록체인, 접근제어 토큰 관련 내용을 기록하는 블록체인을 활용하여 토큰 프라이버시를 보호하고 가능한 공격을 방지하는 토큰 기반 접근제어를 수행한다.

Ⅰ. 서 론

IoT(Internet of things) 기기들은 한정된 저장공간과 네트워크 및 컴퓨팅 능력으로 접근제어를 포함하여 복잡한 보안 솔루션을 적용하는 것에 어려움이 있다. 또한, 서로 다른 도메인 간의 상호 의존성이 증가하면서 다른 도메인에 존재하는 기기 간 데이터 공유의 필요성과 접근제어 수행의 필요성 또한 증가하였다. 이러한 필요성을 바탕으로 IoT 기기들의 상호 작용을 위하여 컨소시엄 블록체인을 기반으로 복잡한 인증 과정을 단순화한 연구가 진행되고 있다. 하지만, 해당 시스템은 접근제어 정책과 접근제어 토큰을 블록체인에 저장하여 컨소시엄 블록체인을 구성하는 모든 노드가 이에 접근할 수 있다는 점에서 프라이버시 문제가 존재한다[1]. 또한, 특정 기기가 자신의 것이 아닌 토큰을 악용하여 지속적인 통신 요청을 함으로써 IoT 기기의 오버헤드를 증가시키는 공격이 가능하다는 문제가 존재한다. 따라서, 본 연구에서는 블록체인을 이용하여 데이터 공유 과정에서의 인증 복잡성 축소 및 single point of failure 문제 해결을 수행하면서도 프라이버시를 보호하고 공격을 방지하는 시스템을 설계하고자 한다.

Ⅱ. 관련 연구

블록체인과 접근제어는 두 종류의 관점에서 연구되고 있다. 첫 번째로 블록체인의 내용에 누구나 접근할 수 있다는 프라이버시 문제를 보완하기 위해 블록체인에 대한 접근제어 방법이 연구되고 있다. 두 번째로 single point of failure 문제를 해결할 수 있고, 감시가 가능하다는 블록체인의 장점을 활용하여 블록체인, 스마트 계약을 이용하여 접근제어를 구현하는 방법에 대한 연구가 진행되고 있다.

Hao 등은 블록체인과 접근제어 토큰을 기반으로 IoT 기기에서 동작하는 다중 도메인 접근제어 방법을 제안하였다[1]. IoT 기기들은 다른 IoT 기기에 데이터를 요청하고자 할 때, 블록체인 네트워크로부터 접근 권한을 검증받은 뒤 토큰을 발급받고, 토큰을 이용하여 다른 기기에 직접 데이터를 요청한다. 해당 시스템은 중앙 집중 환경에서 IoT 기기들이 데이터 공유를 수행할 때 필요한 복잡한 인증 과정을 컨소시엄 블록체인을 통해 단순화하였다. 하지만, 접근제어 정책, 접근제어 토큰을 통한 권한 부여 내용, 토큰 등을 모두 블록체인에 추가하여 프라이버시 문제가 존재한다.

Steichen 등은 프라이버시 문제로 민감한 데이터를 IPFS를 이용하여 공유할 수 없다는 문제를 해결하기 위하여 이더리움 스마트 계약을 기반으로 접근제어 기능을 추가한 IPFS인 ACL-IPFS를 제안하였다[2]. 해당 연구에서는 ACL(Access Control List)를 관리하는 ACL network라는 요소를 소개하였지만, 본 연구에서는 접근제어 토큰 관련 블록체인이 토큰 발급에 대한 기록과 감시뿐만 아니라 ACL의 역할을 할 수 있도록 하였다.

Ⅲ. 다중 도메인 IoT 환경에서 블록체인 기반 접근제어 토큰 보안 강화를 위한 시스템

본 연구에서는 IPFS (InterPlanetary File System)과 접근제어 정책을 기록하는 관리자 블록체인, 접근제어 토큰에 관련된 블록체인을 활용하여 프라이버시를 보호하면서도 토큰을 악용한 공격을 방지할 수 있는 접근제어 토큰 기반 다중 도메인 IoT 환경에서의 접근제어 시스템을 제안한다. 속성 기반 접근제어는 속성의 유연성과 정교함을 바탕으로 도메인 간 접근제어 수행이 편리하다는 장점이 있으므로 해당 시스템은 속성 기반 접근제어를 수행한다.

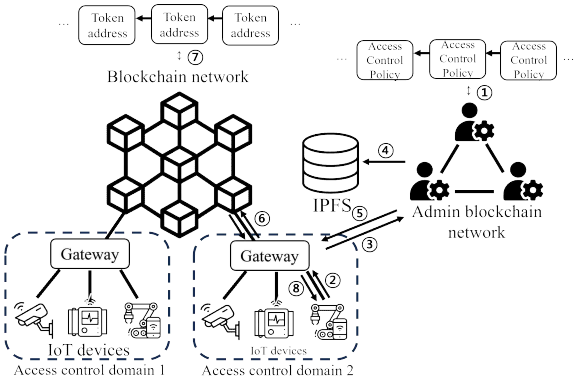
3.1. 제안 시스템 개요

제안 시스템의 개요는 다음과 같다. 블록체인 네트워크는 충분한 저장공간과 컴퓨팅 능력을 갖춘 노드들로 구성된 컨소시엄 블록체인 네트워크이며 PBFT (Practical Byzantine Fault Tolerance) 합의 알고리즘을 사용하여 합의를 수행한다. 본 연구에서는 PBFT 합의 알고리즘에서 선정된 리더 노드를 primary 노드라고 정의한다. 해당 블록체인 네트워크가 관리하는 블록체인에는 발급된 접근제어 토큰에 대한 정보와 해당 토큰에 대한 요청 내용이 저장된다. 이를 통해 토큰의 주소와 소유자를 저장함으로써 토큰 발급 내용을 관리하고, IoT 기기가 접근제어 토큰을 요청하였을 때 블록체인의 내용을 확인하여 토큰의 소유자에게만 토큰을 전달할 수 있도록 한다. 또한, 토큰 요청 내용을 저장하여 잘못된 토큰 요청에 대한 감시가 가능하게 한다. 게이트웨이는 IoT 기기들이 관리자 블록체인에 토큰 발급 및 전달을 요청하고, 블록체인에 접근할 수 있도록 돕는 기능을 추가로 수행하는 컨소시엄 블록체인 네트워크 내 노드 중 하나이다. IoT 기기들은 토큰의 발급 및 전달, 그리고 데이터 공유를 요청하는 주체이며, 각 IoT 기기는 특정 접근제어 도메인에 포함된다. 관리자 블록체인 네트워크는 접근제어 정책을 관리하는 관리자들로 구성된 블록체인 네트워크이다. 각 접근제어 도메인을 관리하는 관리자들이 프라이빗 블록체인 네트워크를 구성한 결과이다. 관리자 블록체인 네트워크가 관리하는 프라이빗 블록체인에는 각 IoT 기기 혹은 접근제어 도메인의 속성과 접근제어 정책이 정의되어 있다. 접근제어 도메인의 관리자가 많지 않고, 관리자 블록체인 네트워크는 접근제어 속성 및 정책을 수립하고 수정하는 과정에서만 블록을 추가하므로 많은 자원이 필요하지 않다. IPFS는 접근제어 토큰

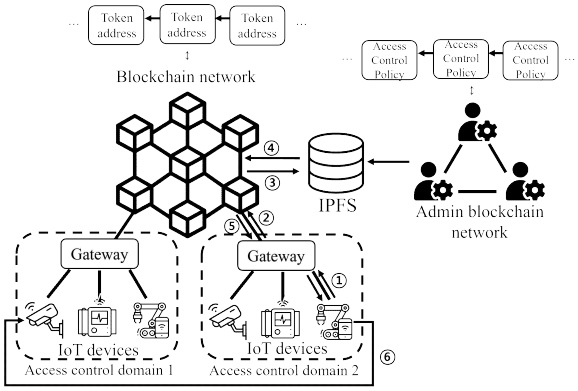
이 실질적으로 저장되는 저장소이다.

3.2 시스템 동작 과정

해당 시스템은 접근 권한과 접근제어 정책 수립 과정, 접근제어 수행 과정으로 동작하며, 접근제어 수행 과정은 다시 토큰 발급, 토큰 요청 및 전달, 데이터 요청 과정으로 나눌 수 있다.



[그림 1] 접근제어 정책 수립 및 토큰 발급



[그림 2] 토큰 요청과 전달 및 데이터 요청

3.2.1. 접근제어 정책 수립 및 토큰 발급

[그림 1]은 접근 권한과 접근제어 정책 수립 및 토큰 발급 과정을 보여준다. 해당 과정은 다음과 같이 진행된다.

① 관리자 블록체인 네트워크는 각 IoT 기기의 속성을 정의하고, 특정 IoT 기기나 접근제어 도메인에 데이터를 요청할 수 있는 기기 혹은 도메인의 속성을 정의함으로써 접근제어 정책을 생성한다. 해당 정책은 관리자 간의 합의를 통해 프라이빗 블록체인인 관리자 블록체인에 보관된다. 추가적인 블록을 생성함으로써 기존의 접근제어 정책을 수정할 수 있다.

② IoT 기기가 다른 IoT 기기에 데이터를 요청하기 위해서는 접근제어 토큰을 발급받아야 한다. 데이터를 요청하고자 하는 IoT 기기는 자신이 속한 도메인의 게이트웨이에 토큰 발급을 요청한다. 이때, 접근하고자 하는 접근제어 도메인과 기기 정보, 자신에 대한 연결 정보를 서명한 내용과 공개키를 함께 전달한다.

③ 게이트웨이는 전달받은 내용을 바탕으로 관리자 블록체인 네트워크에 토큰 발급을 요청한다.

④ 관리자 블록체인 네트워크의 primary 노드는 관리자 블록체인에 저장된 접근 권한과 접근제어 정책을 기반으로 요청이 유효하다면 토큰을 생성한다. 해당 토큰에는 토큰 소유자의 접근 권한과 연결 정보와 관련된 내용이 포함되어 있다. 이후 IPFS에 토큰을 저장한다.

⑤ 관리자 블록체인 네트워크는 토큰이 저장된 주소와 토큰 소유자의 공개키를 토큰 발급을 요청한 게이트웨이에 리턴한다.

⑥ 주소와 공개키를 돌려받은 게이트웨이는 해당 내용을 블록체인 네트워크의 primary 노드에 전달한다.

⑦ 블록체인 네트워크는 전달받은 토큰 발급에 대한 내용을 PBFT 합의 알고리즘을 통해 검증하고, 토큰 소유자에 대한 정보와 함께 트랜잭션으로 기록한다.

⑧ 발급된 토큰의 소유자는 게이트웨이에 요청하여 블록체인에 기록된 토큰의 주소를 얻을 수 있다.

3.2.2 토큰 요청과 전달 및 데이터 요청

데이터를 요청하고자 하는 IoT 기기가 토큰을 사용하기 위해서는 토큰 요청 및 전달 과정이 필요하다. [그림 2]는 토큰 요청 및 전달, 그리고 IoT 기기가 토큰을 이용하여 다른 IoT 기기에 직접 데이터를 요청하는 과정을 보여준다.

① 다른 IoT 기기에 데이터를 요청하고자 할 때, IoT 기기는 게이트웨이를 통해 블록체인 네트워크에 이전에 발급받은 토큰을 요청한다. 이때 IoT 기기는 자신의 서명과 전달받고자 하는 토큰의 주소를 제시하여야 한다.

② 게이트웨이는 해당 요청을 블록체인 네트워크에 전달한다.

③ 블록체인 네트워크의 primary 노드는 전달받은 내용을 기반으로 토큰 전달 스마트 계약 트랜잭션을 발생시킨다.

④ 블록체인에 기록된 토큰 발급 내용에 따라 전달받은 서명을 검증하여 토큰을 요청한 IoT 기기가 소유자임이 확인되면 primary 노드는 IPFS에 저장된 토큰 정보를 가져온다.

⑤ primary 노드는 가져온 토큰 정보를 토큰 소유자의 공개키로 암호화하여 게이트웨이에 전달하고, 게이트웨이는 토큰 요청을 한 IoT 기기에 암호화된 토큰을 전달한다. 전달 내용은 블록체인에 기록한다.

⑥ 데이터를 요청하는 IoT 기기는 블록체인 네트워크로부터 전달받은 토큰을 자신의 비밀키로 복호화하여 데이터 요청에 사용한다. 토큰을 사용함으로써 일정 시간 동안 서로 다른 도메인에 속한 IoT 기기 간 직접적인 데이터 통신이 가능하다.

Ⅳ. 결 론

본 연구는 IPFS와 관리자 블록체인 네트워크, 블록체인 네트워크를 이용하여 프라이버시를 보호하고 가능한 공격을 방지하는 접근제어 토큰 기반 다중 도메인 IoT 환경에서 작동하는 속성 기반 접근제어 시스템을 제안하였다. 접근 권한과 접근제어 정책을 프라이빗 블록체인인 관리자 블록체인에 저장하여 접근제어 정책 관련 프라이버시 문제를 해결하였다. 토큰을 IPFS에 저장하고 블록체인에는 저장된 주소만 저장하여 소유자만 토큰을 열람하고 접근할 수 있도록 함으로써 토큰 프라이버시 문제를 해결하고, 다른 기기의 토큰을 악용하는 공격을 방지하였다.

향후 연구로 관리자 블록체인의 관리자가 늘어날 경우, 관리자 블록체인 네트워크의 성능을 향상할 수 있도록 관련 연구를 진행할 예정이다.

ACKNOWLEDGMENT

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2023R1A2C1005712) (교신저자: 도인실)

참 고 문 헌

[1] X. Hao, W. Ren, Y. Fei, T. Zhu and K. -K. R. Choo, "A Blockchain-Based Cross-Domain and Autonomous Access Control Scheme for Internet of Things," in IEEE Transactions on Services Computing, vol. 16, no. 2, pp. 773-786, 1 March-April 2023, doi: 10.1109/TSC.2022.3179727.

[2] M. Steichen, B. Fiz, R. Norvill, W. Shbair and R. State, "Blockchain-Based, Decentralized Access Control for IPFS," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1499-1506, doi: 10.1109/Cybermatics_2018.2018.00253.