IoT 환경에서 블록체인 기반 데이터 접근제어 시스템

이준영, 박기성*, 박요한**, 박영호

경북대학교, *한국전자통신연구원, **계명대학교

harry250@knu.ac.kr, ks.park@etri.re.kr*, yhpark@kmu.ac.kr**, parkyh@knu.ac.kr

Blockchain-based Data Access Control System in IoT Environment

Lee Joon Young, Park Ki Sung*, Park Yo Han**, Park Young Ho

Kyungpook National Univ., *Electronics and Telecommunications Research Institute, **Keimyung Univ.

요 약

최근 IoT 기기를 활용한 환경이 늘어남에 따라 IoT 데이터 생성량이 기하급수적으로 늘어나고 있다. 보편적인 IoT 환경은 클라우드를 통해 데이터가 관리되고 있으나 클라우드 환경은 중앙화 문제로 인해 단일 실패 지점에 매우 취약하며 데이터의 접근 제어에 어려움이 있다. 이를 해결하기 위해 블록체인 및 속성 기반 암호를 활용하여 탈중앙화 및 접근 제어를 제공하는 연구들이 진행되고 있다. 본 논문에서는 IoT 환경에서 데이터 접근 제어를 위한 블록체인 기반 시스템을 분석하여 문제점을 지적한 후 이를 해결하기 위한 시스템을 제안한다.

Ⅰ. 서 론

최근 IoT 기기를 활용한 스마트 시티가 개발됨에 따라 다양한 IoT 정보들이 생성되고 있다[1,2]. 보편적인 IoT 환경은 클라우드를 통해 데이터가 관리되고 있으나 데이터를 생성하는 사용자들의 정보에는 개인정보 등의 민감한 정보가 포함되어있다. 클라우드 환경은 중앙화 문제로 인해 단일 실패 지점에 매우 취약하며 데이터 관리에 취약한 문제점을 가지고 있다[3,4]. 따라서 데이터의 프라이버시 제공 및 접근제어를 위한 속성 기반 암호 연구가 필요하다. 또한 데이터 송·수신은 공개 채널을 통해 이루어지므로 공격자의 공격에 매우 취약하다. 이러한 문제점을 해결 하기 위해 블록체인을 활용하여 탈중앙화하는 연구가 진행되고 있으며 안전한 데이터의 송·수신을 위한 키 합의 및 인증 시스템 연구가 이루어지고 있다[5,6]. 본 논문에서는 IoT 환경에서 생성되는 데이터의 안전한 접근 제어 및 관리를 위한 시스템의 동향 및 문제점을 분석하며 문제점을 해결하기 위한 블록체인 기반 키 합의 및 인증방식의 방향을 제시한다.

Ⅱ. 배경 지식

속성 기반 암호 및 블록체인 기술의 자세한 설명은 다음과 같다.

2.1. 속성 기반 암호

속성 기반 암호 방식은 사용자와 관련된 특정 속성에 기반한 암호화를 통해 평문을 암호화하는 방식이다. 사용자의 신원을 기반으로 하는 신원 기반 암호 방식 (Identity Based Encryption)이 있으며 접근 구조의 위치에 따라 암호문에 대한 접근을 제어할 수 있는 KP-ABE (Key-policy Attribute Based Encryption) 및 CP-ABE (Ciphertext Policy Attribute Based Encryption)이 있다. KP-ABE는 데이터 송신자가 속성 집합으로 암호화를 하며 수신자는 복호키 생성 시 자신의 속성 집합을 바탕으로 접근 구조를 통해 암호문을 복호화한다. CP-ABE는 데이터 송신자가 암호문을 생성할 시에 접근 구조를 생성하여 수신자의 속성 집합을 바탕으로 복호화를 한다.

2.2. 블록체인

블록체인은 P2P (Peer-to-Peer) 네트워크를 기반으로 자신 및 트랜잭션의 레지스트리를 저장하는 데이터베이스 원장이다[7]. 블록체인은 탈중앙화, 분산, 공유 및 변경 불가능하다는 특징을 가진다. 원장의 모든 거래는 블록체인 네트워크에 존재하는 수만 개의 채굴 노드에 의해 디지털 서명화가 이루어지며 검증된다. 트랜잭션은 블록을 통해 그룹의 타임 스탬프 별로 저장되고 구성이 되며 이러한 블록은 서로 해시되어 블록체인을 형성하게 된다. 블록체인은 타원 곡선 암호화 (ECC) 및 SHA-2 해싱 체계를 사용하여 데이터 인증 및 무결성을 위한 강력한 암호화 증명을 제공한다.

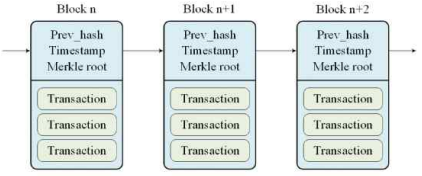

그림 1. 블록체인의 구조.

Ⅲ. IoT 환경에서 데이터의 접근 제어 및 관리를 위한 시스템

본 논문에서는 IoT 환경에서 블록체인을 기반한 데이터의 접근 제어 및 관리 시스템을 분석한다.

3.1. Ding 등이 제안한 시스템

2019년 Ding 등은 기존 네트워크의 구조는 복잡하며 방대함으로 인한 IoT 시스템의 새로운 보안 위협이 존재할 수 있다고 언급하였다. 그들은 데이터 보안을 보장하기 위해 기존의 출입 통제 기술은 복잡한 출입 관리 및 중앙 집중화로 인해 신뢰성이 부족하며 IoT 시스템에서 출입 통제를 관리하는 데 사용하기 적합하지 않다고 주장하였다. Ding 등은 IoT 시스템을 위한 새로운 속성 기반 출입 통제 방안을 제시하며 그 시스템 모델은 그림 2와 같다. 그들은 간소화를 위해 속성 기반 암호를 사용하며 단일 지점 실패 및 데이터 변조를 방지하기 위해 블록체인 기술을 사용한다. 그러나 Ding 등이 제안한 프로토콜은 사용자의 신원을 확인할 수 있는 자세한 인증 내용이 없으며 속성 기반 암호를 사용하지만 그에 관한 자세한 접근

정책 및 제어 방법의 설명이 부족하다.

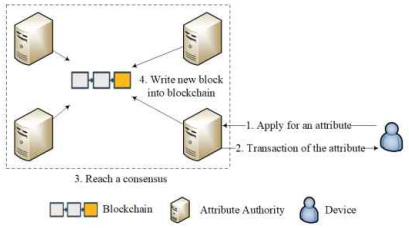

그림 2. Ding 등이 제안한 출입 통제 시스템.

3.2. Zhang 등이 제안한 시스템

2018년 Zhang 등은 IoT 장치에서 발생하는 데이터를 수집하고 제어하기 위한 기존의 클라우드 기반 시스템의 문제점을 지적하였다. 그들은 클라우드를 완전히 신뢰할 수 없으며 데이터 및 사용자의 개인 정보가 유출되고 손상될 위험이 있다고 주장하였다. 또한 클라우드 시스템에 대한 개인 정보 보호 데이터 처리 솔루션이 있지만 악의적인 클라우드 서비스 제공 업체 및 직원에 의해 공격에 취약하다고 주장하였다. 따라서 그들은 블록체인 모델과 속성 기반 암호화 시스템을 기반으로 세분화 된 액세스 제어를 통한 개인 정보 보호 및 사용자 제어 데이터 공유 시스템을 제안하였다. 그들의 체계에서 인증은 이전에 연구하였던 구조를 사용한다고 명시하였지만 제안한 시스템에서 적용 가능한지 여부에 대한 설명은 존재하지 않는다. 제안한 시스템에 적합한 인증 체계가 이루어지지 않으면 악의적인 사용자에 의해 시스템의 보안 위협이 발생할 수 있다.

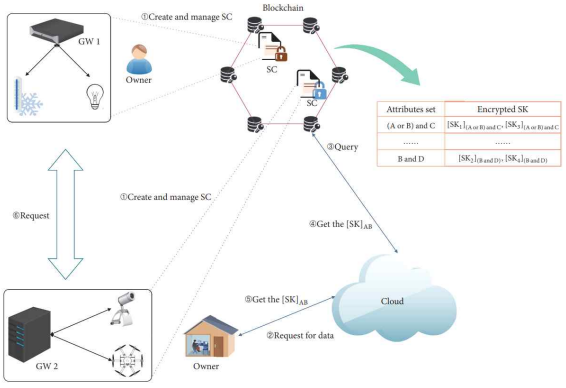

그림 3. Zhang 등이 제안한 데이터 공유 시스템.

Ⅳ. 제안 시스템

Ding 등 및 Zhang 등이 제안한 시스템은 IoT 환경의 데이터 접근 제어를 위한 블록체인 기반 보안 시스템이다. 그러나 그들이 제안한 시스템은 명확한 인증 및 접근 제어 체계가 존재하지 않아 유효한 사용자 및 데이터 정보인지 판단할 수 없다. 따라서 본 논문에서는 인증 및 접근 제어 시스템을 위해 아래 그림과 같은 시나리오 구성을 계획하며 자세한 사항은 다음과 같다.

· 등록 단계에서 게이트웨이 클라우드 및 매니저는 보안 채널을 통해 TA(Trusted Authority)에 등록한다.

· 인증 단계에서는 게이트웨이 클라우드 및 매니저가 서로를 인증하고 통신을 위한 세션 키를 생성한다.

· 인증 시 TA는 게이트웨이의 속성 정책 생성 및 업데이트를 한다.

· 게이트웨이는 IoT 환경에서 생성된 데이터를 속성 기반 암호화를 통해 클라우드에 업로드한다. 클라우드는 매니저가 블록체인의 속성에 맞는 데이터를 요청할 시 해당하는 데이터를 매니저에게 전달한다.

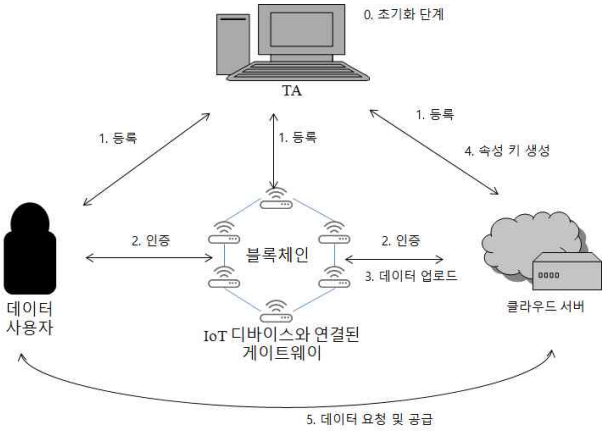

그림 4. IoT 환경에서 블록체인 기반 보안 데이터 접근제어 시스템.

· 매니저는 인증을 완료한 후 TA에게 속성 키를 요구하며 이를 이용해 클라우드에 저장된 데이터를 요청한다.

Ⅴ. 결론

최근 IoT 데이터를 관리 및 공유하기 위한 연구가 활발히 이루어지고 있다. 본 논문에서는 Ding 등 및 Zhang 등이 제안한 시스템을 분석하여 그들이 제안하는 시스템은 인증 및 접근 제어에 대해서 자세히 다루지 않으며 이는 악의적인 사용자 및 클라우드 서버 등에 의해 시스템의 보안 위협이 발생할 수 있는 문제가 있다. 이러한 문제점을 보완하여 본 논문에서는 인증 및 접근 제어를 위한 시스템을 제안하였으며 향후 제안하는 시스템을 기반으로 보안 프로토콜 개발을 진행할 것이다.

참 고 문 헌

[1] Lee, J., Yu, S., Park, K., Park, Y., and Park, Y. “Secure Three-Factor Authentication Protocol for Multi-Gateway IoT Environments,” Sensors, vol. 19, no. 10, pp. 1-25, 2019.

[2] Park, Y., and Park, Y. “Three-Factor User Authentication and Key Agreement Using Elliptic Curve Cryptosystem in Wireless Sensor Networks,” Sensors, vol. 16, no. 12, pp. 1-17, 2016.

[3] Kim, M., Yu, S., Lee, J., Park, Y., and Park, Y. “Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain,” Sensors, vol. 20, no. 10, pp. 1-21, 2020.

[4] Son, S., Lee, J., Kim, M., Yu, S., Das A. K., and Park, Y. “Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain,” IEEE Access, vol. 8, pp. 192177-192191, 2020.

[5] Ding, S., Cao, J., Li, C., Fan, K., and Li, H. “A novel attribute-based access control scheme using blockchain for IoT,” IEEE Access, vol. 7, pp. 38431-38441, 2019.

[6] Zhang, Y., He, D., and Choo, K. K. R. “BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT,” Wireless Communications and Mobile Computing, vol. 2018, 2018.

[7] Underwood, S. “Blockchain beyond bitcoin,” Communications of the ACM, vol. 59, no. 11, pp. 15-17, 2016.