클라우드 기반 IoT 환경에서 데이터 프로비넌스 및 접근 제어 시스템 설계

배태모[1], 방지원[2], 최미정[1, 2, 3, *]

[1]강원대학교 컴퓨터공학과

[2]강원대학교 빅데이터메디컬융합과

[3]강원대학교 데이터사이언스학과

{tm3693, jiwonbang, mjchoi}@kangwon.ac.kr

Design of a Data Provenance and Access Control System in Cloud-Based IoT Environment

Taemo Bae[1], Jiwon Bang[2], Mi-jung Choi[1, 2, 3, *]

[1]Dept. of Computer Science and Engineering, Kangwon National Univ.

[2]IGP. of Medical Bigdata Convergence, Kangwon National Univ.

[3]Dept. of Data Science, Kangwon National Univ.

요 약

클라우드 (Cloud) 기반 IoT (Internet of Things) 환경에서는 다수의 기기에서 생성되는 대규모 데이터의 무결성과 기밀성을 보장하기 위한 접근 제어가 필수적이다. 본 논문은 이를 해결하기 위해 블록체인 (Blockchain) 기반 데이터 프로비넌스 (Data Provenance) 및 접근 제어 시스템을 제안한다. 제안 시스템에서 IoT 장치와 클라우드 사이에 위치한 Fog 노드는 블록체인 노드를 유지하며, 데이터의 생성·수정 이력을 기록하고 머클 트리 (Merkle Tree)를 통해 무결성을 검증한다. 또한 DID (Decentralized Identifier)와 VC/VP (Verifiable Credential/Verifiable Presentation)를 활용한 분산형 접근 제어로 장치 및 사용자 권한을 관리하여 기밀성을 강화한다. 이를 통해 블록체인과 분산 신원 기반 접근 제어를 결합하여 클라우드 기반 IoT 환경의 신뢰성과 보안성을 향상시킨다.

Ⅰ. 서론

IoT (Internet of Things)는 카메라나 센서 등의 모듈을 통해 실시간 데이터를 생성·활용하는 기술이다. 그러나 IoT 장치는 계산 능력과 저장 공간이 제한되어, 대규모 데이터의 장기 저장이나 복잡한 분석이 어렵다. 이러한 한계를 보완하기 위해, 인터넷을 통해 스토리지와 서버 자원을 제공하는 클라우드 컴퓨팅 (Cloud Computing)과 결합되어 활용된다. 하지만 클라우드 기반 IoT 환경에서는 데이터 무결성과 접근 제어 측면의 보안 문제가 발생한다 [1]. IoT 장치는 물리적 환경에서 데이터를 수집하므로, 수집된 데이터가 전송이나 저장 과정에서 변조되지 않도록 무결성을 보장하는 것이 중요하다. 무결성이 훼손될 경우, 실시간 제어 시스템에서 오작동이 발생할 수 있다. 또한 다수의 이기종 장치와 사용자가 연결되는 개방형 구조로 인해 인증되지 않은 접근이나 내부자 공격의 위험이 존재하며, CSP (Cloud Service Provider)가 데이터를 임의로 변경하거나 삭제할 가능성도 있다 [2][3]. 따라서 데이터 무결성과 접근 제어는 클라우드 기반 IoT 환경에서 신뢰성과 안정성을 유지하기 위한 핵심 요건이다.

본 논문에서는 블록체인 (Blockchain) 기반 데이터 프로비넌스 (Data Provenance) 시스템을 제안한다. 블록체인은 분산 노드가 합의를 통해 데이터의 정당성을 검증하는 기술이며 [4], 데이터 프로비넌스는 데이터 생성부터 접근 이력까지를 추적해 신뢰성을 보장한다 [5]. 제안 시스템은 데이터 프로비넌스를 머클 트리 (Merkle Tree) [6]에 저장하고, 루트 해시만 블록체인에 기록한다. 또한 DID (Decentralized Identifier)와 VC/VP (Verifiable Credential/Verifiable Presentation)를 이용해 신원 인증과 접근 제어를 수행한다.

Ⅱ. 관련 연구

클라우드 기반 IoT 환경에서 데이터 무결성을 보장하기 위해 데이터 프로비넌스 (Data Provenance)를 적용한 연구가 활발히 진행되어 왔다. Jaigirdar et al.은 IoT 데이터 전송 과정에서의 투명성 부족과 신뢰성 문제를 해결하기 위해, 데이터의 생성·이동 등 이력을 기록한 프로비넌스 그래프에 보안 메타데이터를 통합한 보안 인식형 프로비넌스 그래프 (Secure-Aware Provenance Graph)를 제안하였다. 이를 통해 DoS나 악성 코드 삽입 등의 공격을 탐지·진단하고, 데이터의 신뢰성을 검증할 수 있는 근거를 제공하였다. 그러나 해당 연구는 CSP를 신뢰할 수 있다고 가정하였으며, 신원 인증 기반의 접근 제어는 고려하지 않았다 [7]. Pajooh et al.은 IoT 기기에서 수집된 데이터를 클라우드에 저장하는 환경에서 데이터 프로비넌스를 보장하기 위한 3계층 구조의 시스템을 제안하였다. 시스템은 데이터 생성 및 서명을 수행하는 IoT 계층, 데이터 무결성을 위해 로그를 기록하고 정책을 검증하는 블록체인 계층, 그리고 원본 데이터를 저장·분석하는 빅데이터 계층으로 구성된다. 하지만 이 연구 역시 신원 인증과 접근 제어에 대한 고려가 부족하다는 한계를 가진다 [8].

Ⅲ. 시스템 설계

본 논문에서 제안하는 시스템의 전체 구조는 그림 1과 같다. IoT 기기는 카메라와 센서 등 다양한 모듈을 통해 데이터를 생성·수집한다. 게이트웨이는 IoT 기기에서 수집된 데이터를 집계하고 필터링하며, 전송 전 정규화와 암호화를 수행한다. 또한 IoT 기기와 Fog 컴퓨터 간의 통신을 중계하고, IoT 기기의 토큰을 관리한다. Fog 컴퓨터는 블록체인 노드를 유

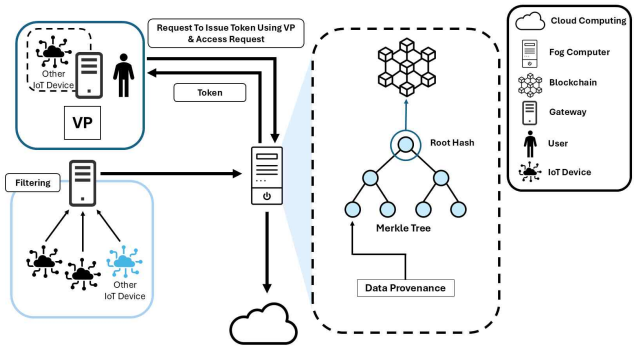

그림 1. 제안 시스템의 구조

지하면서 VP 검증을 통한 토큰 발급, 데이터 프로비넌스 생성, 머클 트리 구성 및 블록체인에 루트 해시 기록을 담당한다. 마지막으로 클라우드 컴퓨팅은 수집된 원본 데이터를 저장한다.

제안 시스템은 검증, 저장, 사용의 세 단계로 동작한다. 첫 번째 단계는 검증 단계로, VP를 이용해 접근 제어용 토큰을 발급받는 과정이다. DID와 VC/VP는 W3C (World Wide Web Consortium)에서 제안한 디지털 신원 인증 기술로, DID는 사용자가 직접 생성할 수 있으며 [9], VC는 학교나 기업 등 신뢰 기관으로부터 발급받는다. 사용자는 필요한 VC들을 조합하여 자신의 신원을 증명하는 VP를 생성한다 [10]. 본 시스템에서 저장된 데이터를 사용하는 주체는 사용자와 다른 IoT 기기이며, IoT 장치 소유자는 읽기·수정·삭제 권한을, 데이터 사용자는 읽기 권한만 가진다. 사용자와 IoT 장치는 생성한 VP를 Fog 컴퓨터에 제출하고, Fog 컴퓨터는 이를 검증한 후 토큰을 발급한다. VP 기반의 신원 인증과 토큰 기반의 접근 제어를 통해 데이터 기밀성을 보장한다. 두 번째 단계는 저장 단계로, IoT 장치가 수집한 데이터를 게이트웨이를 통해 Fog 컴퓨터로 전송한다. 게이트웨이는 데이터를 필터링·정규화·암호화한 뒤 IoT 장치의 토큰과 함께 전달한다. Fog 컴퓨터는 데이터를 바탕으로 머클 트리를 생성하고, 루트 해시를 블록체인에 기록하여 데이터의 위·변조 여부를 검증한다. 원본 데이터는 클라우드 컴퓨팅 환경에 안전하게 저장된다. 세 번째 단계는 사용 단계로, 사용자나 다른 IoT 장치가 저장된 데이터를 활용하는 과정이다. 데이터 요청 시, 주체는 검증 단계에서 발급받은 토큰을 Fog 컴퓨터에 제출한다. Fog 컴퓨터는 조작되었거나 유효하지 않은 토큰을 차단하고, 승인된 요청만을 처리하여 그 내역을 머클 트리에 반영함으로써 데이터 프로비넌스를 생성한다.

제안 시스템의 전체 동작 흐름은 그림 2에 나타나 있다. IoT 기기가 데이터를 생성해 게이트웨이로 전송하면, 게이트웨이는 이를 필터링·정규화·암호화 후 Fog 컴퓨터로 전달한다. Fog 컴퓨터는 VP를 검증하고 데이터 프로비넌스를 생성한 뒤, 클라우드 컴퓨팅에 원본 데이터를 저장한다.

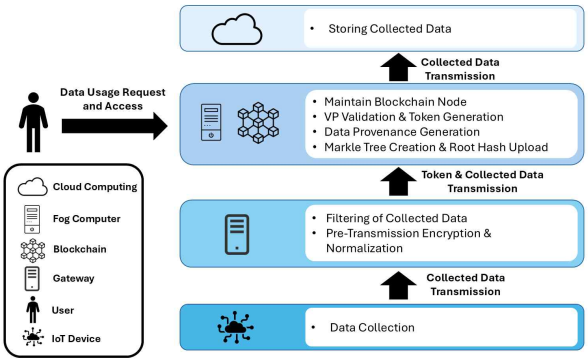

그림 2. 제안 시스템의 전체적인 흐름

Ⅳ. 결론 및 향후 연구

본 논문에서는 클라우드 기반 IoT 환경에서 데이터 무결성과 접근 제어를 보장하기 위한 시스템을 제안한다. Fog 컴퓨터는 수집된 데이터를 기반으로 데이터 프로비넌스 정보를 생성하고, 이를 머클 트리에 기록한 후 루트 해시를 블록체인에 업로드한다. 또한, VP를 이용한 신원 인증을 통해 접근 제어를 수행하며, 데이터 접근 및 변경 이력을 머클 트리에 기록함으로써 데이터의 무결성과 신뢰성을 보장한다. 향후 연구로는 제안 시스템의 실제 구현을 진행할 예정이다. 또한, 데이터 읽기·수정·삭제 요청이 빈번하게 발생하는 경우 블록체인의 낮은 TPS (Transactions Per Second)로 인해 지연이 발생할 수 있으므로, 이를 개선하는 방법을 찾을 생각이다.

ACKNOWLEDGMENT

논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 지역지능화혁신인재양성사업임(IITP-2025-RS-2023 00260267)

참 고 문 헌

[1] M. Almutairi, T. F. Sheldon, “IoT - Cloud Integration Security: A Survey of Challenges, Solutions, and Directions,” *Electronics 2025,* Vol. 14, No. 7, pp. 1 - 28, Mar. 2025..

[2] X. Mu and M. F. Antwi-Afari, “The applications of Internet of Things (IoT) in industrial management: a science mapping review,” *International Journal of Production Research,* Vol. 61, No. 5, pp. 1928 - 1952, Dec. 2024..

[3] P. Goswami, N. Faujdar, S. Debnath, A. K. Khan, and G. Singh, “Investigation on storage level data integrity strategies in cloud computing classification, security obstructions, challenges and vulnerability,” *Journal of Cloud Computing,* Vol. 13, No. 45, pp. 1 - 23, Feb. 2024.

[4] M. Di Pierro, “What is the blockchain,” *Computer in Science & Engineering,* Vol. 19, No. 5, pp. 92 - 95, Sep. 2017.

[5] Y. L. Simmhan, B. Plale and D. Gannon, “A survey of data provenance in e-Science,” *ACM Sigmod Record,* Vol. 32, No. 3, pp. 31 - 36, Sep. 2005.

[6] G. Tripathi, M. A. Ahad and G. Casalino, “A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges,” *Decision Analytics Journal,* Vol. 9, pp. 1 - 21, Dec. 2023.

[7] F. T. Jaigirdar, B. Tan, C. Rudolph and C. Bain, “Security-aware provenance for transparency in IoT data propagation,” *IEEE Access,* Vol. 11, pp. 55677 - 55691, May. 2023.

[8] H. Honar Pajooh, M. A. Rashid, F. Alam and S. Demidenko, “IoT Big Data provenance scheme using blockchain on Hadoop ecosystem,” *Journal of Big Data,* Vol. 8, No. 114, pp. 1 - 26, Aug. 2021.

[9] “Decentralized identifiers(DIDs) v1.0,” W3C, Jul. 2022. [Online]. Available: https://www.w3.org/TR/did-1.0/. Accessed: Sep. 19. 2025.

[10] “Verifiable credentials data model v2.0,” W3C, Sep. 2024. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0. Accessed: Sep. 21, 2025.