TPM 기반 ECC-DAA 익명 인증을 적용한 DAG-PBFT IoT 원장 설계 및 프로토타입 구현

김현준* 서화정**

*한성대학교 (대학원생)
**한성대학교 (교수)

TPM-Backed Anonymous Attestation for a DAG-Based IoT Ledger with PBFT Consensus

Hyun-Jun Kim*, Hwa-seong Seo**

*Hansung University(Graduate student)

**Hansung University(profesor)

요 약

4차 산업혁명 시대에 사물인터넷(IoT) 기기의 급격한 확산으로 인해 대규모 데이터 교환과 기기 간 협업이 필수가 되었다. 그러나 기기가 증가함에 따라 해킹, 무단 침입, 데이터 위·변조 등 보안 위협이 심화되는 문제가 발생한다. 기존 중앙 서버 구조로는 단일 실패 지점(SPoF, Single Point of Failure)과 확장성 문제를 완전히 해결하기 어렵다. 이에 따라 분산원장(Blockchain) 기술이 보안 대안으로 주목받고 있으나, 전통적인 체인 구조 블록체인은 트랜잭션 처리 속도와 확장성 측면에서 한계가 있다. 본 연구에서는 DAG(Directed Acyclic Graph) 구조를 적용한 분산원장과 TPM(Trusted Platform Module) 기반 ECC-DAA(Direct Anonymous Attestation)를 결합하여, IoT 환경에서 기기의 익명 인증과 안전성을 보장하고 PBFT(Practical Byzantine Fault Tolerance) 합의를 통해 높은 처리량(TPS)과 빠른 트랜잭션 확정(Finality)을 달성하는 방법론을 제안한다. 시뮬레이션 TPM 모듈(ibmtpm)을 사용한 프로토타입 구현 통해 제안 아키텍처의 가능성과 보완점을 검토한다.

I. 서론

사물인터넷(IoT) 기기의 급증과 함께 스마트 공장, 자율주행 차량, 스마트 홈 등 다양한 산업 현장에서 센서 데이터를 활용하는 사례가 늘고 있다. 이러한 데이터는 산업 자동화, 교통 관리, 환경 모니터링 등에서 핵심적 역할을 수행한다. 하지만 기기가 증가하고 연결성이 복잡해질수록 해킹, 무단 침입, 위·변조 등의 보안 위협이 함께 증대된다. 전통적인 중앙 서버 기반의 구조는 단일 취약점이 전체 서비스를 마비시킬 수 있고, 트래픽 폭주 상황에서 서버 확장에 한계를 보인다. 이에 따라 데이터 위·변조를 근본적으로 방지하기 위한 분산원장 기술이 각광받고 있지만, 기존 체인 구조는 트랜잭션 처리 속도가 낮고 확장성이 제한되는 문제를 안고 있다. 이에 따라 기존 체인 기반 블록체인 대비 DAG 구조 연구가 최근 주목받고 있다.

IoT 환경에서는 기기가 생성하는 소규모 트랜잭션이 빈번하게 발생한다. 따라서 초당 수백~수천 건 이상의 트랜잭션을 실시간으로 처리할 수 있는 확장성이 요구되며, 동시에 각 기기가 신뢰할 수 있는 상태인지 확인하고 기기 식별 정보를 노출하지 않는 개인정보 보호(프라이버시)도 중요하다. 본 논문에서는 DAG 구조의 분산원장을 통해 확장성을 높이고, TPM 모듈을 통한 하드웨어 차원 보안과 ECC-DAA 기법을 접목하여 기기의 익명 인증과 무결성 확인을 동시에 구현하는 방안을 제시한다. 본 논문은 DAG 기반 구조로 확장성 제고, ECC-DAA를 통한 기기 익명성 및 무결성 보장, 프로토타입 실험으로 제안 아키텍처의 가능성과 보

완점을 검토한다.

II. 관련 연구

2.1 IoT 확산과 보안 위협

IoT 기기는 2025년 약 768억 대에 달할 것으로 전망되며, 다양한 산업에서 활용되고 있다[1]. 그러나 저성능, 저가 설계로 인해 보안 취약점이 증가하고 있다. 주요 위협은 데이터 유출·변조, DDoS 공격, 악성 펌웨어 주입 등이 있다. IoT는 무선 통신을 사용하므로 도청, 중간자 공격에도 취약하다. 특히 Mirai 봇넷 사례는 IoT 기기가 대규모 DDoS 공격에 얼마나 쉽게 악용될 수 있는지를 보여준다[2]. 또한, IoT 기기는 관리가 어렵고 업데이트가 드물어 취약점을 악용한 펌웨어 공격이 쉽게 일어날 수 있다[3]. 이를 해결하기 위해 경량 암호화, 분산형 보안 아키텍처, AI 기반 이상 탐지 등 새로운 접근법이 연구되고 있다[2].

2.2 DAG 분산원장

전통적 블록체인(비트코인, 이더리움)은 낮은 처리량(비트코인 7 TPS, 이더리움 20-30 TPS)과 높은 거래 지연으로 IoT에 적합하지 않다[24]. DAG 기반 원장은 개별 트랜잭션이 병렬로 처리되는 구조로, 확장성과 처리속도를 개선하여 IoT 환경에 적합한 대안으로 주목받고 있다. 특히 IOTA의 탱글(Tangle)은 거래 증가에 따라 네트워크가 더욱 안정되고 처리 속도가 향상되는 특성을 지니며, 미세 거래를 거의 제로 비용으로 처리한다. 최근 연구에서도 DAG 기술의 우수성이 확인되었으며, DAG 원장은 IoT 시스템에 대한 높은 처리 성능과 낮은 수수료를 제공한다고 보고되었다[4].

2.3 TPM과 DAA를 통한 보안

TPM은 하드웨어 기반 암호 프로세서로, 키 생성·보호 및 원격 인증을 통해 IoT 장치의 신뢰 기반을 제공한다[5]. 그러나 기본 원격 인증 방식은 기기 식별 정보가 노출되어 프라이버시 침해 우려가 있다. 이를 해결하기 위해 제안된 것이 DAA로, 익명 그룹 서명을 이용해 TPM의 신뢰성을 증명하면서도 개별 장치의 익명성을 보호한다[6]. TPM과 DAA 결합으로 스마트카, 전자결제 등에서 사용자의 프라이버시 보호가 가능하며, 블록체인이나 DAG 기반 DLT 시스템에서도 강력한 보안 및 프라이버시 보호 수단으로 평가받고 있다[6].

III. 제안 방법

3.1 설계 목표

본 연구는 익명성·확장성·최종성이라는 세 축을 동시에 만족하는 컨소시엄-규모 원장을 지향한다. 첫째, 트랜잭션 발신자의 실체적 신원을 숨기면서도 무결성만을 증명하기 위해 DAA 서명을 채택하였다. DAA는 “인증된 그룹 구성원”임을 증명하되 서명자의 개별 ID는 노출하지 않는다. 둘째, 거래를 DAG 구조에 기록함으로써 전통적인 선형 체인 대비 병렬 처리량을 극대화한다. 다중 IoT 디바이스가 동시다발적으로 지불이나 센서 데이터를 전송하더라도, 트랜잭션이 서로를 부모로 참조하며 독립적으로 확장될 수 있다. 셋째, DAG에 포함된 각 트랜잭션은 PBFT합의를 거쳐 2f+1개의 서명을 수집하면 최종 확정된다. 이를 통해 IoT-규모 네트워크에서도 짧은 왕복 지연 내에 거래 불변성을 확보한다.

3.2 아키텍처 개요

시스템은 응용 계층의 노드 모듈, 서명 계층의 DAA 엔진, 합의 계층의 PBFT 상태기계로 논리적으로 분리된다. 각 노드는 Flask REST API를 통해 트랜잭션 및 PBFT 메시지를 송수신하며 내부에 DAG 저장소(Node.DAG)와 합의 상태(PBFTState)를 유지한다. Transaction 객체는 송·수신 주소, 금액, 부모 해시 배열, DAA 서명을 포함한다. DAA 엔진은 외부 CLI(daa_sign_message, verify_daa_signature)를 통해 TPM에서 서명을 생성·검증하며, 검증 성공 시에만 트랜잭션이 DAG 상에 유효 엔트리로 삽입된다. 합의 계층에서는 Primary가 PREPREPARE 메시지로 트랜잭션을 제안하고, PREPREPARE 후, 노드들은 PREPARE를 브로드캐스트하고, 최종적으로 COMMIT 메시지를 교환하여 2f+1 확인 시 최종 확정한다..

3.3 트랜잭션 수명 주기

생성: 노드는 최신 확정 트랜잭션(tips) 1 - 2개를 부모로 선택하여 새로운 트랜잭션을 구성하고, 내용을 해시한 뒤 DAA 서명 파일을 첨부한다. 2) 전파: attach_transaction() 호출 후 이 트랜잭션을 인근 노드에 HTTP POST로 브로드캐스트한다. 3) 검증: 수신 노드는 서명을 즉시 verify_daa_signature로 검증하고, DAG 내에서 부모 관계를 확인한 뒤 임시 저장한다. 4) 합의: Primary가 PREPREPARE를 발행하면, 노드들은 PREPARE·COMMIT을 교환하며 PBFTState에 카운트한다. 2f + 1개의 COMMIT이 누적되면 해당 트랜잭션의 state가 1(확정)로 전이되며 DAG의 새로운 tip이 된다.

3.4 DAA 서명 모듈

DAA 엔진은 트랜잭션 정보를 합쳐 만든 메시지를 해시하고, 이에 대해 ECC-DAA(Elliptic Curve Direct Anonymous Attestation) 서명을 생성한다. 프로토타입에서는 tpm2-tss[7]와 ecc-daa 오픈 코드[8]를 활용하며, 소프트웨어 TPM(ibmtpm)을 통해 TPM 2.0 명령 인터페이스를 모사한다. 이 과정에서 개별 디바이스의 신원은 노출되지 않고, 검증자는 합법적인 ECC-DAA 그룹 멤버임만 확인할 수 있다. 이를 통해 대규모 IoT 디바이스 환경에서도 프라이버시(익명성)를 보장하면서도, 위조 서명에 의한 합의 교란은 차단할 수 있다.

IV. 프로토타입 구현

4.1 실험 환경

CPU	Intel(R) Core(TM) i5-8259U CPU @ 2.30GHz (4 vCPU)
메모리	16GB RAM
실행 환경	Docker 환경 (단일 컨테이너 내에서 4개 Flask 노드를 포트 구분하여 동작)
운영 체제	x86-64 Ubuntu 22.04 LTS
TPM/ DAA 스택	ibmtpm1682: TPM 2.0 소프트웨어 시뮬레이터 (TCP 2321 포트 사용) ibmtss1119: IBM TPM 2.0 툴킷 (버전 1119) ecc-daa: ibmtpm, ibmtss 기반의 ECC-DAA 오픈소스 활용하여 TPM 상에서 DAA 키 생성, 서명, 검증 수행

4.2 동작 구현

본 프로토타입은 파이썬(Python) 언어로 작성하였으며 그림 1.과 같이 최대 4개의 노드(Node A, Node B, Node C, Node D)를 각각 Flask 기반 REST 서버로 실행하고, 각 노드 내부에 DAG 저장소(DAG store)와 PBFT 상태 기계를 유지한다. 노드 간 트랜잭션 및 PBFT 메시지는 HTTP POST 방식을 통해 주고받는다.

Node: 각 노드는 Flask 서버로 동작하며, DAG store에 트랜잭션을 저장하고 PBFTState를 통해 합의 단계를 추적·관리한다.

소프트웨어 TPM: 물리 TPM 대신 ibmtpm 모듈을 사용하며, 2321번 포트(TCP)로 가상 TPM 2.0 인터페이스를 제공한다.

DAA CLI 호출: 트랜잭션 생성 시 ecc-daa의 CLI 연동과 연동하여 daa_sign_message, 검증 시 verify_daa_signature를 fork/exec 형태로 호출하여, 소프트웨어 TPM(ibmtpm)과 통신한다.

PBFT : 프로토타입은 4개 노드까지 병렬 실행하며, 노드들 간 PBFT 메시지 교환을 통해 2f+1의 서명이 모이면 트랜잭션에 최종성(Finality)을 부여한다.

이러한 아키텍처 구현을 통해 DAG 기반의 병렬 트랜잭션 처리와 PBFT 합의를 결합하고, DAA 서명을 통해 익명성 및 무결성 검증을 수행하는 최소 단위의 테스트베드를 구성하였다.

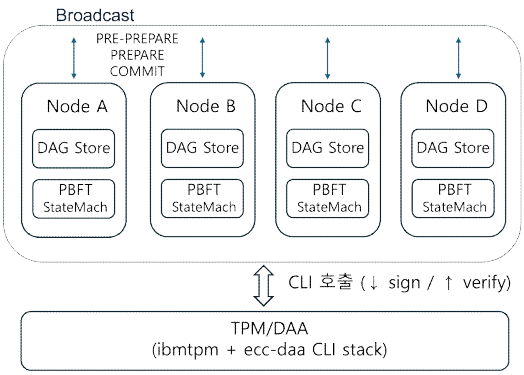

그림 1 프로토 타입 구성도

4.1 실험 결과

최대 4개 노드로 PBFT를 구성했을 때, 한두 번의 REST 메시지 왕복으로 2f+1개의 서명을 모아 트랜잭션 최종성을 확보할 수 있었다. 작은 규모 환경에서 DAG 기반 병렬 트랜잭션과 DAA 익명성이 정상 작동함을 확인하였다. 다만, 트랜잭션마다 TPM 서명 생성에 평균 약 0.74초가 소요되어, 프로토타입 처리율(TPS)을 제한하는 병목으로 작용했다. 이 지연은 하나의 프로세스에서 모든 노드가 동작하고, Python에서 외부 CLI로 DAA를 호출하는 오버헤드, 그리고 소프트웨어 TPM 시뮬레이션 특유의 암호 연산 지연이 복합적으로 영향을 미친 것으로 분석된다. 향후 개선 방향으로 gRPC 스트리밍, 메시지 큐 기반 이벤트 처리 등을 도입해 REST 호출 오버헤드를 줄여 통신 최적화를 진행할 예정이다. 또한 실 TPM 필드 테스트: 실제 하드웨어 TPM 환경에서 DAA 서명 속도를 측정함으로써 시뮬레이터 대비 성능 차이를 확인할 예정이다. 이후 실제 대규모 IoT 환경으로 확장하기 위해 Edge-Gateway 혼합 합의 모델: IoT 디바이스가 직접 PBFT에 참여하기 어려운 상황을 고려하여, 게이트웨이가 기기를 대표해 서명·합의를 수행하는 구조로 확장성을 탐구한다. 또한 키 수명·재인증, 대형 DAG 동기화, 영속 저장(온체인/오프체인) 전략 등의 DAA 정책을 고도화, 보다 안정적인 IoT 배치 시나리오에 대응하고자 한다.

V.결론

본 설계는 DAG, PBFT, DAA라는 세 가지 핵심 요소를 통합해, 컨소시엄-규모 IoT 환경에서도 익명성을 유지한 채 병렬 트랜잭션 처리와 빠른 최종성을 동시에 달성하기위한 시스템을 제안합니다. 향후 보안 통신, 합의 스케일링, 하드웨어 서명 모듈 통합을 정교화함으로써 본 프로토타입을 실서비스 수준으로 발전시킬 수 있을 것으로 기대한다.

VI.Acknowledgment

This work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.RS-2025-02306395, Development and Demonstration of PQC-Based Joint Certificate PKI Technology, 50%) and this work was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 50%).

[참고문헌]

[1] A.Aljumah, Blockchain-inspired distributed security framework for Internet of Things, Scientific Reports vol. 15 art. 10066, March, 2025, doi: 10.1038/s41598-025-93690-2.

[2] E.Dritsas and M.Trigka, A Survey on Cybersecurity in IoT, Future Internet vol. 17 no. 1 art. 30, January, 2025, doi: 10.3390/fi17010030.

[3] T.Sasi, A.H.Lashkari, R.Lu, P.Xiong and S.Iqbal, A Comprehensive Survey on IoT Attacks: Taxonomy, Detection Mechanisms and Challenges, Journal of Information and Intelligence vol. 2 no. 6 pp. 455 - 513, November, 2024, doi: 10.1016/j.jiixd.2023.12.001.

[4] F.Kahmann, F.Honecker, J.Dreyer, M.Fischer and R.Tönjes, Performance Comparison of Directed Acyclic Graph-Based Distributed Ledgers and Blockchain Platforms, Computers vol. 12 no. 12 art. 257, December, 2023, doi: 10.3390/computers12120257.

[5] Microsoft, Trusted Platform Module (TPM) Technology Overview, Microsoft Learn documentation, July, 2024.

[6] L.Chen, C.Dong, N.El Kassem, C.J.P.Newton and Y.Wang, Hash-based Direct Anonymous Attestation, in PQCrypto 2023 (LN

CS 14154), Springer, pp. 565 - 600, 2023, doi: 10.1007/978-3-031-40003-2_21.

[7] A. Fuchs and tpm2-software community, TPM2-TSS: OSS implementation of the TCG TPM 2.0 Software Stack (TSS2), GitHub repository, ver. 4.1.3 (tag 30e6057), May, 2024.

[8] S. Wesemeyer, C. J. P. Newton, H. Treharne, L. Chen, R. Sasse and J. Whitefield, ecc-daa: Implementation of a TPM 2.0-based Direct Anonymous Attestation Scheme, GitHub repository, commit eebd40d, October, 2020.