양자-후보암호 기반 IoMT 블록체인 보안 프레임워크 및 디지털 제품 여권 확장에 관한 연구

이유진, 인호*
고려대학교, *고려대학교

yyujin98@korea.ac.kr, hoh_in@korea.ac.kr

A Study on the Quantum and Post-Quantum Cryptography-based Blockchain Security Framework for IoMT and Its Extension to Digital Product Passports

Lee Yu Jin, Hoh Peter In*
Korea Univ., *Korea Univ.

요 약

본 논문에서는 IoMT(Internet of Medical Things) 환경에서 양자 내성 암호(Post-Quantum Cryptography, PQC)와 양자 키 분배(Quantum Key Distribution, QKD)를 통합한 하이브리드 보안 프레임워크(PQCIF)를 제안하고 이를 디지털 제품 여권(Digital Product Passport, DPPs)으로 확장하는 구조적 방안을 다루고 있다. 본 논문에서는 계층별 암호 기법 설계 및 데이터 흐름 구조를 정리하여 IoMT 보안성과 ESG 대응을 동시에 고려한 아키텍처를 제시하고 있다.

Ⅰ. 서 론

IoMT 환경은 환자의 생체 정보 수집, 응급 대응, 실시간 모니터링 등 다양한 의료 서비스를 가능하게 하지만, 민감한 정보가 네트워크를 통해 전송되기 때문에 강력한 보안 체계가 필수적이다 [1]. 양자 컴퓨터의 발전으로 기존 공개키 암호 기반 인증 기법의 안전성은 점차 위협받고 있으며, 이에 따라 Post-Quantum Cryptography(PQC) 및 Quantum Key Distribution(QKD) 기술이 차세대 보안 솔루션으로 주목받고 있다 [2].

최근 유럽연합(EU)에서 추진 중인 디지털 제품 여권(Digital Product Passport, DPPs)은 ESG 대응을 위한 제품의 제조, 유통, 사용, 재활용 정보를 투명하게 기록하는 방식으로, 의료기기 및 헬스케어 데이터의 블록체인 기반 관리에도 활용될 수 있는 잠재성이 존재하고 있다 [3].

본 논문에서는 블록체인 기반 IoMT 시스템에서 PQC 와 QKD 를 통합한 보안 프레임워크를 제안하고 있으며, 해당 프레임워크가 DPPs 와 연계될 수 있는 구조를 분석하고 있다.

Ⅱ. 본론

본 논문에서는 PQC 와 QKD 를 결합한 하이브리드 보안 프레임워크를 응용 계층, 네트워크 계층으로 구분하여 설계하고 있으며, 각 계층에 최적화된 암호 기법을 적용하는 방식을 설명하고 있다. 응용 계층에서는 NIST PQC 후보 알고리즘(Falcon, Dilithium, NTRU 등)을 활용하여 사용자 인증 및 데이터 서명을 수행하도록 설계하고 있으며 [4], 이로 인해 IoMT 환경에서의 데이터 무결성과 인증 신뢰성이 강화될 수 있는 구조를 갖추고 있다.

네트워크 계층에서는 BB84 기반 QKD 프로토콜을 통해 안전한 키 분배를 수행하고 있으며, 분배된 대칭키는 AES-GCM 과 같은 고속 대칭 암호

알고리즘과 함께 사용되어 전송 데이터의 보안을 확보하도록 구성되어 있다 [5].

또한 본 논문에서는 DPPs 시스템을 IoMT 보안 체계에 통합하는 구조를 설명하고 있으며, 이를 통해 의료기기의 제조, 유지보수, 폐기까지의 전 생애 주기 정보를 블록체인 상에 저장하고 검증하는 방식을 제시하고 있다. 각 트랜잭션에는 PQC 기반 서명이 포함되어 위변조 방지를 가능하게 하며, ESG 관련 메타데이터를 암호화하여 보호할 수 있는 구조가 적용되고 있다 [6].

본 논문에서는 구조 설계와 이론 기반의 보안성 분석을 중심으로 프레임워크의 적용 가능성을 검토하고 있다.

Ⅲ. 결론

본 논문에서는 IoMT 환경에 적합한 보안 체계를 구현하기 위해 PQC 와 QKD 를 통합한 하이브리드 보안 프레임워크를 제안하고 있으며, 해당 프레임워크가 디지털 제품 여권(DPPs) 시스템으로 확장 가능한 구조를 지니고 있음을 확인하고 있다.

또한 데이터 유형 및 사용 시나리오에 따라 PQC 또는 QKD 를 선택적으로 적용할 수 있는 계층별 아키텍처를 설계하고 있으며, 이를 통해 보안성과 확장성 측면에서 효율적인 구조를 제시하고 있다.

향후 본 논문에서는 QNN(Quantum Neural Network)을 기반으로 한 이상 탐지 기법과의 연계 가능성을 고려할 수 있으며, IoMT 와 ESG 기반 제품 관리 시스템의 통합적 보안 체계를 심화 연구할 수 있는 방향성이 존재하고 있다.

ACKNOWLEDGMENT

This work was supported by the Brain Korea 21 FOUR Research Program of the Department of Computer Science at Korea University. It was also funded by the Institute of Information & Communications Technology Planning & Evaluation (IITP), under the Korea government (MSIT), through the National Program for Excellence in Software (Project No. 2023-0-00044), the High Assurance of Smart Contract for Secure Software Development Life Cycle project (Grant No. RS-2021-II210177), the Convergence Security Core Talent Training Business Support Program (Grant No. IITP-2024-RS-2022-II221198), and the Global Research Support Program in the Digital Field (Grant No. R2409841/2021-0-00177). Additional support was provided by the National Research Foundation of Korea (Grant No. NRF-2021R1A2C2012476) and the Seoul-type Private Investment-linked Technology Commercialization Support Program of the Seoul Business Agency (Grant No. VC230019). This research was partially supported by research funding from Korea University.

참 고 문 헌

[1] NIST, “Post-Quantum Cryptography Standardization,” https://csrc.nist.gov/projects/post-quantum-cryptography

[2] S. Pirandola et al., “Advances in Quantum Cryptography,” Adv. Opt. Photon. 12, 1012- 1236 (2020).

[3] European Commission, “Proposal for a Regulation on Ecodesign for Sustainable Products,” COM(2022) 142 final.

[4] J. Hoffstein, J. Pipher, J.H. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem,” Lecture Notes in Computer Science, vol 1423, 1998.

[5] M. Sasaki et al., “Field test of quantum key distribution in the Tokyo QKD Network,” Optics Express, 2011.

[6] Tan, S. et al., “Blockchain-based Smart Contracts for Digital Product Passport,” Sensors, 21(12), 4325, 2021.