Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 9 pp. 733-738, 2023

https://doi.org/10.5762/KAIS.2023.24.9.733
ISSN 1975-4701 / eISSN 2288-4688

IoT 펌웨어 업데이트의 블록체인 적용을 위한 성능 연구 - 플랫폼을 중심으로

김지량, 이용준, 강장묵*
극동대학교 해킹보안학과

Performance study for blockchain application of IoT firmware update - Focusing on Platform

Ji Ryang Kim, Yong Jun Lee, Jang Mook Kang*
Division of Hacking Security, Far East University

요 약 코로나 시대로 인한 비대면 서비스 수요의 증가로 사물인터넷 기기의 보급률이 증가했다. 사물인터넷 기기의 펌웨어 업데이트 과정은 인증자의 권한이 크고 다양한 데이터를 다루기 때문에 보안의 관점에서 매우 중요하다. 사물인터넷 기기의 펌웨어 업데이트 보안을 확보하기 위하여 블록체인의 특징을 활용할 수 있다. 본 연구에서는 IoT 펌웨어 업데이트 플랫폼을 실제로 구축하여 데이터 입력과 조회의 성능을 측정하기 위한 실험을 진행하였다. 실험 결과 조회 기록은 약 1,600 TPS 이상을 기록하였고 입력 기록의 평균은 약 360 TPS 이상을 기록하였다. 실험 결과를 공공기관에서 발주되는 제안요청서의 성능 요구치와 비교한 결과 조회 성능은 성능 요구치를 충족하지만 입력 성능은 네트워크 환경 및 트렌젝션의 구조체 용량 등에 따라 서비스 요구 성능치를 충족할 수 있을 것으로 판단된다. 따라서 IoT 펌웨어 업데이트 과정에 블록체인을 적용하기 위해서는 성능 향상을 위한 네트워크 성능 및 체인코드 구조와 관련된 연구가 지속되어야 할 것으로 판단된다.

Abstract Due to the increase in demand for non-face-to-face services due to the COVID-19 era, the penetration rate of IoT devices has increased. The firmware update process of IoT devices is very important from a security point of view because the certifier's authority is large and deals with various data. In order to secure the firmware update security of IoT devices, the characteristics of the blockchain could be utilized. In this study, an experiment was conducted to measure the performance of data input and inquiry by establishing an IoT firmware update platform. As a result of the experiment, the inquiry record was more than about 1,600 TPS, and the average input record was more than about 360 TPS. We compared the experimental results with the performance requirements of a proposal request ordered by public institutions, and the inquiry performance met the requirements, but the input performance meeting the service requirements depended on the network environment and the structure capacity of the transition. Therefore, in order to apply blockchain techniques to the IoT firmware update process, research related to network performance and chain code structure should be continued to improve performance.

Keywords : IoT, BLOCKCHAIN, Firmware, Transaction, Security

본 논문은 극동대학교 연구과제로 수행되었음.
*Corresponding Author : Jang Mook Kang (Far East Univ.)
email: honukang@gmail.com, honukang@kdu.ac.kr
Received August 1, 2023 Revised August 31, 2023
Accepted September 1, 2023 Published September 30, 2023

1. 서론

1.1 사회적 배경

코로나 시대로 인한 비대면 서비스 수요의 증가는 다양한 원격 디바이스 시장의 확대를 가져왔고 네트워크에 연결된 IoT 기기의 숫자는 지속적으로 증가하였다. 2020년에는 2019년 대비 약 44억 개가 증가한 약 310억 개의 IoT 기기가 네트워크에 연결된 것으로 예상되며 그 원인은 다음과 같다.

IoT 원격 관리의 필요성은, 감염병 발생에 따른 '비대면사회를 가속시키는 주된 원인'으로 유추할 수 있다.

IoT의 필요성은 내부요인으로 일반인과 전문가 모두 '감염병', 환경오염을 주된 요인으로 지목하였다[1]. 외부요인으로는 기술혁신에 따른 가치관의 변화가 있다.

코로나는 종식되었으나 원격 디바이스의 보급 확산으로 인하여 IoT 기술의 원격제어 기술이 보안의 확장된 영역으로 매주 중요하게 인식되었다.

1.2 기술적 배경

원격 디바이스에서는 운영체제와 서비스 업데이트를 위한 펌웨어 업데이트가 지속적으로 발생한다. 원격 펌웨어 영역의 업데이트는 인증자가 부여받은 권한이 크고 데이터 영역에서 디바이스를 다루기 때문에 보안의 관점에서 취약하다. 펌웨어 업데이트 과정의 다양한 보안 취약점을 강화하기 위하여 다양한 연구가 지속되고 있다. 예를 들면, 국가 사이버 안보센터에서는 전체 33건의 사이버 안보 중, 비대면 서비스 환경에서의 보안, IoT보안 취약점 논문, IoT보안 업데이트 취약점 등이 연구되었다[2].

특히, 보안 취약점 강화의 관점에서 블록체인 기술의 특징은 많은 이점을 가지고 있다. 블록체인의 특징 중 이력의 불변성을 증명할 수 있는 무결성 특성은 다양한 산업에서 시스템 로그 저장에 응용하여 활용되고 있다. 사례를 살펴보면 최초 인증 등록 후에는 블록체인이 최초 정보의 신뢰성을 증명하여 간편 로그인 기능을 지원한 간편 로그인 서비스, 최초 발행한 증명서의 진위를 증명하기 위한 블록체인을 활용한 진위 확인 서비스 사례 등이 있다. 이런 서비스 사례를 살펴볼 때 탈중앙화된 데이터 저장, 암호화된 데이터 처리, 합의 알고리즘을 통한 견고함, 분산 데이터 저장 등 보안의 관점에서 요구하는 특징을 가지고 있다고 할 수 있다.

1.3 성능 검증의 필요성

블록체인의 이런 특징을 활용하면 IoT 기기 펌웨어 업데이트 과정의 보안 강화 기술로 활용할 수 있다. 하지만 이런 가능성을 검토하기에 앞서 펌웨어 업데이트 과정의 데이터가 블록체인 원장에 기록되는 과정의 안정성이 전제되어야 한다. 시스템 성능 미달로 인하여 탐지, 동작의 지연이 발생하면 보안성이 감소하기 때문이다.

따라서 블록체인을 IOT 펌웨어 업데이트 과정에 적용하기 위해서는 첫째, 성능과 데이터의 일관성이 검증되어야 한다. 둘째, 실제 실증 과정에서 해당 데이터의 특성에 따라 구체적인 활용 가이드라인[이 제시되어야 한다[3]. 본 연구에서는 실제 IoT 펌웨어 업데이트 플랫폼을 구현하여 펌웨어 업데이트 과정에서 발생하는 시스템 로그를 블록체인의 체인코드로 구성하였다. 체인코드로 구현된 트렌젝션을 통하여 시스템 로그를 원장에 기록하였고 초당 트렌젝션의 입력 및 조회 성능을 측정하여 블록체인의 활용 가능성을 실험하였다.

또한 사용자가 펌웨어를 업데이트할 수 있는 사용자 페이지를 구성하고 데이터베이스를 구성하는 대신 블록체인의 데이터베이스와 원장을 활용하였다.

1.4 논문의 구성

1장에서는 본 연구의 배경과 목적을 2장에서는 블록체인의 현황과 펌웨어 업데이트의 적용 가능성을 검토하고 실제로 구현된 플랫폼에서 수행된 실험 결과를 제시하였다. 마지막으로 3장 결론에서는 연구 결과의 시사점과 향후 연구 방향을 제시하였다.

2. 본론

2.1 블록체인의 특징과 펌웨어 업데이트

2.1.1 블록체인의 특징과 발전

블록체인은 탈중앙화 환경에서 익명성, 보안성, 투명성, 신뢰성, 안정성, 효율성, 자동성 등 다양한 가치를 제공하지만, 확장성 및 프라이버시 보호의 측면에서는 제한적인 특징을 가지고 있다. 또한 블록체인 기술은 공개형 블록체인에서 확장성과 효율성을 보완한 허가형 블록체인으로 발전하였으며, 향후 사회 기반구조로서 산업융합 등에 활용될 전망이다.

2.1.2 하이퍼레져 패브릭

다양한 블록체인 메인넷 중 하이퍼레져 패브릭은 금융, 유통 등의 기업 서비스 분야에서 많이 활용되고 있다.

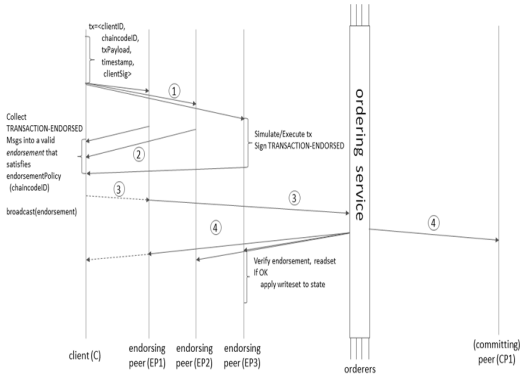

Fig. 1. Proof of transition step between peer, oreder [4]

하이퍼레져 패브릭은 체인코드, 피어, 오더러 등의 네크워크 요소로 구성되어 있으며 체인코드를 구조체로 가지고 있는 트렌젝션의 유효성을 합의 과정을 통하여 검증하여 원장에 기록한다. 이런 프라이빗 블록체인의 특징은 퍼블릭 블록체인과 비교하여 높은 속도와 보안성을 보장하기 때문에 많은 기업체에서 활용하고 있다. 하지만 분산 환경에서는 블록 전파의 지연이나 네트워크 단절 같은 문제가 발생할 때 블록체인의 갈래가 생실 수 있다[5].

2.1.3 IoT 펌웨어 업데이트와 블록체인

IoT 디바이스의 펌웨어 업데이트 과정은 원격 환경에서 진행된다. 펌웨어 업데이트 데이터는 디바이스 제어와 관련되어 있어, 높은 수준의 보안성을 요구한다. 우리나라의 경우 정보기기의 등급은 관리하는 데이터의 기밀성 등을 기준으로 분류하고 이에 부합하는 다양한 지침을 포함한다.

이런 이유로 특정 정보시스템 기기는 보안 지침 준수를 위하여 오프라인 업데이트를 수행하는 경우가 발생한다. 그러나 펌웨어 업데이트 과정에서 블록체인 네트워크의 특징을 활용하면 원격 관리를 하면서도 보안성을 강화할 수 있다. 예를 들면 최신 펌웨어를 사용할 경우 가장 최근에 기록한 블록 내의 펌웨어 해시값을 비교하여 조작 여부를 확인하는 방식 등을 제안할 수 있다[6].

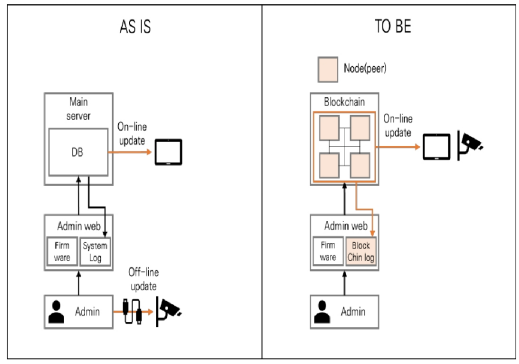

Fig. 2. Changes in firmware update methods with blockchain

2.2 펌웨어 업데이트 플랫폼

2.2.1 펌웨어 업데이트 플랫폼 구성

블록체인기술로 펌웨어 업데이트 과정을 적용할 경우, 시스템 성능을 검증하기 위하여 하이퍼레져 기반의 블록체인 네트워크를 데이터베이스로 사용하는 펌웨어 업데이트 플랫폼을 구성할 것을 제안한다.

REST API를 통하여 IoT 디바이스와 플랫폼이 연동이 가능한 인터페이스를 구성하고 디바이스와 API는 상호키교환 방식으로 인증하도록 구현하였다. 4개의 피어 서버가 블록체인의 구성원과 데이터베이스 역할을 담당하고 REDIS는 IoT 디바이스와 플랫폼 간의 교환키를 저장하고 관리한다.

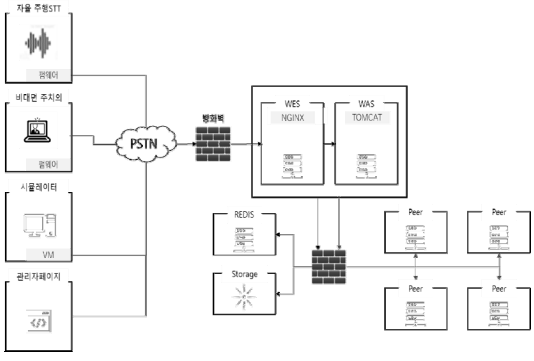

Fig. 3. Blockchain technology verification system structure diagram

스토리지는 펌웨어 파일을 저장하는 역할을 담당하고 WEBWAS는 API의 호스팅과 사용자페이지 웹을 위한 서버로 구성하였다.

Table 1. Chincode for transection

Spec.		Key	Value
1	Service	service number	id
			name
			user
2	Firmware	firmware number	id
			name
			version
			path
			date
			servicenumberid
3	device	device number	id
			uuid
			servicenumberid
			firmware version
			date

시스템에서 블록체인으로 전달되는 구조체인 체인코드는 키벨류 방식으로 위 Table 1과 같이 구성하였다.

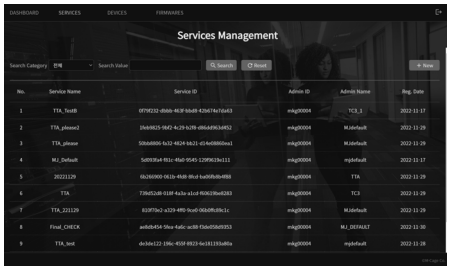

Fig. 4. Service Registration User web

Fig. 5. Device Registration User web

위 Fig. 4와 5는 플랫폼과 연동할 수 있는 디바이스 정보를 등록하고 새로운 펌웨어 파일을 버전 정보와 함께 등록하는 DashBoard이다. Fig. 5와 같이 IOT 디바이스에게 원격으로 배포가 가능한 사용자 페이지를 구성하였다.

2.2.2 펌웨어 업데이트 블록체인 성능 시험

펌웨어 업데이트 플랫폼에 블록체인 데이터베이스를 적용하여 서비스 구현 수준의 성능을 검증하기 위하여 시험을 진행하였다. 서비스 입력처리와 서비스 조회 처리 성능을 시험하였다. 시험 항목 및 목표는 다음과 같다.

Table 2. Test items and objectives

Name	Target
Service input processing performance	Quantitatively measure average performance (TPS) when multiple users request data registration at the same time
Service query processing performance	Average performance when multiple users request data lookup at the same time (TPS)

블록의 생성 주기는 2초, 최대 트렌젝션 사이즈는 20MB로 설정하고 도커의 형상은 20.10.17, 블록체인 데이터베이스는 CouchDB를 활용하였다. 네트워크의 경우 내부 네트워크는 1G. 외부 네트워크는 100M 환경에서 진행하였다. 실험방법은 JMETER를 활용하여 10,000개의 실험 데이터를 입력하여 총 5회 입력 성능을 측정하였다. 측정 결과 최소값은 344.8 TPS, 최대값은 384.6 TPS를 기록하여 평균 365.5 TPS를 기록하였으며 측정 결과를 표로 정리하면 다음과 같다.

Table 3. Imput TPS

no	Input time (hhmmss)	Block time (hhmmss)	duration (s)	TPS
1	1:33:11	1:33:39	28	357.1
2	1:51:41	1:52:07	26	384.6**
3	2:34:09	2:34:36	27	370.4
4	2:42:04	2:42:31	27	370.4
5	2:48:01	2:48:30	29	344.8*

조회 성능의 경우 400명의 사용자가 동시에 데이터 조회 요청을 가정하고 실험을 진행하였다. 측정 결과는 아래와 같다.

Table 4. Quary TPS

no	TPS
1	1638.7
2	1676.4**
3	1604.5*
4	1626.7
5	1632.0

측정 결과 최소값은 1604.5 TPS, 최대값은 1676.4 TPS를 기록하였다.

3. 결론

일반적인 정보시스템의 성능 요구사항을 충족하기 위한 블록체인 기술의 어려움은 다음과 같다. 첫째, 블록체인은 트렌젝션이 체인코드 구조체를 통하여 발생되는 환경을 가지고 있어 일반적인 정보시스템의 트렌젝션보다 패킷의 용량이 큰 환경에 놓여있다. 둘째, 제한적인 네트워크 환경에서 블록체인으로 일반적인 서비스의 성능 요구치를 충족시키기 위하여 체인코드를 분할하고 간소화하기 위한 최적화가 필요하다.

블록체인 환경에서 수행되는 펌웨어 업데이트 시스템을 일반적인 정보시스템 환경에 적용하여도 상용화 수준의 서비스에서는 성능에 문제없이 시스템이 운영되어야 한다. 본 연구에서는 펌웨어 업데이트 과정에 블록체인을 적용하기 위한 데이터의 입력 및 조회 성능을 기존의 정보시스템의 요구사항과 비교하였다. 그 결과 일반적인 시스템의 요구사항에 부합하였다.

본 연구에서는 펌웨어 업데이트 플랫폼에 블록체인 데이터베이스를 적용하여 성능을 측정한 결과 1G의 네트워크 환경에서 입력 TPS는 300을 상회 하였고 조회 TPS는 1600을 기록하였다. 해당 실험값을 토대로 현재 공공기관 등의 시스템 구축 시 성능 요구사항과 비교한 결과 다음과 같은 결과를 확인하였다. 첫째, 조사 결과 100M의 외부 네트워크에서 3초 이내 조회 처리 요구사항을 충족하였다. 둘째, 동시 최대 1,000건의 데이터 처리, 동시 사용자 100명의 접속 요구사항을 충족하였다.

연구 결과는 IoT 펌웨어 업데이트 단계에서 블록체인 기술이 성능저하 등의 문제점 없이 적용될 수 있는 가능성을 보여준다. 따라서 이후 발전된 수준의 서비스 기능으로 블록체인 적용을 확대할 수 있을 것으로 사료 된다.

본 연구의 한계는 다음과 같다. 첫째, 입력 성능의 경우 네트워크, 서버 사양 등의 주변 환경 요소에 따라 성능 요구치 달성 여부가 달라졌다.. 따라서 IoT 디바이스의 펌웨어 업데이트 플랫폼을 대상으로 블록체인을 적용하기 위해서 네트워크 환경 등을 고려하여 트렌젝션 크기 등을 조정하기 위한 연구가 후속 연구로 필요할 것으로 사료 된다.

References

[1] Park, noun etc., 2021 KISTEP Promising Technology Research on selection, 2021, p.24. Fig. 3-7

[2] URL: https://www.ncsc.go.kr:4018/PageLink.do?link=forward:/cop/bbs/selectBoardList.do?bbsId=EducationData_main&menuNo=070000&subMenuNo=070400&thirdMenuNo (Retrieved 15 August 2023)

[3] Jang Mook KANG, Kim do hyoung, YoonCheolhee, “A review on stake, trust, and proof-of-work methods applicable to blockchain-based IOT firmware”, Proceedings of KIIT Conference, KIT, South Korea, 1, 48-50. 2022

[4] URL: https://www.hyperledger.org (Retrieved 10 August 2023)

[5] Jea-Min Lim, Youngpil Kim, Chuck Yoo."A usage of blockchain for secure firmware verification in IoT environment", *Korea Information Science Association, A* collection of academic presentations, 482-484. 2017

[6] B. H. Lee, *Blockchain based Firmware Verification and Update Scheme for Embedded Devices, Master's thesis, Sangmyung University, Seoul, Korea, pp.24, 2017.*

[7] Yejun Kim, Jeonghyeon Gim, Seungjoo Kim."A Study on Systematic Firmware Security Analysis Method for IoT Devices", Journal of the Korea Institute of Information Security & Cryptology, 31, 1 , 31-49, 2021

김 지 량(JI-Rhyang Kim) [정회원]

- 2020년 7월 ~ 현재 : 엠케이지 주식회사 CTO
- 극동대학교 해킹보안학과 석사과정

〈관심분야〉
블록체인, 인공지능, 보안

이 용 준(Yong-Joon Lee) [종신회원]

- 2005년 2월 : 숭실대학교 컴퓨터학과 박사
- 2010년 2월 ~ 2016년 3월 : 한국인터넷진흥원 수석연구위원
- 2016년 4월 ~ 2020년 3월 : 국방보안연구소 연구관
- 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
해킹보안, 국방보안, 인공지능보안

강 장 묵(Jang Mook Kang) [정회원]

- 2005년 8월 : 고려대학교 정보보호대학원 공학박사
- 2010년 3월 ~ 2017년 8월 : 고려대학교 컴퓨터공학과 연구교수
- 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
인공지능, 블록체인, 인공지능보안