https://doi.org/10.33778/kcsa.2022.22.4.161

사물인터넷 환경에서 블록체인 기술을 이용한 보안 관리에 관한 소고 (주행 환경 센싱 데이터 및 탑승자 데이터를 포함한 자율주행차량에서의 보안 사례를 중심으로)

강 장 묵*

요 약

코로나 바이러스 출현 이후, 비대면 서비스가 활성화되면서, 사물인터넷(IoT)의 센싱 정보를 블록체인 기술로 담아 무결성을 보장하는 서비스가 확대되고 있다. 예를 들면, CCTV 등을 이용한 안전, 치안 등의 영역에서는 실시간으로 안전하게 펌웨어가 업데이트되고 악의적 침입이 없었음을 확인하는 과정이 요구된다. 기존의 안전한 보안 처리 절차에서는 공무를 수행하는 담당자가 USB 등을 휴대하고 직접 펌웨어를 업데이트 하는 경우가 많았다. 그러나 하이퍼레저 등 프라이빗 블록체인 기술을 활용할 경우, 사물인터넷 환경의 편리성 및 업무 효율성의 증대와 안전을 기대할 수 있다. 이 글은 비대면 환경하에서 펌웨어 업데이트, 기기변경 등 사물인터넷의 취약점을 예방하는 방안을 시나리오적으로 기술하였다. 특히 해킹이나 정보유출 등 악의적인 보안위험에 노출되기 쉬운 사물인터넷에 최적인 블록체인 기법을 소개하였다. 이 글에서는 점차 확대되고 있는 사물인터넷 환경하에서 블록체인기술을 적용한 운영을 통해 무결성을 담보한 보안관리의 필요성 및 체제를 제안하였다. 이를 활용할 경우 추후 사물인터넷 환경의 보안 강화를 위한 가이드라인 등에 블록체인 기법을 어떻게 적용할지에 대한 통찰력을 얻을 것으로 기대된다.

The study of security management for application of blockchain technology in the Internet of Things environment (Focusing on security cases in autonomous vehicles including driving environment sensing data and occupant data)

Jang Mook KANG*

Abstract

After the corona virus, as non-face-to-face services are activated, domain services that guarantee integrity by embedding sensing information of the Internet of Things (IoT) with block chain technology are expanding. For example, in areas such as safety and security using CCTV, a process is required to safely update firmware in real time and to confirm that there is no malicious intrusion. In the existing safe security processing procedures, in many cases, the person in charge performing official duties carried a USB device and directly updated the firmware. However, when private blockchain technology such as Hyperledger is used, the convenience and work efficiency of the Internet of Things environment can be expected to increase. This article describes scenarios in how to prevent vulnerabilities in the operating environment of various customers such as firmware updates and device changes in a non-face-to-face environment. In particular, we introduced the optimal blockchain technique for the Internet of Things (IoT), which is easily exposed to malicious security risks such as hacking and information leakage. In this article, we tried to present the necessity and implications of security management that guarantees integrity through operation applying block chain technology in the increasingly expanding Internet of Things environment. If this is used, it is expected to gain insight into how to apply the blockchain technique to guidelines for strengthening the security of the IoT environment in the future.

Key words : blockchain, internet of things, integrity, AI, IoT, security management system

접수일(2022년 08월 09일), 수정일(1차: 2022년 09월 06일), (2차: 2022년 09월 26일), 게재확정일(2022년 10월 31일)

* 극동대학교 과학기술대학 해킹보안학과 AI융합보안 교수

1. 서 론

전 세계 사물인터넷 (IoT; Internet of Things) 시장 규모가 2021년 3,845억 달러에서 2027년에는 5,664억 달러로, 연간 6.7%로 성장할 전망이다[1]. 코로나 바이러스 출현 이후, 비대면 서비스가 증가하면서 사물인터넷이 빠르게 일상생활에 스며들고 있다. 사물인터넷은 우리 생활 속에 부지불식 중에 스며들고 있지만, 이를 보안 관리 체계 또는 전체 사물인터넷을 조망하는 거버넌스적 연구는 부족한 실정이다.

다양한 제조사가 고객의 수요에 맞추어 고객과 대화가 가능한 스마트 스피커, 홈오토메이션을 스마트폰과 연계한 사물인터넷, 집안의 전구부터 에어콘까지 자동센싱 또는 음성인식으로 처리하는 사물인터넷 디바이스 외에도 호텔이나 빌딩 내 사물인터넷, 전력과 같은 공공재에 있어서 사용량 등을 측정하는 여러 형태의 사물인터넷이 등장하고 있다. 해당 서비스는 이기종 다품종이라는 특징을 갖는다.

여러 회사가 다양한 분야에서 경쟁을 하다보니 이를 통합하거나 전체적 시야에서 보안을 다루는 체계가 미흡하다.

이 글은 여러 센싱이 빅데이터로 수집되고 분석을 위해 특정 전처리가 이루어진 후 인공지능 등 알고리즘을 거쳐 고객에게 서비스되는 과정에서 발생할 수 있는 보안의 무결성을 보장하는 방안을 제시하였다.

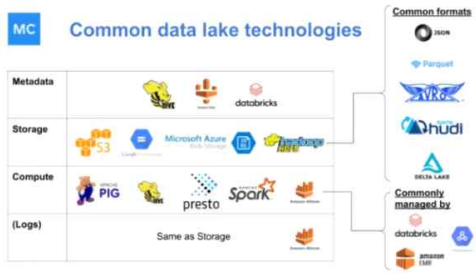
무결성 보장을 위해 사물인터넷의 펌웨어 업데이트 과정에서 무결성을 테스트 하는 간단한 실험과 이를 바탕으로 일반화가 가능한 수준의 사물인터넷 보안 관리 체계를 제시하였다.

2. 관련 연구

2.1 사물의 연결을 통한 지능형 플랫폼과 보안 취약점 증가

일상에서 쓰는 사물부터 군부대에서 이용하는 군사물자까지 인터넷에 연결 가능한 기기로 발전해 오면서, 사물과 사물 간에 정보를 교류하고 상호 소통하는 지능형 플랫폼이 개발되고 있다.

각 플랫폼은 각각의 사물이 갖는 고유한 목적에 따라 센서들을 연결하고 상호 소통을 한다.



(그림 1) 데이터 레이크와 기술

(그림 1)은 이러한 센서를 통해 사물은 데이터를 수집하고, 각각의 사물은 인터넷을 통해 사물인터넷 플랫폼에 보내어 빅데이터 또는 데이터 레이크를 구성한다[2].

그러나 사물인터넷 플랫폼은 대부분 중앙 집중형 플랫폼으로 확장성, 보안성, 안정성에 대한 단점이 존재한다. 기존 시스템에 사물인터넷을 중앙 집중형으로 추가하는 레거시 시스템은 해킹, 단일 장애점 등 여러 가지 한계를 보인다[3]. 이처럼 다양한 센싱 정보의 활용과 데이터 처리 기술이 복합적으로 적용된 사물인터넷 서비스는 기술 자체 혹은 구현하는 방법의 취약점으로 인해 다양한 보안 위협에 노출되고 있다.

2.2 사물 인터넷의 정의에서 비추어본 보안 위협 범위

사물인터넷 플랫폼은 비정형 데이터를 기반으로 생활에 도움이 될 수 있는 서비스를 제공하지만 사물인터넷의 정의를 바탕으로 명확한 보안 범위를 제한하는 것이 정보보호 관리 차원에서 효과적이다.

(그림 2) M2M, IoT, IoE의 포괄적 개념

(그림 2)는 사물통신, 사물인터넷, 만물인터넷에 대한 구체적인 세부 기술을 통해 해당 서비스 별 보안 영역을 추론하는데 도움을 준다[4]. M2M, IoT, IoE는 다양한 프로토콜과 방대한 양의 정형/비정형/메타 데이터 송수신이 이루어진다. 따라서 사물인터넷 서비스는 보안 위협에서 중간 공격, 데이터 위·변조, 사칭 그리고 도청 등에 노출되어 있다.

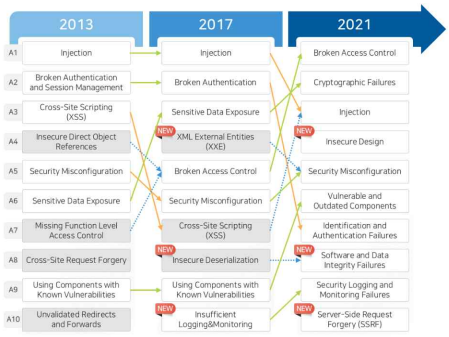
이러한 보안 위협은 M2M의 CCTV 등, IoT의 RFID 등, IoE의 커넥트카 등 구체적인 대상과 범위를 정의하는 보안 관리 체계의 필요성이 요구된다.

이기종의 다양한 데이터의 무결성 보장을 위한 기술로 3장에서 블록체인을 해결방안으로 제시하였다.

3. 블록체인을 이용한 사물인터넷 관리 체계 방법

3.1 사물인터넷 영역별 취약점 분석

앞 장에서 다룬 M2M, IoT, IoE와 같은 개념의 변천에 맞춘 보안 관리 체계의 필요성을 언급하였다. 본 장의 아래 (그림 3)은 IoT기술이 발전함에 따라 세부 보안 기술도 달라짐을 도식화하여 보여준다[5].



(그림 3) 주요 년도별 OWASP IoT Top10 취약점

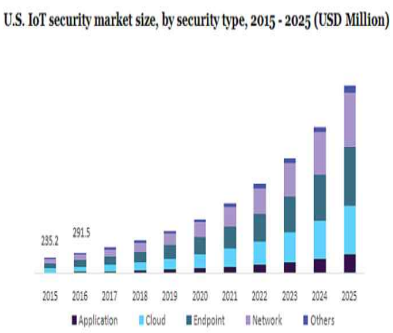
OWASP가 전세계 보안 전문가로부터 설문을 통해 분석한 관련 기술에는 센서 등의 엣지 장치에서 데이터를 수집, 전송, 저장, 관리, 분석하는 과정들이 포함된다. 이러한 데이터 수집 과정은 IoT 측면에서는 사물 통신의 사설망과 공용망을 모두 사용하기 때문에 안전한 네트워크가 필요하다.

즉, 연결된 장치의 수가 증가함에 따라 보안 취약점의 대상과 중첩된 범위가 넓어지는 것을 뜻한다.

구체적으로는 장치 구성, 모니터링, 소프트웨어 및 펌웨어 관리 및 해결 등 사물인터넷 서비스 운용에 따른 보안 취약점이 있다. 이 글에서는 이를 해결하기 위한 방식으로 기존방식에 블록체인기술을 적용한 후, 무결성을 검증하는 관리 방안을 제안한다.

3.2 블록체인 기술을 이용한 IoT 관리 체계

앞 장에서 언급한 사물인터넷 산업 시장 중 사물인터넷 대상 보안 시장은 아래 (그림 4)와 같다. 구체적으로는 2017년 12억 4천만 달러였던 IoT보안 시장은 2027년까지 연간 29.7% 큰 폭으로 증가할 전망으로 이는 사물인터넷 전체시장의 증가폭을 뛰어넘는 수치이다[6].



(그림 4) U.S IoT security market size

이러한 사물인터넷 산업의 발전에 따른 새로운 보안 요구사항을 증대하고 있는데 그 해결 방안 중 하나로 사이버 보안 인증이 있다[7]. 사물인터넷 보안 장비에 대한 사이버 보안인증을 받도록 하는 방안은 레거시 관리 체계로 여전히 그 효과가 기대된다. 그러나 다양한 이기종 디바이스가 연동되는 사물인터넷에서는 블록체인 기술 중 프라이빗 블록체인을 응용한 보안 관리 체계를 추가하는 방안을 고려할 수 있다.

구체적으로는 기존 사물인터넷 검증을 위한 연산을 지속적으로 수행해야 하는 PoW(작업 증명) 블록체인가 아닌, 네트워크에 축적된 지분을 통해 블록을 검증하는 PoS(지분 증명), 그 중에서 확장성 부분을 해결하고자 하는 DPoS(위임 지분 증명) 방식으로 스마트 홈 IoT 환경에 적절한 보안용 블록체인 체제를 제시하였다[8]. 그러나 본 연구에는 PoW, PoS, DPoS 등 퍼블릭 방식이 아닌 하이퍼레저 기반의 IoT의 펌웨어 업데이트 등에 활용 가능한 블록체인 기술을 제안한다.

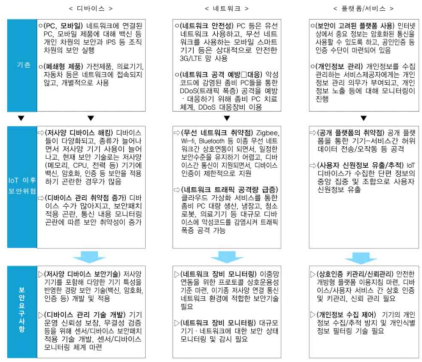
4. IoT 보안 요구사항 별 블록체인 기반의 관리체계

4.1 IoT 분야별 보안 요구 사항

사물인터넷은 디바이스, 네트워크, 서비스 플랫폼이라는 세 가지 분야로 나누어 서비스된다. 첫째, 디바이스는 무결성 보장을 위한 해시기술 개발, 경량 암호 기술 개발, 저전력 장치 개발 등을 통해 보안 요구사항을 충족시킨다. 둘째, 네트워크 영역은 낮은 성능을 고려한 프로토콜 기술, 상호운용 통신정책 및 보안 프로세스 마련, 외부 접근 탐지 및 감시를 위한 AI 응용 기술로 보안 요구사항을 충족한다. 셋째, 서비스 플랫폼은 안전한 개방형 플랫폼 가이드라인, 인증과 키 관리에 최소한의 보안 기술 및 리소스 사용, 정보 사용 정책과 필터링 정책 등으로 보안 요구사항을 충족한다.

4.2 IoT 보안 별 관리 방안

IoT 개발 장치의 보안 취약점을 해결하기 위한 관리 방안으로는 다음과 같다. 첫째, IoT 장치를 인터넷에 직접 연결하지 않는다. 둘째, 인터넷에 직접 연결되는 특정 장치를 사용해야 하는 경우에는 차단된 별도의 시스템으로 격리한다. 셋째, 민감한 데이터처리 및 장치 관리는 관련 보안 장치 및 소프트웨어 등을 개별적으로 탑재하여 운용한다.



(그림 5) 사물인터넷 보안위협과 보안요구사항

위 (그림 5)는 사물인터넷 구성 요소 중 인증 프로세스를 예로 한 보안 관리 프로세스를 보여주는데 자세한 설명은 다음과 같다[9].

1) 식별 (Identification): 식별은 주체가 시스템으로 식별자를 요청하여 정당한 사용자임을 검증한다. 시스템은 검증에 필요한 식별자를 사용자에게 요구할 수 있으며 이는 문자, 숫자 등을 조합

하여 Login ID형태로 사용된다. 식별자는 책임 추적성에도 중요하기 때문에 개인 식별자는 서로 다른 사용자 간에 중복되지 않도록 하여야 한다. 사용자는 식별자를 타인과 공유하는 것을 지양해야 하고 개인과 관련된 정보라면 가급적으로는 사용하지 않도록 해야 한다. 그 이유는 공격자가 소셜 네트워크 혹은 사회공학적 기법으로 수집된 개인 정보를 조합하여 식별자를 유추할 수 있기 때문이다.

2) 인증 (Authentication): 사용자가 정보에 접근할 때 정당한 자격이 있는지 검증하는 과정이다. 이를 통해 시스템과 관련이 없는 외부 접근자 구분이 가능하며 인가되지 않은 사용자들이 정보에 접근하는 것을 1차적으로 방지한다.

3) 인가 (Authorization): 인증된 사용자가 어느 정도의 권한을 가지는지 검증하는 단계이다. 한 시스템에서 사용자마다 정보의 접근권한이 다를 수 있으며 인증되었다고 하더라도 모든 정보를 공개하지 않고 단계적으로 공개하도록 구축할 수 있다.

4) 책임추적성 (Accountability): 책임추적성은 검증된 사용자가 정보접근 및 어떻게 사용하였는지 기록하는 것이다. 이를 통해 시스템에서 정보를 사용한 행위자의 행동을 추적할 수 있으며 정보사용의 책임을 명확히 할 수 있게 해준다.

이상의 레거시 보안 방식을 유지하면서 자율주행차량 등 새로운 사물인터넷 기반 서비스에 적용가능한 블록체인기술 시나리오는 다음 절과 같다.

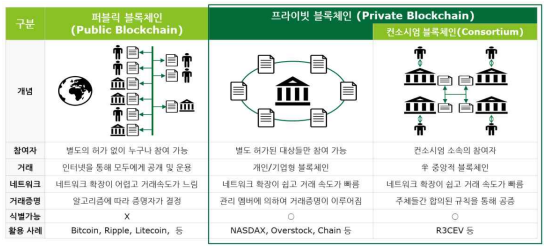
4.3 IoT 서비스 시나리오에 적용가능한 블록체인기술

사물인터넷의 블록체인 기술 적용을 구체적인 예를 통해 살펴보면 다음과 같다.

최근 블록체인 연구가 활발히 진행 중인 자율주행차량 시장에서는 각 주행 차량에 구현된 인포믹스 장치 및 펌웨어 등을 사물인터넷의 각 노드로 가정한다.

이 경우, 자율주행차량 시장의 경우 실시간의 차량데이터 등이 업데이트됨에 따라 궁극적으로는 퍼블릭 형태의 블록체인 생태계로 발전할 것으로 사료된다.

아래 (그림 7)은 자율주행차량의 펌웨어 업데이트라는 구체적인 사례에서도 적용 가능한 블록체인 종류에 대한 설명이다. 우선, 퍼블릭 블록체인은 데이터 접근 또는 합의 방식에 불특정 노드 모두가 무차별적으로 접근할 수 있는 반면 프라이빗 블록체인은 특정 대상만 접근할 수 있다[10]. 퍼블릭 블록체인의 대표적인 예가 비트코인과 이더리움(2022년 머지 이전까지)이다.



(그림 7) 블록체인의 종류

프라이빗 블록체인은 구성원 내 특정 목적이나 서비스를 갖는 비즈니스에 적합하다. 서로 신뢰할 수 있는 노드만 네트워크에 참여하기 때문에 합의 방식에 기여한 것에 대한 보상이 필요 없다.

따라서 자율주행차량의 운행기록 등을 빅데이터로 되새김하는 선순환구조가 필요한 초기에는 허가된 내부 구성원들을 참여시키는 방식이 효과적일 수 있다. 프라이빗 환경에서 최적화된 합의에 따라 거래를 기록하고 무결성을 검증하여 블록을 형성시키면 불특정 다수의 실시간 노드 접근에 따른 보안 취약점을 극복할 수 있다.

코로나 등 비대면성이 강조되고 초기 고품질의 데이터를 통해 자율주행차량의 시험 운행 및 충분한 검증이 필요한 현시점에서는 보안이 중요하다. 따라서 이 글에서는 프라이빗 형태의 블록체인 하에서 합의방식에 따른 블록생성의 무결성을 검증한 이후, 퍼블릭 블록체인 시스템으로 확장하는 보안관리 절차를 다음과 같은 시나리오를 통해 구체적으로 제안한다.

첫째, 산업의 특성에 따른 퍼블릭/프라이빗/컨소

시엄 형태의 블록체인을 선별한다. 앞서 언급한 자율주행차량 등의 사물인터넷 기반 서비스는 하이퍼렛져 패브릭과 같은 프라이빗 블록체인 하에서 합의방식 및 노드구성을 제안한다.

자율주행차량 서비스는 다양한 탑승자의 바이오 센싱데이터, 주행기록 데이터, 운전 환경 데이터, 도로 등 센싱데이터, 주행 환경 중 하나인 날씨 데이터 등을 포함한다. 따라서 하이퍼렛져 패브릭과 같은 프라이빗 블록체인 하에서 합의방식 및 노드구성을 통한 아키텍처 설계로 보안성을 강화할 필요성이 있다. 또한 충분한 테스트베드를 사전에 실시하여 보안성을 검증할 수 있다.

둘째, 자율주행차량 또는 경찰청 등이 관리하는 CCTV의 펌웨어 데이터는 업데이트 전문 플랫폼을 구축하여 보안을 강화하는 방식이 요구된다.

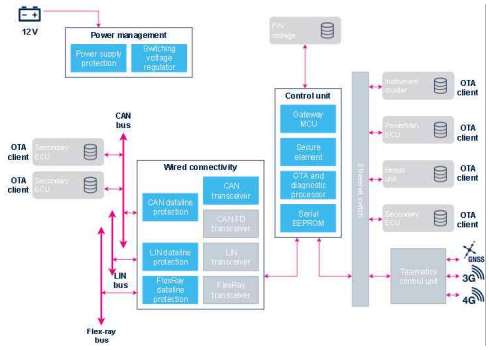
비대면으로 실시간 데이터의 획득이 요구되는 환경과 수집된 데이터에 따른 의사결정으로 실시간 비즈니스가 수행되는 다양한 산업에서 펌웨어 업데이트는 매우 중요한 업무 프로세스이다. 특히, 다양한 기업이 특정 IoT를 공유하여 사용하거나 이해관계가 있는 장비의 경우에는 더욱 보안이 중요하다. 예를 들어, IoT 기반의 교통신호시스템 중 거리에 설치된 교통 관측 기계, 교통 신호 기계, CCTV의 교통 정보 수집 기계, 무선 AP 등의 펌웨어 업데이트가 해킹이나 특정 기업의 이익에 따라 허락없이 업데이트가 된 것이 아님을 증명할 필요가 있다.

따라서 이를 블록체인 기반으로 업데이트를 수행하는 플랫폼을 통해 신뢰를 확보할 수 있다.

4. 제안된 시나리오 기반 펌웨어 업데이트에 대한 검증

사물인터넷 환경에서 무결성을 보장한 펌웨어 업데이트를 위한 시나리오는 다음과 같다. 앞장에서는 하이퍼레저로 시작하여 퍼블릭의 작업증명, 지분증명, 위임지분증명 등을 실증 및 검증하는 것을 제안하였다.

해당 제안을 실제 구현 사례인 OTA (over the air programming)로 설명하면 다음과 같다.



(그림 8) OTA(Over-The-Air)

(그림 8)의 OTA는 무선 환경에서 다양한 사물인터넷 디바이스에 대한 업데이트 플랫폼이다[11]. OTA는 세부 블록체인 모델, 트랜젝션, ACL, 쿼리 등의 블록체인 데이터 처리 및 운용에 적합한 구현 기술이다.

OTA와 같은 서비스 및 플랫폼은 보안성 강화가 요구되어야 하기 때문에, 첫 번째 단계로는 프라이빗 형태의 블록체인 시스템을 설계한다. 프라이빗 환경 하에서는 데이터 블록 생성과 트랜젝션을 처리가 검증된 노드(closed network)에서 수행되어 안전하다. OTA의 허가된 구성원(node) 간의 합의를 통해 최적의 트랜잭션 계약을 작성하고 배포(depoly)한다.

OTA 검증 시나리오는 사물인터넷 디바이스의 다양한 속성값과 필드값 등을 처리하는 무결성 검증 방식으로 효과적이다. 이와 같은 구현을 수행할 때, 하이퍼레저 패블릭 네트워크를 이용하면 오프체인과 온체인 네트워크 공격으로부터 상대적으로 안전하다. 이후 두 번째 단계로 퍼블릭 블록체인 환경은 콘소시엄 형태로 제공하여 보다 많은 불특정 노드의 참여를 가능하게 할 수 있다.

OTA와 블록체인을 응용한 기술을 자율주행차량에 적용하여 검증한다면 다음과 같이 구현할 수 있다. 첫째, 자율주행차량에서는 운전자의 개입 없이 자동차가 스스로 주행할 수 있는 자율주행차와 ICT 기술이 접목된 커넥티드카 등이 있다. 특히 자율주행차량의 사고 발생 시, 기존의 차량은 대부분 운전자의 과오이지만 자율주행차량은 제조사의 과오가 부각될 전망이다. 즉 자동차를 둘러싼

기술 환경 뿐만 아니라 보험과 자동차 사고 수사 등을 해야하는 경찰의 포렌식 등 자동차 관련 제도를 포함한 전반적인 패러다임이 변화하고 있다. 따라서 자율주행차량의 사고 등을 데이터 기반의 수사를 통해 경찰, 피해자, 가해자, 제조사, 보험사 등이 수긍할 수 있어야 하는데, 이때 활용할 수 있는 기술로 하이퍼레저 기반의 블록체인을 제안하였다.

둘째, 전기차와 자율주행차의 등장은 전장부품의 업데이트 빈도를 늘리고 있다. 즉 과거에는 자동차를 구매하면 1-2번 정도 서비스 센터에서 펌웨어를 업데이트하였다. 그러나 자율주행차량이 대중화되면 실시간으로 또는 훨씬 많은 빈도로 자율주행차량 내 여러 디바이스의 펌웨어 업데이트가 요구되낟. 해당 전자 제품 및 부품을 운영하는 소프트웨어사가 OTA기술로 펌웨어 등을 업데이트 할 수 있으나 안전하고 무결한 데이터의 검증 방안이나 정책은 제시되지 않았다. 구체적인 디바이스로는 기존의 내비게이션이나 인포테인먼트 등 차량 내 시스템을 향상해주는 '소프트웨어 OTA(SOTA)'와 동력 장치 등 차량 자체의 성능을 업그레이드해주는 '펌웨어 OTA(FOTA)'가 있다. OTA의 응용 서비스로는 서비스센터에 방문 없이 원격으로 차량 내 소프트웨어를 업데이트해주는 기술이다. 이 경우 해킹 등으로부터 안전한 정품 소프트웨어의 업데이트임을 확인하여 무결성을 보장할 필요가 있다.

즉 IoT기기에 필수적으로 포함되고 주기적으로 업데이트되어야 하는 펌웨어는 이 글에서 제안한 블록체인 검증 시스템으로 무결성을 보장받는다.

5. 결론

2022년 9월 이더리움 머지 이후, 작업 증명 알고리즘의 네트워크 공격 취약성은 획기적으로 줄어든 반면, 지분 증명 알고리즘에서의 네트워크 취약점이 증가하였다. 예를 들면 작업 증명에서는 51%의 해시 파워를 가진 작업증명자 또는 작업증명 집단에 의한 네트워크 공격이 가능했다. 반면, 이더리움 머지 이후에는 소수 거래소 또는 개인의 지분이 50%를 넘어서는 네트워크 공격에 따른 취약점이 대두되고 있다. 이상의 POW, POS 알고리즘 기반의 퍼블릭 블록체인은 네트워크 51% 공격에 취약하다.

따라서 사물인터넷에 대한 무결성을 강화한 IoT 비즈니스를 위해서는 프라이빗 또는 컨소시엄형 블록체인 서비스 형태로 구현을 제안한다.

이 글은 사물 인터넷 환경에서 블록체인의 무결성 보장 기술을 하이퍼레저 방식을 활용한 컨소시엄 구현 그리고 범용화서비스 후 퍼블릭 블록체인으로 전환할 경우에 참고할 보안 체크리스트 구성에 기여할 것으로 사료된다. 무결성을 담보한 보안 관리의 필요성에 부합하는 향후 연구와 블록체인 시스템 운용의 신뢰성 향상에 필요한 가이드라인 등이 후속 연구로 요구된다.

참고문헌

[1] Global Industry Analysts, Inc., Internet of Things (IoT) Monetization, May., 2021, https://m.giikorea.co.kr/report/go994651-internet-things-iot-monetization.html [Accessed: Oct. 05, 2022].

[2] Lior Gavish, "Data Lake vs Data Warehouse: 3 Key Differences", Monte carlo, August 24, 2022, https://www.montecarlodata.com/blog-data-lake-vs-data-warehouse/ [Accessed: Oct. 10, 2022].

[3] 산업연구원(KiET), '초연결시대 사물인터넷의 창조적 융합 활성화 방안', Oct., 2014. pp. 56-60.

[4] 우민지, '사물인터넷의 현재, IoT 산업 어디까지 왔나', SmartPC, Oct., 2014, https://www.ilovepc.co.kr/news/articleView.html?idxno=8822 [Accessed: Oct. 1, 2022].

[5] igloo, '한발 앞서 살펴보는 OWASP Top10 2021 Draft', 보안이슈, sep., 2021, https://owasp.org/Top10/ or https://www.igloo.co.kr/security-information/

%ED%95%9C%EB%B0%9C-%EC%95%9E%EC%84%9C-%EC%82%B4%ED%8E%B4%EB%B3%B4%EB%8A%94-owasp-top-10-2021-draft/ [Accessed: Oct. 7, 2022].

[6] Philipp Wegner, 'Global IoT market size grew 22% in 2021 – these 16 factors affect the growth trajectory to 2027', IoT Analytics, https://iot-analytics.com/iot-market-size/ [Accessed: Oct. 11, 2022].

[7] Million insights, 'Internet of Things (IoT) Security Market Analysis Report By Component, By Solution, By Services, By Application, By Security Type And Segment Forecasts From 2018 To 2025', 2020, pp.179, https://www.millioninsights.com/industry-reports/global-internet-of-things-iot-security-market [Accessed: Oct. 3, 2022].

[8] 김미희, 김영민, "블록체인 DPoS 합의 알고리즘을 활용한 IoT 장치 관리 시스템 개발", 전기전자학회논문지, 제23권, 제2호, 한국전기전자학회, June, 2019, p. 508.

[9] 미래창조과학부, '사물인터넷 정보보호 로드맵', Oct., 2014,https://securityin.wordpress.com/tag/internet-of-things/[Accessed: Oct. 10, 2022].

[10] 김상환, '블록체인에 기반한 금융업 혁신', Deloitte, jan., 2019,https://www2.deloitte.com/content/dam/Deloitte/kr/Documents/financial-services/2019/kr_fsi_issue-highlights_20190128.pdf.

[11] STlife,augmented, 'Smart Gateway and Firmware Over-The-Air (FOTA)'. https://www.st.com/en/applications/telematics-and-networking/smart-gateway-and-firmware-over-the-air-fota.html#overview.

〔저자소개〕

강 장 묵 (Jang Mook Kang)
1999년 2월 : 고려대학교 대학원 (경영석사)
2005년 8월 : 고려대학교 정보보호대학원(공학박사)
2020년 8월~현재 : 동국대학교 국제정보보호대학원 AI융합 보안 교수
2021년 4월~현재 : 극동대학교 해킹보안학과 교수

관심분야 : 인공지능, 블록체인, 융합보안, 산업보안