블록체인 기술을 활용한 사물 인터넷 플랫폼 인터워킹 프레임워크 모델 제안

김동규*, 김요한*, 권율*, 김호원*
*부산대학교 정보융합공학과
donggyu@islab.re.kr, yohan@islab.re.kr, kwonyool@islab.re.kr, howonkim@gmail.com

Proposal of IoT Platform Interworking framework model using blockchain technology

Dong-gyu Kim*, Yo-han Kim*, Yool Kwon*, Ho-Won Kim*
*Dept. of Computer Engineering, Pusan National University

요 약

최근 IoT 기술은 가전제품, 웨어러블 디바이스, 친환경 사업등 여러가지 분야에서 사용되고 있고 각 분야의 애플리케이션의 수와 애플리케이션에 연결된 장치 수가 증가함에 따라 엄청난 양의 데이터가 생성되고 있다. 수집된 많은 양의 데이터는 전송과 저장등의 과정을 거쳐야 하지만 현재 각기다른 여러가지 IoT 플랫폼들의 프로토콜들이 존재하고 있어 서로 다른 프로토콜 간의 데이터 전송이나 디바이스 연동이 힘들다는 문제점이 존재하고 있다[1]. 또한 센서로 수집된 데이터들이 중앙 집중식 구조로 저장되기 때문에 이 데이터들을 신뢰할수 있는가에 대한 문제가 존재한다. 이 문제들을 해결하기 위해 이 논문에서는 IoT 플랫폼에서의 서로다른 프로토콜간의 연동과 데이터들의 중앙 집중화 문제를 해결하기 위한 블록체인을 활용한 IoT 플랫폼 인터워킹 프레임워크 모델을 제안하고 이어 결론과 향후 연구방향을 제시한다.

1. 서론

최근 하드웨어 및 네트워크 관련 IoT(Internet of Things) 기술이 급속도로 발전함에 따라 다양한 산업 분야에서 IoT 기술의 활용 범위가 넓어지고 있다. 이에따라 데이터 무결성, 시스템 보안, 프로토콜에 대한 중요성이 높아지고 있다[2]. 가전 제품이 해킹되어 사생활 침해 및 피싱메일등의 피해가 이미 발생하였으며 확장된 규모에 비해 보안체계가 부족하여 IoT 는 해커들의 주요타겟이 되고 있다. IoT 네트워크는 기본적으로 중앙집중형의 구조로 되어있어 전적으로 네트워크를 관리하는 기관을 신뢰해야하는 문제가 존재한다. 본 논문에서는 IoT 플랫폼에서의 서로 다른 프로토콜간의 연동과 데이터들의 중앙집중형의 문제를 해결하기 위해 상호운용성과 탈중앙화의 성질을 가진 블록체인을 활용하여 IoT 플랫폼 인터워킹 프레임워크 모델을 제안하고 이어 결론과 향후 연구방향을 제시하였다.

2. 배경지식

2.1 블록체인

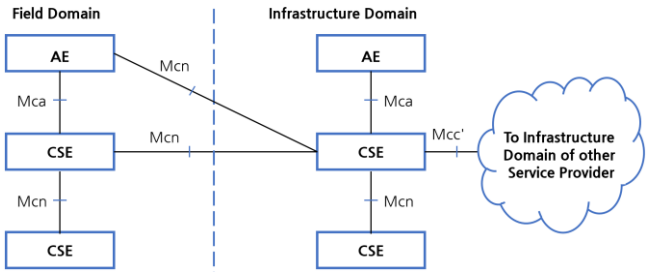
블록체인이란 다수의 거래내역이 담긴 블록을 해시를 이용하여 체인처럼 연결한 뒤 다수의 사람들이 복사하여 분산 저장하는 알고리즘을 뜻한다. 블록체인의 종류로는 퍼블릭 블록체인과 프라이빗 블록체인 그 둘을 섞은 혼합형 블록체인 하이브리드 블록체인이 있다. 컨소시움 블록체인이란 동일한 목적이나 가치를 가지고있는 다수의 기업과 단체들이 하나의 컨소시엄을 구성하고 그 안에서 작동하도록 만든 블록체인이다. 하이퍼레저 패브릭이 대표적이며 하이브리드 블록체인으로 분류하기도 한다. 블록체인이 가진 문제점으로는 저장되는 데이터가 네트워크에 참가하는 모든 피어들에게 공개되는 문제점이 존재할 수 있다.

2.2 하이퍼레저 패브릭

하이퍼레저 패브릭은 리눅스 재단이 주도하여 설립한 프라이빗 블록체인의 성격을 띄고 있다. 체인코드라는 스마트 계약을 최초로 호스팅한 분산원장 시스템이다. 하이퍼레저 패브릭의 PDC(Private Data Collection) 는 앞서 말한 블록체인의 개방성에 따른 민감 데이터처리에 도움을 줄 수 있다.

2.3 oneM2M

oneM2M 은 대표적인 서비스 플랫폼 표준으로, 기존의 산업 종속적이고 폐쇄적이고 파편화된 서비스 플랫폼 개발 구조를 탈피하고, 통합 공동서비스 플랫폼 환경을 개발하기 위한 목적으로 여러 주요 표준화 기구들에 의해 설립되었다.



[그림 1] oneM2M 기능 아키텍처와 참조점

oneM2M 의 아키텍처 참조 모델은 서로 다른 계층에서 작동하는 여러 엔티티를 제공하는데 [그림 1]과 같이 도식화하여 설명할 수 있다. 크게 기능 아키텍처(Entities)와 참조점(Reference Points)으로 나누어진다.

기능 아키텍처는 AE(Application entity entity), CSE (Common Services Eentity), NSE(Network Service Entity)의 세가지 기능을 포함한다. 먼저 AE 는 M2M 애플리케이션 서비스 로직을 제공한다. AE 의 예로는 원격 모니터링이나 원격 제어 프로그램 등이 있다. 다음으로 CSE 는 인스턴스화 된 M2M 환경 속에서 공통적으로 사용하는 CSF(Common Services Function)의 집합이다. 다른 CSE 또는 AE 에 CSF 를 제공하여 등록, 검색, 데이터 관리 및 보안 등의 서비스를 제공한다. 마지막으로 NSE 는 위치 서비스 및 장치 관리와 같은 기본 네트워크 서비스를 CSE 에 제공한다.

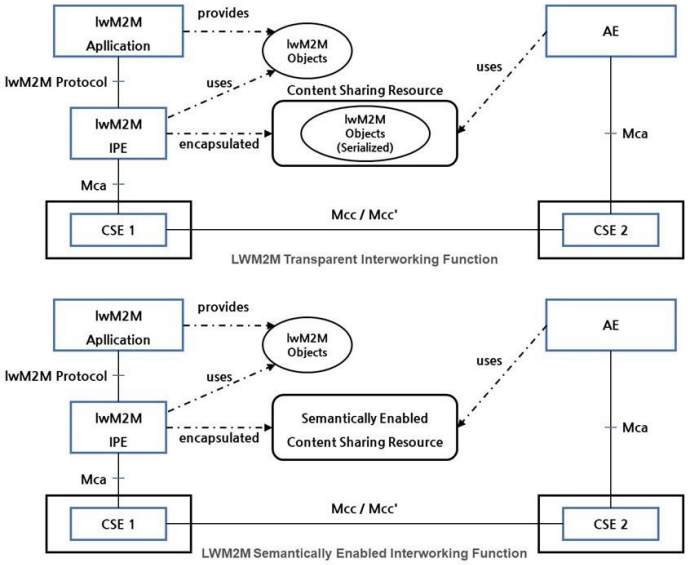
이러한 엔티티들은 여러 개의 인터페이스의 집합인 참조점을 사용하여 통신하는 것으로 CSE 가 다른 엔티티의 서비스를 이용할 수 있다.

2.4 LWM2M

LWM2M 은 IoT 디바이스나 constrained M2M 디바이스를 다루기 위한 프로토콜이다. LWM2M 은 모바일 산업을 위한 공개 표준을 개발하는 산업 표준 개발 기구인 OMA 가 경량 M2M 기능을 제공하기 위해 만들어졌다. 개발 목적에 따라 제약 조건이 있는 디바이스를 위해 효율적인 resource data model 을 지원하고, 네트워크 자원의 최적화를 통해 하나의 LWM2M 서버에 많은 수의 디바이스를 동시에 연결하고 제어할 수 있다.

2.5 IPE(Interworking Proxy application Entity)

LWM2M 과 oneM2M 이 협업을 하기 위해서 LWM2M 이 제공하는 서비스들을 oneM2M 이 이용할 수 있도록 번역하는 과정이 필요하다. 이 과정을 지원하는 것이 IPE 다[3]. 먼저 LWM2M 어플리케이션은 LWM2M 프로토콜을 사용해서 LWM2M IPE 로 LWM2M 객체를 제공한 후, LWM2M IPE 는 LWM2M 서비스를 oneM2M 자원으로 노출시킨다.



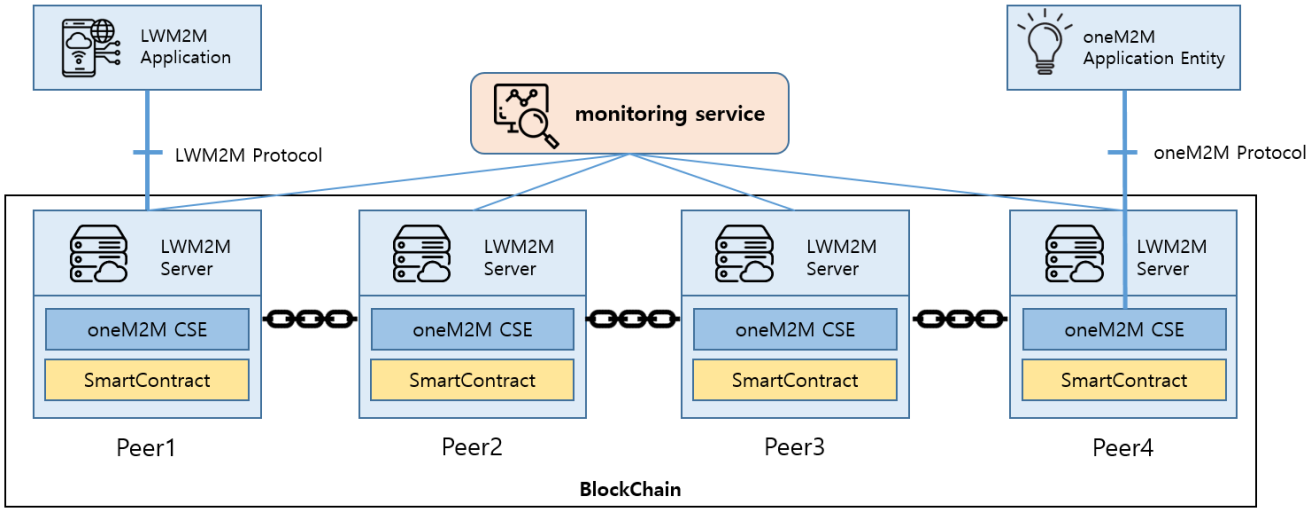
[그림 2] Transparent 모델과 Semantic Enabled 모델

둘의 협업은 LWM2M Application 과 IPE 의 AE 가 Mca 참조점을 통해 lwM2M 의 CSE 에 등록한 뒤, Mcc/Mcc' 참조점을 통해 oneM2M 의 CSE 와 통신하는 구조로 이루어진다. lwM2M IPE 는 [그림 2] 처럼 두 가지 interworking model 을 지원하고 있다.

먼저 Transparent 모델에서, LWM2M IPE 는 이 객체를 캡슐화해서 'Content Sharing Resource'에 넣고 LWM2M 과 oneM2M 의 AE 들이 서로 사용할 수 있도록 CSE 가 Content Sharing Resource 를 호스팅 할 수 있도록 만든다.

다음으로 Semantic Enabled 모델에서, lwM2M IPE 는 콘텐츠 공유 리소스에서 LWM2M 객체를 캡슐화한 다음 AE 에서 사용할 Mca 참조 점을 사용하여 CSE 가 콘텐츠 공유 리소스를 호스팅 하게 만든다. AE 는 Mca 참조점을 사용하여 리소스를 호스팅하는 CSE 의 콘텐츠 공유 리소스에 접근한다. AE 가 콘텐츠 공유 리소스를 받으면 AE 는 AE 의 목적을 위해 콘텐츠 공유 리소스에서 LWM2M 객체를 추출한다. 이때 AE 는 oneM2M 에서 정의한 Semantic Ontology 를 사용하여 추출한 정보를 인코딩한다.

3. 제안 모델



[그림 3] Blockchain Platform with IPE

이 논문에서 제시하는 모델은 위의 [그림 3]과 같다. 이 모델에서는 앞서 설명한 대표적인 IoT 프로토콜인 oneM2M 프로토콜과 LWM2M 프로토콜을 블록체인을 이용하여 연동하고 센서로 수집된 데이터들이 중앙 집중식 구조로 저장되는 것을 막기 위해 블록체인을 적용한다. 모델에서 사용하는 블록체인은 Consortium 블록체인인 하이퍼레저 패브릭을 이용해 구축하며 블록체인의 각 피어에는 LWM2M 프로토콜로 전송된 데이터를 수신하는 LWM2M 서버와 oneM2M 플랫폼의 디바이스를 제어하기 위한 oneM2M CSE 가 실행중이다. 이 LWM2M 서버와 oneM2M CSE 는 항상 필수적인 것은 아니며 각 피어에서 서비스에 필요한 프로토콜에 따라 선택적으로 실행할 수 있다. [4]의 연구에서 제안한 모델은 oneM2M CSE 에서 블록체인 API 를 통해 블록체인에 데이터를 전송하고 받아오는데 블록체인의 역할이 제한되어 있지만 이 모델에서는 CSE 를 피어로 직접 참여 시키기 때문에 탈 중앙화의 목적을 더 잘 이룰수 있다. 블록체인을 구성하는 전체 피어에는 LWM2M 프로토콜로 전송된 데이터를 oneM2M 디바이스가 이용할 수 있도록 맵핑해주는 스마트 컨트랙트가 설치되어있다. 이 스마트 컨트랙트를 실행하고 합의과정을 거쳐 블록체인에 맵핑된 데이터를 저장할 수 있고 반대로 블록체인에 저장된 데이터를 불러올 수 도 있다. 스마트 컨트랙트를 통해 저장되는 데이터가 네트워크에 참가하는 모든 피어들에게 공개되는 문제점이 존재할 수 있지만, 하이퍼레저 패브릭의 PDC(Private Data Collection)과 같이 민감한 데이터를 다루는 방법으로 문제를 해결 할 수 있다. 또한 하이퍼레저 패브릭의 모니터링 도구 grafana 나 explorer 를 사용하여 전체 블록체인의 데이터나 각 피어별 상태를 모니터링할 수 있는 서비스를 제공한다.

기존의 IPE 는 LWM2M 서버와 oneM2M AE 를 함께 가지고 있어 oneM2M AE 와 oneM2M CSE 사이 Mca 포인트가 필요하지만 이 모델에서는 oneM2M CSE 가 모두 블록체인의 피어로 참여하고 있기 때문에 Mca 포인트를 통한 통신이 필요하지 않고 블록체인의 스마트 컨트랙트 실행을 통해 서로의 데이터를 읽을 수 있다. 모델의 구체적인 동작 순서는 다음과 같다.

1) oneM2M CSE 를 피어로 블록체인을 구성하여 스마트 컨트랙트를 설치한다.
2) LWM2M Application 에서 피어의 LWM2M Server 로 LWM2M Protocol 을 통해 데이터를 전송한다
3) 전송된 데이터는 블록체인 네트워크에 설치된 스마트 컨트랙트를 통하여 oneM2M 데이터로 맵핑되어 저장된다.
4) 데이터가 저장될 때 하이퍼레저 패브릭의 이벤트가 발생하여 oneM2M CSE 로 전송된다.
5) oneM2M CSE 는 이벤트를 수신하여 연결된 oneM2M Application Entity(AE)로 oneM2M Protocol 을 이용해 데이터를 전송한다.

이와 같은 동작을 통해 LWM2M 프로토콜로 전송된 데이터를 oneM2M 플랫폼과 연동할 수 있어 블록체인 플랫폼이 IPE(Interworking Proxy application Entity)의 역할을 할 수 있고, 모든 oneM2M CSE 가 같은 데이터를 가지고 있어 데이터의 접근성이 높아진다. 또 블록체인을 사용함으로써 네트워크에 참여하지않는 제 3 자가 데이터를 조작하기가 매우 힘들어져 보안

상의 이점도 얻을 수 있다.

4. 결론

이 논문에서 제안한 모델을 통해 여러가지 IoT 플랫픔을 통해 수집된 데이터들을 블록체인을 이용해 IPE(Interworking Proxy application Entity)의 역할을 하도록 구현된 스마트 컨트랙트를 통하여 변환함으로써, 서로 연동할 수 있고, 데이터를 블록체인에 저장하여 기존의 중앙집중식 저장방식에서 발생하는 데이터의 신뢰 문제와 보안 문제를 해결할 수 있다. 하지만 더 많은 IoT 플랫폼을 지원할 경우 피어에 여러 종류의 플랫폼이 각각 구축되어야 해 오버헤드가 발생할 수 있어 추후 연구가 필요하다.

5. 향후 연구

이 논문에서 제시한 모델은 Consortium 블록체인을 써서 구현하여 사설 IoT 망에서의 사용을 목표로 하였다. 하지만 많은 참여자가 참여하여 데이터를 공유하고 검증하는 경우에는 Consortium 블록체인 만으로는 한계가 있다. 따라서 향후 연구에서는 IoT 서비스에 누구나 참여할 수 있도록 공개된 Public 블록체인(ex. Ethereum)을 사용하여 IPE 모델을 제시할 필요성이 있고. 또한 현재 모델은 두 개의 서로다른 IoT 플랫폼을 다루었지만 더 많은 플랫폼을 지원하도록 확장또한 고려하여 모델을 제시할 예정이다.

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2022-2020-0-01797)

6. 참고문헌

[1] YUN, Jaeseok, et al. Towards Global Interworking of IoT Systems--oneM2M Interworking Proxy Entities. In: *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*. 2015. p. 473-474.

[2] L-TURJMAN, Fadi; ZAHMATKESH, Hadi; SHAHROZE, Ramiz. An overview of security and privacy in smart cities' IoT communications. *Transactions on Emerging Telecommunications Technologies*, 2022, 33.3: e3677.

[3] KAUSHAL, Sakshi, et al. Interworking of M2M and oneM2M. In: *2022 International Conference for Advancement in Technology (ICONAT)*. IEEE, 2022. p. 1-5.

[4] LEE, ChangHyung, et al. Towards a Blockchain-enabled IoT platform using oneM2M standards. In: *2018 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2018. p. 97-102.