

# 블록체인 기술을 이용한 IOT 보안 향상 기법

조익현\*, 이근호\*, 김승호\*, 한성수\*\*, 박진수\*\*\*

\*백석대학교 정보통신학부

\*\*순천향대학교 웰니스코칭서비스연구센터

\*\*\*순천향대학교 컴퓨터소프트웨어공학과

e-mail:whdlrgus8@gmail.com, root1004@bu.ac.kr, bayster0508@naver.com,  
postsky@sch.ac.kr, jpark2147@gmail.com

## A Scheme of IOT Security Enhancement Using Block Chain Technology

Ik-Hyun Cho\*, Keum-Ho Lee\*, Seung ho kim\*, Seong-Soo Han\*\*, Jin-Soo Park\*\*\*

\*Dept. of Information Communication, Baekseok University

\*\*Dept. of Wellness Coaching Service Center Professor, Soonhunhyang University

\*\*\*Dept. of Computer Software Engineering, Soonhunhyang University

### 요 약

현대의 모든 기기나 사물들은 인터넷과 연결이 되어 있어서 직접 조작을 하지 않아도 원격으로 쉽게 사물들을 조작할 수 있고, 사물들이 스스로 필요한 것들을 확인하여 사용자에게 알려주는 시대가 되었다. 사용자 생활면에서는 편리한 시대가 되었다고 볼 수 있다 하지만 보안면에서는 나쁜 의도를 가진 사용자들에게는 좋은 먹잇감이 되었다. 이 논문에서는 해킹을 시도하거나 다른 사람에게 손해를 끼치려는 사람들을 방지하기 위해 블록체인의 보안 기술을 이용하여 IOT의 보안 기능을 향상하는 논문을 작성하려고 한다.

### 1. 서론

블록체인은 기존의 중앙체제에서 운영하던 데이터를 네트워크 내의 모든 클라이언트가 공동으로 소유하고 확인함으로써 거래 기록의 무결성 및 신뢰성을 확보하고 있다. 블록체인이 단순히 암호 화폐 실현을 위한 기술이라는 한계를 뛰어넘어, 데이터의 진위성 여부를 중앙 집중 체제의 인증기관을 거치지 않고 해결할 수 있는 인프라 기술로서의 잠재력을 갖추고 있고, 시각을 넓히므로 다양한 산업 영역에 대한 적용 가능성이 발견하고 있다. 사물 간의 통신을 하는 개념인 IoT의 발전은 우리의 삶에 새로운 편리성, 효율성을 가져왔다. IoT 기술을 통해서 기존의 사람과 사람 사이에서만 이루어지던 통신이라는 개념이 육성에서 정보로, 그 정보가 기기에서 사람, 사람에게서 사람을 뛰어넘어, 사물이라는 개념으로 발전되었다.[1] 하드웨어, 소프트웨어 및 네트워크 관련 IoT 기술이 빠른 속도로 성장함으로써 여러 산업 분야에서 IoT 기술의 활용 빈도의 범위가 넓어지고 있다. 그에 따른 IoT 기술에 있어서 데이터의 무결성 검사, 시스템 보안 기술, IoT 기기 제어에 대한 중요성이 대두되고 있다. 특히 IoT 기술을 기반으로 하는 유통산업에서 활발한 도입 현상을 보여주고 있다. IoT 기술은 최적화된 환경을 제공하여 사용자의 편리함과

효율성 증가라는 특징이 있지만, 기기 간의 신뢰성, 안정성 및 기기 제어와 정보의 무결성 검사 그리고 클라이언트 해킹 및 사생활 침해 등과 같은 피해 때문에 보안에 관한 중요성이 중요시되고 있다. IoT 기기들이 제대로 된 보안 조치 없이 방치되어 공격에 취약하게 노출되어 있다.

### 2. 관련연구

#### 2.1 블록체인

블록체인은 위변조를 판단하기 위해 거래 정보들이 모인 블록의 해시를 만든다. 해시를 만들 때마다 이전 블록의 해시값도 입력되어 현재 블록의 해시를 만들 때 영향을 미치게 된다. 이 블록들을 논리적으로 연결되어 이를 블록체인이라 부른다. 블록체인은 중앙 체제 방식인 클라우드와 비교되는 네트워크 구조로 되어 있다. 네트워크 클라이언트들은 분산된 구조 형태로 모든 정보를 가지고 있고, 중앙 서버에 정보를 모아서 정보를 처리하는 클라우드 방식과 다른 방식으로 동작을 한다. 블록체인의 분산형 구조는, 클라우드 방식과 비교해서 3가지 특징을 가지고 있다.[2]

첫 번째, 위변조 방지이다. 블록체인이 데이터 정보를 한

곳에 저장하지 않고 분산된 형태로 분산배치 했기 때문에 데이터 정보가 위변조될 가능성이 매우 낮다.

두 번째, 투명성이다. 블록체인은 중앙서버에 관리하는 형태가 아니다. 모든 사용자가 데이터 정보를 가지고 있다.

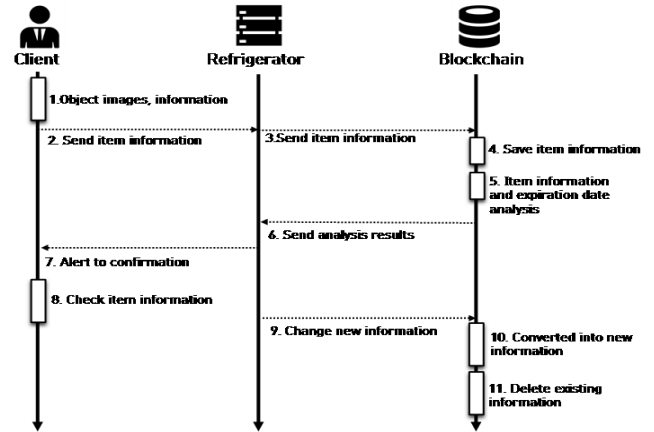
세 번째, 비용감소이다. 중앙체제에서는 서버에 저장한 정보를 보호하기 위해서 보안 시스템들을 운영한다. 그러므로 보안에 필요한 인력 및 유지비가 소모된다. 정보를 서버에 저장하는 방식이 유지비용을 소모하게 한다. 그러나 블록체인 방식은 중앙체제가 필요하지 않은 방식이기 때문에, 중앙서버에 소모되는 유지비용이 적게 든다.

### 2.2 IoT(Internet of Things)

IoT는 적용을 어느 분야에 하나에 따라 개인, 공공, 산업으로 분류된다. 산업 IoT는 산업적 활용에 주목적을 두었다. 실시간으로 주변 정보를 수집해주는 센서 노드, 연결된 여러 센서로부터 모은 정보를 마스터 노드에 전달시켜주는 싱크노드, 싱크노드로부터 받은 정보를 병합, 수정 및 가공하여 클라우드 서버로 전달하는 마스터 노드로 구성된다. 유럽에서는 IoT를 고유의 클라이언트 및 가상의 인격을 가지고 있는 생각 할 수 있는 인터페이스를 통하여 주변 환경들과 연결 및 소통할 수 있는 사물이라고 이야기하고 있다. 우리나라 방송통신위원회에서는 IoT는 사물 지능통신과 비슷한 개념으로 '사람 대 사물, 사물 대 사물간 통신 서비스를 시간과 장소에 구애받지 않고 안전하고 편리하게 실시간으로 이용 가능한 미래 방송 통신 융합 ICT 인프라라고 이야기하고 있다. IoT 보안위협 종류에는 단말기 분실 및 물리적 기기 파괴, 무선 신호의 교란, 자료의 유출, 정보 위, 변조, 서비스 거부 공격 등이 있다.[3] 블록체인 기술을 이용한다면 자료의 유출, 정보 위, 변조 등 정보 보안에 대해서는 안전할 것이다.

### 3. 블록체인 기술을 이용한 IoT기술

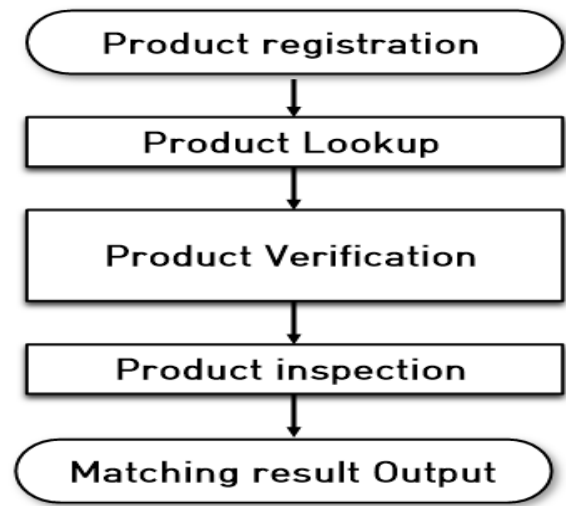
IoT는 사람과 사람, 사람과 사물 가릴 것 없이 모든 것이 네트워크에 연결된 사회이다. IoT에 연결된 네트워크가 해킹당한다면 기존 해킹 사고와는 비교가 안 될 거대한 해킹 사고로 이어질 것이다. IoT 사회를 연결하는 네트워크는 보안이라는 큰 중요 점을 갖고 있다. IoT 환경에서 발생할 수 있는 문제점들은 기존의 통신환경에서 나타났던 문제점들을 포함하고 있다. 그렇기 때문에 IoT 환경에서는 보안이 매우 중요하고 가장 대두 되는 문제이다. 블록체인 기술을 적용한 냉장고 IoT 기기를 나타내는 과정은 그림 1.과 같다.



(그림 1) 블록체인 기술을 이용한 냉장고 IoT 사물

1. 클라이언트는 새로운 제품을 냉장고에 넣고 정보를 입력한다.
2. 냉장고 IoT는 정보를 블록체인에 정보를 전송한다.
3. 블록체인은 새로운 제품의 정보를 저장한다.
4. 제품의 정보와 유통기한을 확인한다.
5. 분석한 정보를 IoT에 전송한다.
6. 클라이언트는 정보를 다시 확인한다.
7. 클라이언트가 새로운 제품을 입력한다.
8. IoT에서 새로운 제품에 대한 정보를 블록체인에 입력한다.
9. 블록체인은 기존 제품의 정보를 삭제한다.

그림 1.과 같이 사용자가 제품을 IoT에 입력을 하면 그 정보가 블록체인에 전송이 되어 해커에 의한 해킹이 불가능하게 만드는 것이다.



(그림 2) 블록체인 기반 IoT 알고리즘

그림 2.은 IoT에서 블록체인의 동작 과정이 어떻게 작동이 되는지 나타내는 프로세스 과정을 플로우 차트로 나타낸 것이다.

#### 4. 결론

IoT 기술에 블록체인 보안 기술을 적용한다면 기존에 존재하던 IoT 보안 취약점 문제를 해결 할 수 있을 것이다. 하지만 IoT 네트워크라는 특수한 환경에 기존의 블록체인을 적용하기에는 문제점이 있다. 기존 블록체인 동작 원리는 IoT 환경에서 적합하지 않다. 다양한 사물이 존재하는 IoT 환경에서 이러한 구조는 적합하지 않기 때문이다. IoT 플랫폼에 블록체인 연동기술이 미숙하다. 블록체인 내에서 IoT 기기 인식 및 클라이언트 검증 기술이 미흡하다. IoT 네트워크의 안전한 블록체인 시스템 도입을 위해서는 연구 및 발전이 되어야 한다. IoT 네트워크 환경에 최적화된 블록체인 연구 개발이 필요하다. 신뢰성 기반의 블록체인 연동 기술 개발이 필요 하다. 여러 대의 디바이스가 네트워크를 공유하는 만큼 기기 식별 기술 및 기기 제어, 접근 권한 및 노드를 식별할 수 있는 기술의 개발 및 연구가 진행되어야 한다.[4] 다음 논문에서는 구체적인 프로토콜과 알고리즘을 개발하여 작성을 할 것이다.

#### Acknowledgement

2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(NRF-2016R1D1A3B03935976)과 2018년도 산학협동재단 학술 연구비 지원사업으로 수행한 결과물임.

#### 참고문헌

- [1] Y. H. Kim, J. K. Yang, H. B. Kim, "M2M/IoT의 동향과 보안위협", Korea Institute Of Information Security And Cryptology 24(6), Vol 12, pp.48-59, 2014. 12.
- [2] H. Y. Kim, "Analysis of Security Threats and Countermeasures on Blockchain Platforms", Korean Institute of Information Technology 16(5) Vol 10, pp.103-112, 2018. 05.
- [3] D. H. Kim, S. O. Yun,, O. P. Iee, "IoT 서비스를 위한 보안", The Journal of The Korean Institute of Communication Sciences 30(8), Vol 7, pp.53-59, 2013, 07.
- [4] H. J. Kang, H. R. Kim, S. P. Hong, "A Study on the Secure Blockchain systems based on IoT", Korea Institute Of Communication Sciences Vol 2, pp.66-67, 2017, 06.