블록체인 기반 IoT 클라우드 시스템에 대한 연구동향 및 고찰

김태우*, 박종혁*
*서울과학기술대학교 컴퓨터공학과
tang_kim@seoulteh.ac.kr, jhpark1@seoultech.ac.kr

Research Trends and Considerations for Blockchain-based IoT Cloud Systems

Tae Woo Kim*, Jong Hyuk Park*
*Dept. of Computer Science and Engineering, Seoul National University of Science and Technology

요 약

클라우드는 가상화 기술을 사용한 리소스의 유연성과 뛰아난 접근성을 장점으로 빅데이터, 딥러닝 등 여러 분야에서 클라우드를 사용하고 있다. 최근 클라우드와 결합된 IoT 시스템을 통해 시스템 관리, 데이터 처리 및 저장, 데이터를 이용한 빅데이터 활용 등 여러 방법으로 사용 할 수 있어 많은 관심을 받고 있다. 그러나 IoT 클라우드의 많은 활용에 따라 대규모 시스템화, 여러 사용자의 개인정보 저장 등의 이유로 많은 공격자의 표적이 되고있다. 여러 공격자의 공격을 방아하기 위해 IoT 클라우드 시스템은 블록체인, 보안 IoT 디바이스, 변형된 클라우드 모델등 여러 연구가 진행되고 있다. 본 논문에서는 최근 연구되고 있는 블록체인, 클라우드, IoT 시스템의 동향에 대해 조사하고, 기존에 연구되었던 기술을 바탕으로 효과적인 블록체인 기반의 IoT 클라우드 시스템을 제안한다. 제안하는 IoT 클라우드 시스템은 블록체인 기술을 사용하여 보안정책을 관리할 수 있어 신뢰성이 높으며, 클라우드 시스템이 작동하지 않을 경우 페일오버 기능을 수행할 수 있어 가용성이 뛰어나다.

1. 서론

클라우드는 가상화 기술을 사용하여 컴퓨팅 리소스를 유연하게 사용할 수 있는 유연성과 언제 어디서든 접근할 수 있는 뛰아난 접근성을 장점으로 빅데이터, 딥러닝 등 여러 분야에서 클라우드를 사용하고 있다. 최근 IoT 시스템과 클라우드와 결합하여, 시스템 관리, 데이터 처리 및 저장, 데이터를 이용한 빅데이터 활용 등에 사용하는 IoT 클라우드로 많이 사용되고 되고 있다.

IoT 클라우드의 많은 활용에 따라 클라우드를 이용한 대규모 시스템 관리하는 사례가 많아지고, 많은 사용자들의 정보가 저장되어 있어 공격자의 주요 표적이 되고 있다. 이러한 IoT 클라우드를 보호하기 위해 블록체인 기술, 여러 종류의 클라우드 시스템, IoT 기술 등 각 분야에서 활발한 연구가 진행되고 있다.

본 논문에서는 최근 연구되고 있는 블록체인, 클라우드, IoT 시스템의 동향에 대해 조사하고, 기존에 연구되었던 기술을 바탕으로 효과적인 블록체인 기반의 IoT 멀티 클라우드 시스템을 제안한다. 제안하는 IoT 멀티 클라우드 시스템은 IoT 계층을 관리하는 단일 클라우드들을 블록체인기반의 통신채널을 구성하여 멀티 클라우드로 사용한다. 멀티 클라우드에서 클라우드 보안정책, IoT 보안정책 등을 블록체인을 사용하여 신뢰성 있는 제어 데이터를 보장하며, 하나의 클라우드가 운영 중단이 발생했을 때 다른 클라우드를 이용하여 시스템을 유지할 수 있는 페일오버 기능을 수행할 수 있어 가용성이 뛰어나다는 장점을 가지고 있다.

2. 관련 연구

2.1 블록체인

블록체인은 데이터들이 저장된 집합체인 블록을 Peer to Peer (P2P) 방식을 사용한 체인 형태의 연결고리를 사용해 연결한 분산원장기술이다[1]. 블록체인을 사용한 네트워크에 데이터를 저정하면 저장하여 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있어 데이터의 신뢰성과 무결

성을 보장한다. 클라우드 모델에서 일반적으로 데이터에 대한 신뢰성을 확보하기 위해 사용되며 이에 대한 활발한 연구가 진행되고 있다.

Dai 등은 블록체인과 IoT를 결합한 Blockchain of Things (BCoT)을 제안했다[2]. BCoT는 Blockchain composite layer, Communication layer, Perception layer로 구성되어 있다. 그 중 Blockchain-composite layer는 다양한 산업 응용 프로그램을 지원하기위해 여러 블록체인 기반 서비스를 제공하여 산업용 애플리케이션 개발의 어려움을 낮출 수 있다. 또한 Blockchain-composite layer을 통해 IoT 시스템의 열악한 상호 운용성, IoT 장치의 리소스 제약, 개인 정보 보호 및 보안 취약성과 같은 많은 문제를 해결할 수 있다.

BARENJI 등은 클라우드 제조 제공 업체를 위한 블록체인기반의 분산형 P2P 네트워크를 제안했다[3]. 제안한 P2P 네트워크는 Core layer, Blockchain Network layer, Cloud manufacturing layer로 구성되어 있다. Blockchain Network layer에서 블록체인 노드는 사용자 수를 기반으로 생성되며 각 노드에는 원장의 로컬 사본이 저장되어 있어 거래자의 계약을 조정하고 검증하는 역할을 한다. 따라서 노드 간의 메시지에 무결성을 제공하고 관련 권한이 있는 엔티티에 의해서만 작업이 수행되도록하여 메시지의 신뢰성을 보장한다.

2.2 클라우드

클라우드는 가상화 기술을 사용하여 하나의 컴퓨팅 자원을 여러 개의 컴퓨팅 자원으로 나눠 각 사용자에게 제공하는 컴퓨팅 기술이다[4]. 필요에 따라 컴퓨팅 자원을 증가시키거나 감소시킬 수 있어 유연성이 뛰어나고, 언제 어디서든 인터넷을 통해 접근할 수 있어 접근성이 높다. 여러 사용자의 데이터가 하나의 클라우드에 저장되므로 공격자의 주요 표적이 되고 있어 안전한 클라우드 모델을 위해 많은 연구가 진행중이다.

Chadwick, 등은 데이터 공유 인프라를 위해 신뢰 모델을 사용한 C3ISP 에지 클라우드를 제안했다[5]. 효과적인 사이버 보안을 제공하기위해 관련된 모든 주체 간의 사이버 위협 정보 (CTI) 공유를 통한 공격 분석은 필수적이다. 그러나 민감한 기밀 보안 정보가 공개 될 수 있어 CTI의 공유에는 어려움이 있다. 제안한 에지 클라우드에서는 협업 및 기밀 정보 공유, 분석을 위한 C3ISP 프레임 워크를 에지 계층에서 사용한다. 또한 저장, 공유 및 분석은 완전히 분산 된 방식으로 이루어지며, 분산 해시 테이블 (DHT) 기반 모델을 활용하여 통신, 정보 배포 및 계산을 수행하여 적절한 신뢰 수준과 CTI 데이터 삭제 접근 방식 사용할 수 있다.

Li 등은 신원 기반 PDP 방식의 다중 복사를 이용한 멀티 클라우드를 제안했다[6]. 멀티 클라우드느 2개 이상의 클라우드를 사용한 클라우드 접근 방식이다. 기존 클라우드에서는 다중 사본의 무결성을 보장하기 위해 다중 사본에 대한 PDP 프로토콜을 제공한다. 그러나 대부분의 PDP 프로토콜은 모든 사본이 하나의 클라우드 스토리지 서버에만 저장되어 다중 복사의 의미가 없다. 또한 이전의 PDP 프로토콜은 많은 유형의 보안 취약성이 있으며 많은 통신 및 계산 비용을 초래하는 공개 키 인프라 (PKI) 기술에 의존한다는 문제점이 있다. 제안한 클라우드는 다중 사본의 무결성을 보장하기 위해 서로 다른 클라우드 스토리지 서버에 저장하며, Diffie-Hellman 연산을 통한 동형 검증 가능한 태그를 이용해 모든 사본의 무결성을 동시에 확인할 수 있다.

2.3 IoT 시스템

사물에 통신 기능을 내장하여 인터넷을 통해 데이터를 연결하고 교환할 수 있는 물리적 기기로 센서를 통해 데이터를 수집하거나 데이터를 출력할 수 있다[7]. 최근 스마트 홈, 스마트 팩토리과 같은 자동화 시스템 사용을 위한 주변 정보 수집을 위해 주로 사용되고 있으며, 대규모 IoT 장비의 트래픽문제, 데이터 신뢰성 보장을 위해 많은 연구가 진행되고 있다.

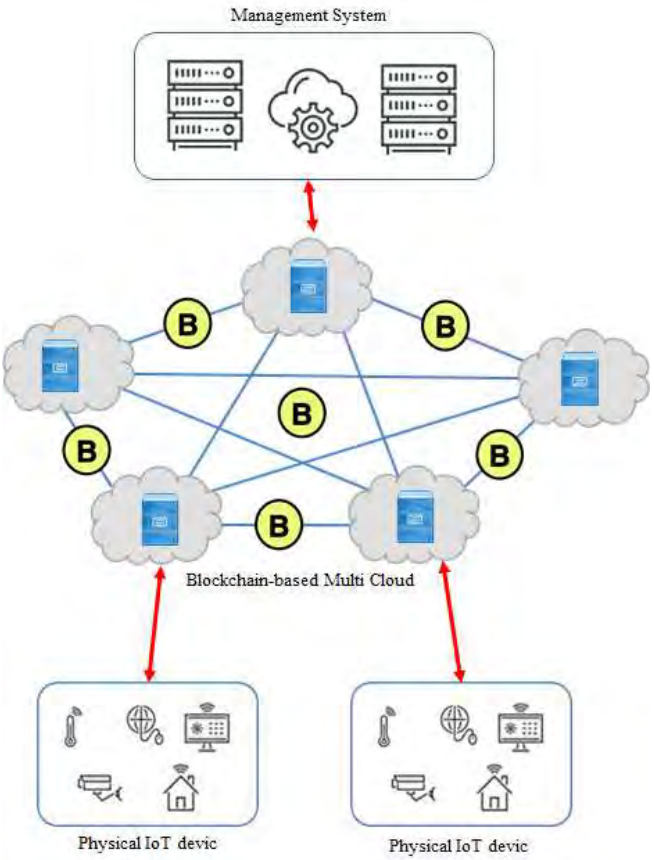
Farris 등은 Software Defined Network (SDN) / Network function virtualization (NFV) 기반 보호 접근 방식을 사용한 IoT 환경을 제안했다[8]. 제안한 IoT 환경에서는 전체 네트워크를 SDN으로 구성하며, 네트워크 인텔리전스를 SDN 컨트롤러로 대체한다. SDN의 네트워크 제어기능을 통해 네트워크 스위칭 장치의 복잡성을 감소시키고, 트래픽 흐름을 적절하게 수정하여 경보 발생시 빠르게 대응 가능하다. 또한 SDN은 프로그래밍 가능 환경을 만들어 외부 애플리케이션이 IoT 시스템 제어와 네트워크 동작을 정의 할 수 있어 유연성이 뛰어나다.

Bu 등은 민감한 정보를 쉽게 공유 할 수 있는

Threshold Secret Sharing (TSS) 기반의 IoT 시스템 체계를 제안했다[9]. 제안한 IoT 시스템 체계는 TSS를 사용하여 정보를 분할하여 시스템의 모든 장치에서 보관한다. 따라서 정보는 장치 그룹에서만 공동으로 검색 할 수 있어 데이터 신뢰성을 유지할 수 있다. 또한 TSS를 통해 손상된 장치를 식별할 수 있어 공격자가 IoT 장치를 공격, 위조하는 경우에도 데이터의 신뢰성을 유지 할 수 있다.

3. 블록체인 기반 IoT 멀티 클라우드 시스템

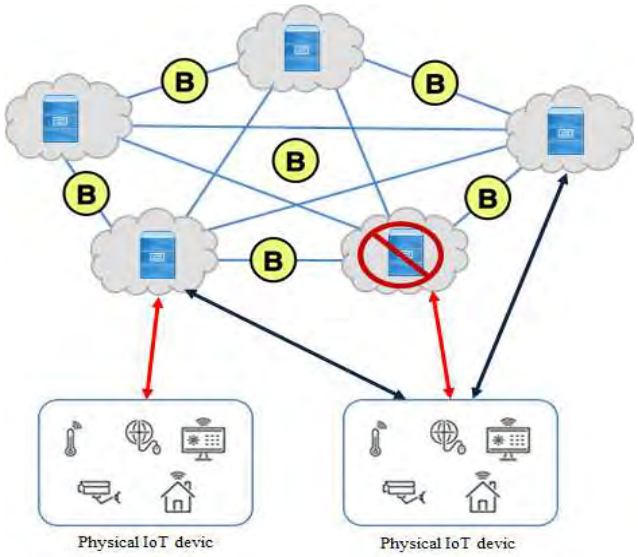
본 논문에서는 블록체인기반의 IoT 멀티 클라우드 시스템을 제안한다. 제안하는 시스템은 (그림 1)과 같이 IoT 장치 계층, 블록체인 기반 멀티 클라우드, 그리고 관리 시스템 계층으로 구성된다.



(그림 1) 제안하는 블록체인 기반의 IoT 멀티 클라우드 시스템

IoT 장치 계층은 물리적인 IoT 장치로 구성된 계층으로 데이터를 수집하여 클라우드로 전송하는 역할을 수행한다. 블록체인 기반 멀티 클라우드는 단일 클라우드로 구성되며 각 클라우드는 IoT 장치 계층과 연결하여 데이터를 수집한다. 수집한 데이터는 블록체인을 이용하여 주변 클라우드에 데이터를 복사하여 분산시켜 저장한다. 또한 관리 계층에서 설정한 IoT 보안정책을 각 IoT계층에게 제공하여 IoT 보안을 설정한다. 마지막으로 관리 시스템 계층은 각 클라우드의 보안정책과 클라우드와 연결된 IoT 장치에 대한 보안정책을 설정하여 멀티 클라우드에게 공유한다.

제안하는 블록체인 기반의 IoT 멀티 클라우드 시스템은 IoT 장치 계층을 관리하는 각 클라우드에 저장된 보안정책을 블록체인 기술을 사용해 멀티클라우드를 구성하는 모든 클라우드에 저장하여 보안정책의 신뢰성을 보장할 수 있다. 또한 (그림 2)와 같이 클라우드 시스템이 공격당해 사용이 불가능한 경우 멀티 클라우드를 구성하는 다른 클라우드에 공격당한 클라우드가 관리하는 IoT의 정보와 보안정책이 저장되어 있으므로 시스템에서 이상이 생겼을 때 예비 시스템으로 자동전환되는 페일오버 기능을 제공 할 수 있어 시스템의 가용성이 뛰어나다.



(그림 2) 멀티클라우드의 페일오버 기능 수행

4. 결론

클라우드는 가상화 기술을 통해 대규모 IoT 장치를 효율적으로 관리하고 제어 할 수 있어 현재 많은 IoT 시스템에서 클라우드를 사용한 IoT 클라우드 시스템을 사용하고 있다. IoT 클라우드 보안을 위해 클라우드 측면에서 C3ISP 에지 클라우드, PDP 방식의 다중 복사를 이용한 멀티 클라우드 등 이 연구되고 있으며, IoT 시스템 측면에서 TSS 기반 IoT

시스템, SDN/NFV 기반 보호 접근 방식을 사용한 IoT 환경 등이 연구되고 있다. 또한 IoT 클라우드의 데이터의 신뢰성 보장을 위한 Blockchain of Things (BCoT), 분산형 P2P 네트워크 등 블록체인 기술의 많은 연구가 진행되고 있다.

기존 IoT 클라우드 시스템의 경우 클라우드가 사용 불가능할 경우 IoT 시스템 전체가 사용할 수 없다는 문제점이 존재한다. 이러한 문제를 해결하기 위해 본 논문에서는 블록체인기반의 IoT 멀티 클라우드 시스템을 제안하였다. 제안한 시스템은 각 IoT 장치 계층을 관리하는 클라우드를 멀티 클라우드로 구성하며, 각 클라우드의 보안정책을 블록체인 기술을 사용하여 공유시켜 보안정책의 신뢰성을 보장한다. 클라우드 시스템이 작동하지 않을 경우, 멀티 클라우드를 구성하는 다른 클라우드가 페일오버 역할을 수행하여 높은 가용성을 제공하여 안전한 IoT 클라우드 시스템으로 사용할 수 있다는 장점을 가진다.

Acknowedgement

This study was supported by the Advanced Research Project funded by the SeoulTech(Seoul National University of Science and Technology)

참고문헌

[1] S. K. Singh, et al, "Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence", Future Generation Computer Systems, vol.110, pp.721-743, 2020.

[2] H. N. Dai, et al, "Blockchain for Internet of Things: A Survey", IEEE Internet of Things Journal, vol.6, no.5, pp.8076-8094, 2019

[3] A. V. BARENJI, et al, "Blockchain-Based Cloud Manufacturing: Decentralization", arXiv preprint arXiv, vol.1901, no.10403, pp.1003-1011, 2019.

[4] D. Y. Kim, et al, "A combined network control approach for the edge cloud and LPWAN based IoT services" Concurrency and Computation: Practice and Experience, vol.32, no.1, pp.e4406, 2020.

[5] D. W. Chadwick, et al, "A cloud-edge based data security architecture for sharing and analysing cyber threat information", Future Generation Computer Systems, vol.102, pp.710-722, 2019.

[6] J. Li, et al, "fficient identity-based provable multi-copy data possession in multi-cloud storage", IEEE Transactions on Cloud Computing, 2019.

[7] N. Y. Kim, et al, "A Survey on Cyber Physical System Security for IoT: Issues, Challenges, Threats, Solutions", Journal of Information Processing Systems, vol.14 no.6, pp.1361-1384, 2018.

[8] I. Farris, et al "A survey on emerging SDN and NFV security mechanisms for IoT systems", IEEE Communications Surveys & Tutorials, vol.21, no.1, pp.812-837, 2018.

[9] L. Bu, et al "A secure and robust scheme for sharing confidential information in IoT systems", Ad Hoc Networks, vol.92, 2019.