안전한 그룹 서명 및 인증 체계를 위한 블록체인 기반 모바일 엣지 컴퓨팅에 관한 연구

명재민[1], 유진호[2], 서대희[3]
[1]상명대학교 핀테크전공 학부생
[2]상명대학교 경영학부 교수
[3]상명대학교 지능데이터융합학부 교수
202110793@sangmyung.kr, jhyoo@smu.ac.kr, daehseo@smu.ac.kr

A Study on Blockchain-Based Mobile Edge Computing for Secure Group Signatures and Authentication

JaeMin MYEONG[1], Jinho YOO[2] ,Daehee SEO[3]
[1]Dept. of Fintech, Sangmyung University
[2]Faculty of Business Administration, Sangmyung University
[3]Faculty of Artificial Intelligence and Data Engineering, Sangmyung University

요 약

모바일 엣지 컴퓨팅 기술은 블록체인과 결합하여 모바일 기기의 낮은 컴퓨팅 파워를 보완함과 동시에 추적성, 무결성이 보장된 데이터베이스를 제공하기에, 미래 IoT 환경에서 중추적인 역할을 할 것으로 기대된다. 그러나 블록체인 기반 모바일 엣지 컴퓨팅을 안전하고 효율적으로 사용하기 위해 보안이 함께 동반되어야 하며, 본 논문은 이러한 보안의 하나로써 안전한 그룹 서명과 인증 체계를 위해 고려해야 하는 보안 위협을 살펴보고, 이를 완화하기 위한 보안 기술을 살펴보고자 한다.

1. 서론

모바일 엣지 컴퓨팅(Mobile edge computing)은 모바일 단말과 근접한 네트워크에서 데이터를 처리하여 IoT(Internet of Thing)의 낮은 컴퓨팅 파워를 보완하고 IoT 디바이스 연결성, 저지연성을 보장한다. 이와 더불어 블록체인은 탈중앙화 방식의 데이터베이스로, 거래 기록을 분산 원장으로 저장하여 데이터의 무결성, 추적성을 제공한다. 이때, 블록체인을 모바일 엣지 컴퓨팅에 적용할 경우, 모바일 엣지 컴퓨팅은 모바일 블록체인 환경에서 디바이스를 위한 컴퓨팅 파워를 제공할 수 있으며[1], 블록체인은 수집된 정보를 저장, 관리하는 탈중앙화 데이터베이스를 제공한다. 점점 더 많은 정보가 모바일 엔드에서 생성 및 소비되기 때문에, 블록체인 기반의 모바일 엣지 컴퓨팅은 미래 융합 기술의 핵심 요소로 대두되고 있다.

그러나 블록체인 기반 모바일 엣지 컴퓨팅은 많은 IoT 및 모바일 디바이스와 연결되어 있기에, 늘어난 공격 표면에 대응하여 사용자 인증을 통해 악의적인 사용자의 접근을 사전에 차단하는 것이 중요하며, 공모, 이중 지불 등 블록체인의 합의 단계에서 발생하는 보안 위협을 추가로 고려해야 한다. 그룹 서명은 하나의 그룹 공개키를 사용하는 검증 방식으로, 효율적으로 이러한 합의 단계의 위협을 해결할 수 있다.

본 논문은 블록체인 기반의 모바일 엣지 컴퓨팅에서의 안전한 그룹 서명과 인증 체계를 위해 고려해야 하는 여러 가지 보안 위협들을 살펴보고, 이러한 보안 위협을 보완할 수 있는 보안 기술을 분석하고자 한다.

2. 블록체인 기반 모바일 엣지 컴퓨팅 보안 위협 분석

블록체인 기반 모바일 엣지 컴퓨팅에서 안전한 그룹 서명 및 인증을 위해 그룹 참가, 그룹 탈퇴, 인증 과정에서 그룹원과 그룹 사이의 안전한 네트워크 형성이 필요하다. 그룹원과 그룹 사이에 안전한 네트워크 형성이 이루어지지 않을 경우, 다음과 같은 보안 취약성이 있다.

- **블록체인 사용자의 프라이버시 침해 공격**: 공격자는 블록체인에 참여하려는 사용자와 블록체인을 관리하는 관리자 사이에서 통신을 감청하거나 데이터를 가로챌 수 있다. 이는 블록체인 기반으로 이뤄지는 통신 과정의 취약성이며, 블록

체인을 모바일 엣지 컴퓨팅에 적용할 경우 참여자들의 가용성 침해와, 데이터 변조 등의 보안 위협을 제시할 수 있다.

- **모바일 엣지 컴퓨팅 네트워크의 통신 취약성:** 모바일 엣지 컴퓨팅은 클라우드를 활용하는 서비스이며, 클라우드와 모바일 엣지 사이의 실시간 응답과 처리를 필수적으로 지원해야 한다. 그러나 공격자는 클라우드-모바일 엣지 컴퓨팅 네트워크 사이에 과도한 인증 요청을 통해 클라우드 서버에 대한 DoS(Denial of Service), DDoS(Distributed Denial of Service) 공격을 수행할 수 있다.

3. 블록체인 기반 모바일 엣지 컴퓨팅을 위한 보안 기술

본 장에서는 2장에서 제시한 보안 위협으로부터 안전성을 보장하기 위한 보안 기술을 설명한다.

- **블록체인 기반 PKI**(Pubilc Key Infrastructure)**:** RSA(Rivest Shamir Adleman) 기반 시스템을 활용하기 위해서는 공개키에 대한 인증이 보장되어야 한다. 블록체인은 공개 및 변경 불가능한 원장 내에서 디지털 인증서를 저장하고 관리할 수 있는 능력을 갖추고 있으며[2], 블록에 기록이 존재할 경우, 다른 블록체인 네트워크 참여자의 동의 없이 개인에 의한 기록의 삭제나 수정이 불가능하기 때문에 완전히 추적 가능한 기록을 유지한다. 블록체인에 저장된 인증서는 무결성이 보장되어 공개키를 인증하고, 공격자가 공개키를 위조하는 것을 방지하여 블록체인 사용자의 프라이버시를 안전하게 보호할 수 있다.
- **제로 트러스트:** 제로 트러스트를 블록체인 기반 모바일 엣지 컴퓨팅에 적용하기 위해서는 자원에 대한 식별과 가능한 보안 범위를 설정하는 것이 중요하며, 사용자에 대한 신뢰 없이 각각의 요청에 인증 및 권한 부여를 수행하여 공격자가 네트워크에 침입하여 정보를 유출하고자 할 때, 다른 네트워크로 피해가 확산되는 것을 예방한다. 또한, 제로 트러스트는 전체 사용자의 트래픽을 신뢰하지 않기 때문에, 트래픽 흐름을 관리하여 공격자의 악의적인 트래픽을 실시간으로 탐지 및 차단하여 DDoS 공격에 대응할 수 있다.
- **안전한 그룹 서명 방식:** 블록체인 기반 모바일 엣지 컴퓨팅에서 그룹 서명은 다른 서명 방식과 융합되어 안전성과 효율성을 높일 수 있다. 함께 적용될 수 있는 서명 중, BLS(Boneh-Lynn-Shacham) 서명의 적용은 다수의 서명을 하나의 서명으로 집계하여 검증하기에 기존의 그룹 서명 검증 방식보다 효율적이다. 이러한 연구 내용은 2020년 S. Zhang외 1명이 제안한 BLS 서명을 활용한 연구[3]가 대표적이다. 본 방식의 경우 BLS를 활용한 그룹 서명을 채택하여 블록체인 기반 모바일 엣지 컴퓨팅의 효율성을 높이고, 이중 지불과 stake-bleeding 공격에 대한 안전성을 제공한다.

4. 결론

블록체인 기반 모바일 엣지 컴퓨팅은 안전한 그룹 서비스와 합의 단계의 인증이 필수적이다. 따라서, 본 논문은 안전한 그룹 서명 및 인증 체계를 위해 블록체인 기반의 모바일 엣지 컴퓨팅에서 발생할 수 있는 보안 위협과 이를 해결하기 위한 보안 기술을 분석하였다.

향후 연구로써, 제시된 각 보안 기술이 실제 블록체인 기반 모바일 엣지 컴퓨팅 시스템에 실제적인 적용과 효율적인 보안 서비스에 대한 연구를 수행하고자 한다.

참고문헌

[1] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, “When mobile blockchain meets edge computing,” IEEE Communications Magazine, vol. 56, no. 8, pp. 33 - 39, 2018.

[2] A. Yakubov, W. M. Shbair, A. Wallbom, D. Sanda and R. State, "A blockchain-based PKI management framework," NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, pp. 1-6, 2018.

[3] S. Zhang and J. -H. Lee, "A Group Signature and Authentication Scheme for Blockchain-Based Mobile-Edge Computing," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4557-4565, 2020.

[4] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu and W. Lv, "Edge Computing Security: State of the Art and Challenges," in Proceedings of the IEEE, vol. 107, no. 8, pp. 1608-1631, 2019.

[5] Xie, Qingqing et al. “ECLB: Edge-Computing-Based Lightweight Blockchain Framework for Mobile Systems,” Secur. Commun. Networks, 2021.