A Blockchain-based Architecture for Secure Delivery in Content-Centric Networks

Kamrul Hasan and Seong Ho Jeong
Hankuk University of Foreign Studies
kamrul@hufs.ac.kr, shjeong@hufs.ac.kr

콘텐츠 중심 네트워크에서 안전한 전송을 위한 블록체인 기반 구조

하산 캄룰, 정성호
한국외국어대학교 정보통신공학과

Abstract

Blockchain is effective in content delivery from a security and trust perspective in a distributed network. On the other hand, content centric networking (CCN) has been considered a new paradigm for future generation networks due to its unique characteristics, such as in-network content caching, content retrieval mechanisms, and packet-level content security. However, there are still some limitations in the CCN-based content delivery mechanism. For instance, an intruder can participate in the content handling procedure, leading to several security vulnerabilities in the network such as content request message flooding and false routing of content request messages. To address these security concerns in the content-centric networks, we propose a blockchain-based CCN architecture for more secure content delivery. Our proposed architecture ensures the security of content delivery, fostering trust between content providers and receivers.

Ⅰ. Introduction

As the digital landscape continues to evolve, the demand for secure and efficient content delivery mechanisms becomes increasingly paramount. In response to the challenges posed by potential security vulnerabilities in conventional CCN, this paper introduces a new solution, which enhances content delivery security. The existing research combined blockchain and encrypted cloud storage to preserve privacy and information sharing [1]. By leveraging the decentralized and tamper-resistant nature of blockchain technology, this architecture aims to identify malicious nodes in the network, fostering heightened security measures and instilling trust in the dynamic realm of digital communications.

Ⅱ. Method

Figure 1 illustrates the architecture of the blockchain-based CCN, with the green node denoting a valid node and the red node representing a malicious node within the network. Each node adheres to the CCN forwarding mechanism for content request and reply messages. Simultaneously, the content is represented by multiple blocks, with the validation of these blocks guided by the consensus mechanism inherent in Blockchain networks. The malicious node tampers with valid content request and reply messages, forwarding them to neighboring nodes as new content requests or replies, as illustrated in Content Provider-3 of Figure 1.

Initially, a leader node is determined by applying a clustering mechanism within the network. The leader node retains various information such as nodes' integrity, which is assessed by other member nodes in the cluster. Each receiver node analyzes content request messages to gauge potential tampering, leading to the identification of nodes' integrity, which is then communicated to the leader node. The leader node ultimately identifies malicious nodes based on the analyzed reports received from other clustered nodes. Subsequently, the malicious node can be blocked within the network and information about its status is conveyed to other leader nodes. This proactive measure prevents the malicious node from participating in other areas of the same network.

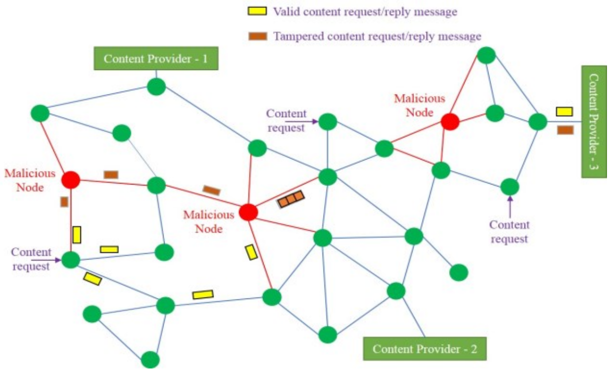

Figure 1: A Blockchain-based CCN Architecture

Ⅲ. Conclusion

In this paper, we proposed an architecture to support more secure content delivery using the blockchain-based CCN. Specifically, it can refrain the malicious nodes from manipulating the user request by content request message flooding, message modification, or false routing of content request messages.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2021-0-00484).

REFERENCES

[1] Fan, K., Ren, Y., Wang, Y., Li, H. and Yang, Y., 2018. Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G. IET communications, 12(5), pp.527-532.