Research Progress of Internet of Things Security Application based on Blockchain and Edge Computing

Wanying Feng [1], Qin Wang [1], Yiyang Ni [2]
[1]Nanjing University of Posts and Telecommunications, Nanjing, China
[2]Jiangsu Second Normal University, Nanjing, China
E-mail: wfeng07@nyit.edu, wangqin@njupt.edu.cn, niyy@jssnu.edu.cn

三等奖

Abstract

The development of 5G brings opportunities and challenges to the Internet of things (IoT) industry, especially in terms of real-time communication and security. We analyzed the motivation and challenges of combining blockchain and edge computing technology, and introduced two kinds of security architecture design and analyzed its feasibility. We also introduced two kinds of IoT security applications based on blockchain and edge computing.

Introduction

In the existing research, blockchain has attracted extensive attention by virtue of its smart contract, decentralization and immutability characteristics. But it is not suitable for IoT devices with limited resources because processing data will consume a lot of CPU time and energy. Edge computing has advantages in data processing, but its ability to secure data is limited. So we analyze the possibility of combining the two technologies, and analyze the challenges to be met.

Problem

The theoretical network speed of 5G can reach 100 times of 4G network. The improved transmission rate, higher throughput and lower latency are exactly what is needed for the development of IoT. However, the number of IoT devices has increased exponentially, which produces a large number of high-speed data flow. Higher requirements for the security of IoT applications and operation efficiency under multiple devices are needed.

Integration of Edge Computing and Blockchain

1.1 Motivations for IoT devices based on edge computing
IoT devices based on edge computing, a mechanism of security and transparency is needed. Because the edge server may be deployed in a place without strict monitoring and protection, it may encounter many malicious attacks. The key to solve it is the digital signature in the blockchain, which can ensure the identity of the IoT devices is verified and identified, and the information is not tampered in the transmission process.

1.2 Motivations for IoT devices based on blockchain
Blockchain can solve most security problems brought by the network. However, in distributed system, data transmission and storage are still challenging. Edge computing transfers computing work to distributed nodes. Thus computing mainly occurs in the nodes near the edge equipment, which provides the terminal equipment with fast and stable data sharing and processing capabilities. It just solves the big problem that restricts the development of blockchain.

2 Challenges

2.1 Extendibility
Edge computing helps to solve the limited storage space problem. However, when combined with blockchain, the smart contract requires each participant to maintain the same distributed ledger and every transaction needs to be tracked. Therefore, with the increasing number of access devices, each participant will generate and store a great quantity of transactions, which puts forward higher requirements for the operation performance of IoT devices and servers. So, how to optimize the efficiency and expand the network on the basis of the existing mode is an important challenge.

2.2 Cost standardization
The processing and storage capacity of edge servers cannot solve all data generated by IoT devices. Therefore, the processed data must be transferred to the cloud server for further processing and storage. However, due to the intelligent settlement of service fees generated by using smart contracts, it is necessary to use the cost distribution standard to complete the intelligent services of the network.

Architecture design of IoT security based on blockchain and edge computing

1. Detection and defense architecture
Zhou et al. made a source detection scheme for DDoS. The overall framework can be summarized as: preliminary anomaly detection, anomaly summary and analysis, and anomaly filtering.

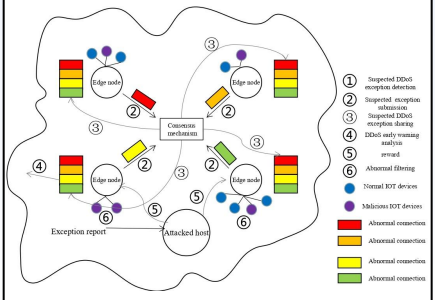

Figure1.Overall architecture of the scheme [1]

The general method is as follows: a single edge node uses protocol feature matching and clustering analysis algorithm to monitor and detect traffic, and submits suspected DDoS exceptions. Many edge nodes form a blockchain network to realize data sharing and analysis between nodes. Then summarize the suspected abnormal connections submitted by multiple edge nodes, and analyze the analysis code in the smart contract to get a DDoS alert for a target IP. After the target IP confirms the alert information, it will send the reward to the corresponding edge node by calling the smart contract. After receiving the reward, the edge node triggers the filtering mechanism to filter the DDoS connection initiated by the IoT devices based on the local newly added DDoS alert.

2. Security model based on cloud scheme
The overall framework is: perception layer, edge layer, data storage layer, application layer.

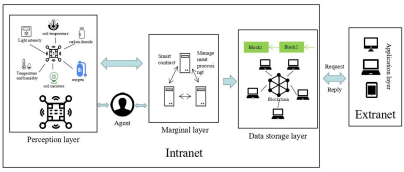

Figure 2. system framework [2]

The general method is as follows: the sensing layer obtains the required external information through sensor nodes. Then the results are returned. The edge layer is mainly the smart contract on the edge node. It includes rules for analyzing and judging the configuration behavior of the IoT and responding to it. It also is an integration system that can evaluate the reliability of the IoT devices and users. Data storage layer relies on smart contract to ensure data reliability. When the data is stored, the smart contract automatically executes. Encrypting the data and storing it in the storage hardware of the edge device. To ensure the security, the encryption algorithm and decryption private key are selected by the smart contract. A series of data operations, including data storage, access, and query will be recorded in the block of the blockchain.

Security application of IoT based on blockchain and edge computing

1. Intelligent agricultural system
By introducing blockchain, smart agriculture system can solve data security problems and ensure data reliability, so as to ensure to find the fault point and responsible party in the first time when agricultural products have problems. Also, edge computing and IPFS are used to overcome the small capacity and poor scalability of blockchain.

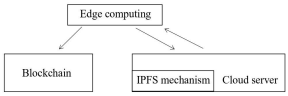

Figure 3. Key technology flow chart

2. Road information sharing service platform
During the driving process, the edge computing node is used to receive the road test, traffic flow, and video monitoring information, etc. and return to the vehicle in real time to realize local shunting and seamless switching. Combined with blockchain, the advantages of its smart contract, decentralization, openness and transparency are used to ensure data security and reliability.

Conclusion

We summarizes the advantages and disadvantages of edge computing and blockchain, and analyzes the motivation and challenges brought by the combination of blockchain technology and edge computing technology in IoT. Also, we introduce two possible architectures and security applications. We believe the combination will become an important technology to promote social progress, and its development prospect in the field of IoT is very promising.

Main references

[1] Zhou, Qihui & Deng, Zuqiang & Zoi, Ping. "DDoS Defense Method of IoT Devices Based on Blockchain" [J]. Journal of Applied Sciences. 2019(2):213-223.
[2] Liu, Shuai & Qi, Rongxin & Dong, Yihui & Feng, meng & Miao, Tiantian & Jiang, Hongling. "A Solution for Internet of Things based on Blockchain and Edge Computing" [J]. Journal of Nanjing University of Information Science & Technology(Natural Science Edition). 2019,11(05):596-600.
[3] Luo, Chuanwen & Xu, Liya & Li, Deying & Wu, Weili. (2020). Edge Computing Integrated with Blockchain Technologies.

Contact Information

Name: Wanying Feng
Phone Number: 17851154796
Email: 2670875150@qq.com