Internet of Things Access Control System Based on Hyperledger

Zheming Yang1*, Di Shao1, Liangyong Qu1 and Mei Zhang1

1 Zhejiang Zheneng Natural Gas Operation Co., Ltd., Hangzhou, Zhejiang, 310052, China

*Corresponding author’s e-mail: yangzhm@zjenergy.com.cn

Abstract. The current access control of IoT devices adopts the traditional method of centralized control, which leads to the shortcomings of single point of failure and low efficiency of the entire system. Due to the increasing amount of data generated by the Internet of Things network and the more complex data structure, the traditional access control system has exposed the problem of insufficient security when communicating. Based on the characteristics of blockchain decentralization, non-tampering, and programmable Hyperledger, an attribute-based access control mechanism combining blockchain with the Internet of Things is proposed to realize dynamic changes to the access control strategy and ensure the access control of the Internet of Things Safety and reliability.

1. Introduction

The Internet of Things network greatly reduces labor costs and reduces system overhead. In the process of obtaining a large amount of data in the Internet of Things, access control is one of the core technologies to protect data security. Its function is mainly to prohibit unauthorized users from using the system and to control users' access to special equipment. In the main access control model, attribute-based access control is more flexible, can better meet dynamic requirements, and achieves fine-grained access authorization. Blockchain is a distributed ledger technology for point-to-point transmission based on encryption algorithms, and a networked decentralized shared database technology. The distributed blockchain architecture is compatible with the distributed IoT system and dynamic access control requirements.

In 2016, there was research on combining blockchain technology with Internet of Things access control. Literature [1] stores access control information in the blockchain. In the above research, a centralized center is still used to implement access control decisions. Literature [2-3] proposed Ethereum as the next-generation blockchain network architecture. Ethereum has added smart contracts with Turing complete functions on the basis of the technical characteristics of the blockchain. Literature [4] uses smart contracts to record access control information. Literature [5] uses multiple smart contracts to jointly implement access control functions. Digital currency must be spent when deploying and executing smart contracts in Ethereum, which hinders the use of the system. Both Bitcoin and Ethereum allow any unknown node to join the network, but they have extremely high requirements on the scale of computing power in the application environment. Hyperledger Fabric has the characteristics of no currency and modular functions. At the same time, it has low computing power requirements for blockchain nodes, so it is more suitable for access control of the Internet of Things.

Hyperledger is suitable for environments where there are multiple participants but do not have strong computing power. In this environment, it still has all the characteristics of blockchain. Literature [6]
proposed to combine the blockchain with the RBAC model, and define an interface on the Ethereum platform to realize the anonymous identity verification mechanism of users. Literature [7] is based on the ABAC model, manages access control strategies and attributes through blockchain transactions, and completes the management and tracking of policy release, update, and cancellation. The policy is stored in the blockchain in an open and transparent form, which solves the problem. The issue of transparency in jurisdiction judgments. Literature [8] uses the combination of Hyperledger and access control to control access control strategies using smart contracts. However, the access control model in this study tends to be coarse-grained, which easily leads to vulnerabilities such as unauthorized access and over-authorization of IoT device users.

The main work of this paper is to combine the blockchain Hyperledger technology, smart contracts and ABAC model to propose a Hyperledger-based access control mechanism for the Internet of Things, and use smart contracts to implement complex algorithms to strictly review access control permissions.

2. Design of Access Control Architecture

Internet of Things access control based on Hyperledger can realize the access control management of Internet of Things devices. The system architecture can be divided into: client, blockchain, and IoT device.

The function of the client is to manage device resources, request access, grant access rights, and verify device usage rights. The blockchain uses Hyperledger as the network structure and uses smart contracts to realize logical judgments on access control. The distributed deployment is realized by the blockchain, which logically processes the various functions of the system, and stores the data on the chain. The IoT device sets a unique ID for each device, accepts instructions according to the ID and executes corresponding user tasks. This design ensures that IoT devices are not connected to the blockchain as a blockchain node.

2.1. Access control framework

The framework is based on Hyperledger blockchain technology and combined with the ABAC model. The framework includes users, user attribute sets, permission sets, policy management, smart contracts, and resource owners. The access control workflow can be divided into two stages: preparation and execution. The preparation stage mainly manages users, attribute information, and access control policies, including adding, updating, and deleting users, attributes, and policies, and responding to device and policy query results. The execution stage mainly judges, responds and executes access requests.

2.2. Access control contract algorithm

The decision result of access control is divided into two types, namely allow access (admit) and deny access (forbid). In response to the corresponding permission access request of the access subject (subject), by traversing the corresponding information in the user set (user_group), attribute set (attribute_group), and permission set (policy_group), if the information in a certain access control policy is satisfied, it is judged to allow access (admit). If the decision request does not satisfy the policy, the decision is forbid.

Input: user set (user_group), attribute set (attribute_group), policy set (policy_group).
Output: If the access subject (subject) exists in the user set and the corresponding attribute and permission are found (defined), then return (admit); if the access subject (subject) does not belong to the user set or the corresponding attribute and permission are not found (undefined), then return (forbid).

2.3. Access control policy decision algorithm flow description

1) Store the access subject in temp_user as a temporary user. 2) Traverse the user_group of the system user set, if the access subject exists in the user set, proceed to the next step; otherwise, return the access subject as an undefined user (undefined), and determine that there is no corresponding access permission
(forbid). 3) Query the corresponding attribute in the attribute_group. If the corresponding attribute of the access subject exists, proceed to the next step; otherwise, it is determined that there is no corresponding access permission (forbid). 4) Traverse the permission set policy_group through the attribute information, if there are corresponding permissions, store the access subject in the allow access result set admit_result_group, and determine that it has the corresponding access permission (forbid); otherwise, store the access subject in the access denied result set In forbid_result_group, it is judged as non-response access authority.

3. Design of Access Control Architecture

This section tests the effectiveness and security of the Internet of Things device access control mechanism based on Hyperledger blockchain proposed in this article. This article deploys Hyperledger in the Ubuntu system. The experimental environment of this system is shown in Table 1.

| Software environment | detailed information |
|----------------------|----------------------|
| OS                   | Ubuntu 16.04 LTS     |
| Hyperledger Fabric   | v1.4.4               |
| Go                   | v1.13.8              |
| Docker               | v19.03.6             |
| Docker-compose       | v1.23.2              |

The system designed in this paper and the Fabric-IoT proposed in [9], DAHB (distributed architecture based on hierarchical blockchain for Internet of thing) proposed in [10], and BBIAC (Blockchain-Based IoT Access) proposed in [11] Control) Perform performance comparison experiments, take the hardware environment and software environment of the machine as the standard, and select the function responsible for the access control method as the comparison object. In the comparison experiment of writing data function, the throughput and average delay of the system designed in this paper (expressed by ABAC-Fabric-IoT) are better than the other three access control schemes. The experimental results are shown in Figure 1 and Figure 2.

The write data performance of ABAC-Fabric-IoT in Figure 1 depends on the functions Policy and Resource. Experimental data shows that the write data throughput of the system designed in this article is better than the other three access control schemes, and the system can cope with the scale increased access request.

The Internet of Things access control system based on Hyperledger designed in this article adds the user attribute information set in the access control policy, and when writing data in Fabric-IoT, you must...
obtain the device’s MAC address (Media Access Control Address) and IP address (Internet Protocol Address) is added to the access control policy as attribute information, but it takes extra time to obtain these two parameters, which will result in poor throughput and average latency when Fabric-IoT writes data. The comparison shows The performance of the system proposed in this paper is better than the other three IoT access control solutions in terms of data writing. For access control systems that require fine-grained access control, the system proposed in this paper can better invest in large-scale data writing In the requested IoT scenario.

4. Conclusions
The Internet of Things access control system based on Hyperledger proposed in this paper combines blockchain technology with Internet of Things access control. Based on the ABAC model, it uses smart contracts to achieve a flexible, scalable, and fine-grained access control process, triggering the device in order. The specified contract content completes the automated operation of equipment trusted access control, solves the central trusted entity problem faced in traditional access control, and improves the reliability and security of access control. The Hyperledger is used as the blockchain platform for executing smart contracts, which makes the system more user-friendly while giving full play to the characteristics of the blockchain.

References
[1] Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: a new Blockchain-based access control framework for the Internet of Things[J]. Security & Communication Networks, 2016, 9(18): 5943-5964.
[2] Maesa D D F, Mori P, Ricci L. Blockchain based access control[C]//IFIP International Conference on Distributed Applications and Interoperable Systems. Neuchâtel, Switzerland: Springer, Cham, 2017: 206-220.
[3] BUTERIN V.A next-generation smart contract and. decentralized application platform[EB/OL]. [2019-06-10]. https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf.
[4] Wood G. Ethereum: A secure decentralised generalized transaction ledger[EB/OL]. [2020-06-08]. https://ethereum.github.io/yellowpaper/paper.pdf
[5] Košťál K, Helebrandt P, Belluš M, et al. Management and monitoring of IoT devices using blockchain[J]. Sensors, 2019, 19(4): 856-868.
[6] Zhang Y, Kasahara S, Shen Y, et al. Smart contract -based access control for the internet of things[J]. IEEE Internet of Things Journal, 2018, 6(2): 1594-1605.
[7] Liu A, Du Xi, Wang N, et al. Big data access control mechanism based on blockchain [J]. Journal of software, 2019, 30 (9): 2636-2654
[8] Lee Y J, Lee K M. Blockchain-based RBAC for user authentication with anonymity[C]//Proceedings of the Conference on Research in Adaptive and Convergent Systems. 2019: 289-294.
[9] Liu H, Han D, Li D. Fabric-iot: A Blockchain-Based Access Control System in IoT[J]. IEEE Access, 2020, 8: 18207-18218.
[10] Du R, Liu Y, Tian J. Access control method based on smart contract in Internet of things [J]. Computer research and development, 2019,56 (10): 2287-2298
[11] Shi J, Li R, Song T. Access control framework of Internet of things based on blockchain [J]. Computer applications, 2020,40 (04): 931-941