Research and Analysis of Blockchain Algorithms Based on Big Data Edge Computing

Leixin Deng(✉)

Southwest Jiaotong University, Chengdu, China
DLeixin@outlook.com

Abstract. With the development of artificial intelligence, big data, IoT and other technologies, more and more data is generated and collected through traditional sensing devices or smart mobile devices. In order to improve the transmission efficiency and availability of data, the original data often needs to be initially analyzed and processed with the help of edge computing, so there will be a large amount of available data in the edge computing network, and if these data can be shared directly in the edge network, it will If these data can be shared directly in the edge network, it will greatly improve the utilization of data and accelerate the modernization process of the city. Therefore, how to securely share data among heterogeneous edge nodes is also a current research hotspot. For the problems of difficult to establish trust relationship, difficult to guarantee privacy and single point of failure of central framework for data sharing in edge computing, a blockchain-based access control mechanism is proposed and implemented in this paper. In this scheme, smart contracts of blockchain are used to manage access rights and audit data, and the decentralization and tamper-evident characteristics of blockchain are utilized to solve the single point of failure and node trust problems.

Keywords: Big data · Edge computing · Blockchain · Access Control

1 Introduction

Edge computing, as one of the core technologies in the 5G era, can solve the problem of limited storage capacity and insufficient computing power of terminals by putting data from smart terminals and other devices into edge servers for storage or computation [1]. In addition, users do not need to be concerned about the specific architecture of compute and storage, management models, or technical issues such as scalability and fault tolerance in the edge network environment [2]. The distributed architecture of edge computing systems has the advantage of low energy consumption and low latency compared to centralized cloud computing systems. The edge server nodes in edge computing systems are the convergence points of many terminals, which include smart mobile terminals, sensors, cameras, and other IoT devices, as well as devices such as computers and servers in the local network. If the data collected, generated or stored by the terminals are shared, the data resources will be maximized, which not only reduces the human and material resources consumed by repeated data collection, but also can facilitate the modernization of the city [3].

K. Hemachandran et al. (Eds.): ICAID 2023, AHIS 9, pp. 423–428, 2023.
https://doi.org/10.2991/978-94-6463-222-4_45

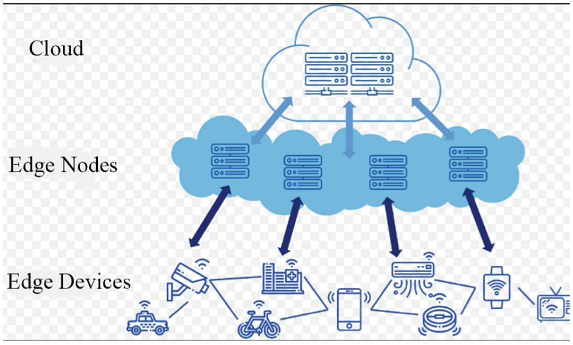

Fig. 1. Edge computing system architecture

2 System Model and Security Model

2.1 System Model

As shown in Fig. 1, the edge computing system considered in this paper consists of cloud servers, edge servers, and terminals [4]. Since the underlying blockchain platform of the scheme in this paper is Ether, which is a public blockchain, any node can join and exit the network at any time, so any device in the edge computing system can become a blockchain node, and each device is connected together through a peer-to-peer (P2P) network [5]. There are intelligent terminals with certain arithmetic resources and IoT sensors with a single function connected to P2P networks through IoT gateways, and each device can freely choose to become a mining node or a lightweight node according to its own arithmetic conditions.

In this paper, each of these elements is classified into the following roles based on their role in access control: data owner, third-party server, blockchain network, and data requester [6].

2.2 Security Model

This paper aims to provide a distributed access control scheme for users in the edge network while guaranteeing the privacy and integrity of shared data [7]. The proposed scheme can defend against the following potential attacks: impersonation attacks, malicious insider attacks, data modification attacks, and collusion attacks [8]. In this paper, the access control list mechanism defined in the literature is used to implement the access control matrix model [9]. As show in Table 1.

Table 1. Access Control List

Main Body	Operation	Permission Hash	Deadline
User1	Read	0X52d65…	2021-07-01
User2	Write	0	2021-07-01
User3	Write	0X4a515k…	2021-07-05

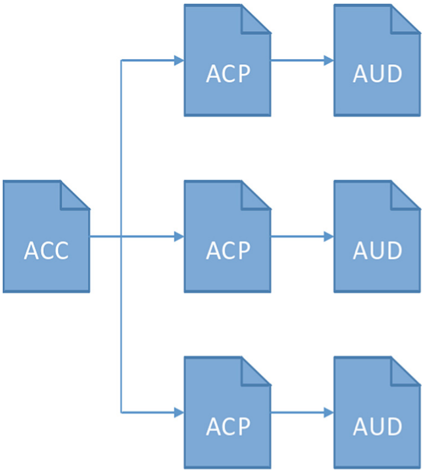

Fig. 2. Smart Contract System Framework.

3 A Blockchain-Based Access Control Mechanism

3.1 Smart Contract System Framework

The smart contract framework proposed in this paper contains multiple ACP contracts, each ACP implements access control of a data object; multiple audit contracts (AUD contracts), each AUD contract is generated by the corresponding ACP contract and deployed to the blockchain, when the third-party server verifies the access control authority of the data requester to the ACP contract, the access record is stored in the corresponding AUD contract; an ACC contract, which is mainly used to index the address of the ACP contract, the third-party server, the key distribution node and other information, and the ACP contract is generated by it. As shown in Fig. 2 and 3.

3.2 Access Control Mechanism

The whole access control process can be divided into two parts: shared data upload and shared data download.

(1) Shared data upload
(2) Shared data download

This digital signature is the data owner's signature to a predefined message (generated according to the message structure), which is shown in Table 2.

In order to decrypt the data coming from the storage server, the data requester initiates a key request to the key distribution node, which contains the above digital signature σ and a predefined message m.

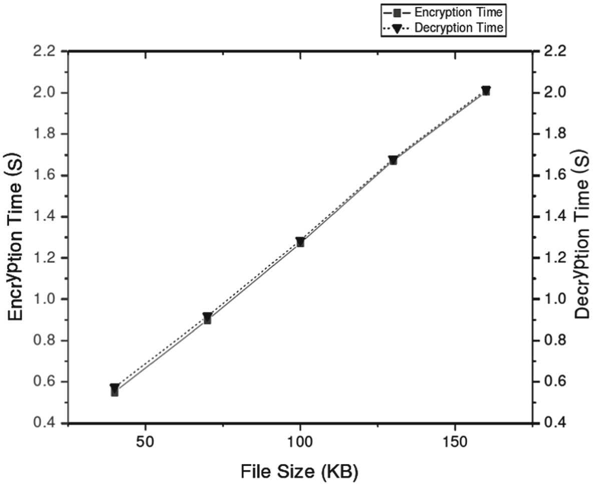

Fig. 3. Encryption/decryption overhead versus file size.

Table 2. Predefined message structure

Fields	Meaning
PK_{do}	Data owner public key
PK_{dr}	Data requester public key
T	Deadline
ID	ID of the requested data

4 System Analysis

The performance of this solution is somewhat dependent on the underlying blockchain platform, i.e., the factors associated with Ether. Ether puts blocks on the chain via PoW consensus and executes smart contracts based on the gas limit of each transaction. Therefore, the following metrics will all affect the performance of this scheme: the hash arithmetic power (system computing power) of the blockchain system, the complexity of smart contracts, the number of tasks, the block generation rate and the network bandwidth, and the performance impact of the above metrics on blockchain-related operations is shown in Table 3.

Where the time overhead for smart contracts to be created/deployed to the blockchain with Ether-related metrics is shown in Table 3, but independent of the shared data size, the time to remotely authenticate the Enclave and pass in the decryption key is constant, so these two operations do not affect the scalability of this solution (sharing of data of arbitrary size).

Table 3. Impact of Ethernet network-related metrics on the performance of blockchain operations

Influencing Factors	**System computing power**	**The Complexity of Smart Contracts**	**Number of tasks**	**Block generation rate**	**Network Bandwidth**
Blockchain operational performance impact	Positive correlation	Negative correlation	Negative correlation	Positive correlation	Positive correlation

5 Conclusion

The edge server in the edge computing system is the convergence point of many terminals, and a large amount of raw data collected, generated or stored by the terminals are processed into directly usable data in the edge network, so these data have great shared value. This paper focuses on the data sharing problem in heterogeneous and complex edge networks. Since it is difficult to establish trust relationships between different individuals and institutions in the edge networks and to form a sharing situation, this paper designs a decentralized access control scheme with the help of the emerging blockchain technology. The solution writes access control policies into smart contracts on the blockchain, allowing the transaction process of data to be monitored in an open environment. To ensure the privacy of the shared data, the shared data is encrypted before uploading to the third-party server, and the encryption key is shared through SGX technology, thus preventing the server from leaking the data information privately. The system analysis shows that the solution is resistant to malicious service provider attacks and man-in-the-middle attacks, is functionally complete, and meets scalability requirements.

References

1. Wang Chuan, Wu Xiaohan, Wu Lan. Research and analysis of real-time big data streams based on controlled clustering edge computing algorithm [J]. Changjiang Information Communication, 2023, 36(02):51-54.
2. Cai Wansheng, Song Xi. LSTM-based edge cache prediction in power grid big data environment [J]. Power Information and Communication Technology,2022,20(12):73-80. DOI:https://doi.org/10.16543/j.2095-641x.electric.power.ict.2022.12.010.
3. Zhong Yunqin, Zhu Yueqin, Jiao Shoutao. Research on predictive modeling methods for edge big data analysis[J]. High Tech Letters,2022,32(10):1067-1075.
4. Fang He, Yang Qiang, Guan Yufeng, Zhou Zhengping. Application of edge computing and big data based equipment condition monitoring and intelligent diagnosis platform in Tianwan nuclear power plant[J]. Power Big Data, 2022, 25(09): 61-67. DOI:https://doi.org/10.19317/j.cnki.1008-083x.2022.09.011.
5. Cao Y. Research on blockchain-based data security management of microgrid in edge computing[D]. East China Jiaotong University, 2022. DOI:https://doi.org/10.27147/d.cnki.ghdju.2022.000201.

6. Wang Yuping. Design and application of cloud-side collaborative management components for intelligent buildings [D]. Zhejiang University, 2022. DOI:https://doi.org/10.27461/d.cnki.gzjdx.2022.000179.
7. Chen H, Zeng YH, Gu Juan. A big data platform for elevator safety supervision based on edge computing[J]. Information Systems Engineering,2021(12):117-121+127.
8. Dong Zhenhui, Song Liang,Jiang G. A verifiable scheme for big data streams in edge computing environment[J]. Journal of the University of Information Engineering, 2021, 22(06): 727-734.
9. Huang Yang. Research on blockchain precision poverty alleviation data security management for edge computing[D]. East China Jiaotong University, 2021. DOI:https://doi.org/10.27147/d.cnki.ghdju.2021.000322.