Intelligent Blockchain System Based on Differential Privacy

Z J WU¹, H DAI¹, Y K YUAN¹ and D MENG¹

¹ School of Computer and Software Engineering, University of Science and Technology Liaoning, Anshan 114051, China
Z J WU Email: 939674778@qq.com

Abstract. Due to the advantages of decentralization, traceability and non deletion, blockchain technology can be well combined with differential privacy algorithm to protect data privacy. Therefore, it effectively ensures the privacy security of data stored in the system in terms of technical structure and algorithm. This paper proposes a micro service system architecture based on super ledger fabric, which carries out data privacy noise processing combined with smart contract, and carries out different noise processing according to the security level recognized by the system at the time of user registration. The implementation and test results of the system show that the system architecture has good scalability, traceability and security, can meet the query control of users for data privacy, and effectively prevent the tampering and destruction of data by malicious attackers.

1. Introduction

In the era of big data, the storage and use of personal information is a pain point faced by the current Internet system technical architecture. The traditional system architecture adopts micro service or distributed architecture, which is stored in the central server or the third-party cloud disk architecture[1]. The system management mostly adopts the way of human management. In this way, there will be potential code vulnerabilities, the possibility of human subjective tampering and destruction of data and human theft of data. Because the traditional system does not record the query records of the thieves, the difficulty coefficient of supervision and investigation of information theft is higher[2]. Due to the advantages of decentralization, traceability and non deletion, blockchain technology can be well combined with differential privacy model in the field of data privacy security protection. Therefore, it can effectively ensure the privacy and security of data stored in the system in terms of technology and algorithm. This chapter proposes an architecture model of micro service system based on super ledger fabric, which is combined with smart contract for data privacy and noise processing. Finally, the test results of hyperledger caliper, a blockchain testing framework, show that the framework has better interaction performance than Ethereum blockchain technology architecture[3].

2. System architecture

Based on the noise processing algorithm of differential privacy and combined with blockchain super ledger technology, this paper designs a blockchain protection framework model based on differential privacy[4]. This structure has the characteristics of micro service architecture, which is convenient for the scheduling and management of blockchain business, and also reduces the attack risk faced by the traditional architecture. The differential privacy protection framework model based on blockchain is shown in Figure 1. The architecture is mainly divided into five modules: Micro service module, local database, cloud cluster and source information collection module.
The crowd gathered. Cloud clusters periodically collect data in the network. The data interaction between cloud clusters will trigger some transactions in the blockchain, which will be uploaded to the blockchain network periodically. Cloud clusters need to interact with the source information collection module.

Local database. The local database is responsible for storing some unnecessary storage information obtained from the source information collection module[5]. Cooperating with the blockchain network can greatly reduce the pressure of the blockchain system and effectively guarantee the data. Once the data is leaked, it is convenient for traceability and query.

Blockchain network. The blockchain network stores the data collected from the source information module through the smart contract, protects the integrity of the data, and stores it in a distributed manner, which can ensure stability and security. Due to the non erasable characteristics of the blockchain, every transaction on the blockchain can be followed.

Microservice module. As the core part of the whole system, the microservice module provides a one-stop solution for service flow limiting degradation, service registration and discovery, message driven, object storage, distributed read scheduling and distributed transactions in the microservice system architecture[6]. The common problems easily encountered in the system architecture are effectively avoided.

Source information collection. As the hub of the blockchain protection framework, the source information collection module interacts with the blockchain network through smart contracts, and has the function of collecting and commanding clusters. The real data uploaded to the blockchain is disturbed by differential privacy injection[7]. When the data from the cloud cluster is received, you can choose whether to submit it to the blockchain. If the information is judged to be non essential storage type, the data will be submitted to the local database for storage.

3. Process analysis of protection framework
In the blockchain protection framework model based on differential privacy, there are three stages of data interactive transmission between modules. It includes data receiving and block packaging of the blockchain system[8], disturbance forwarding and audit decision-making of data. The specific steps are as follows.

Blockchain data packaging. The data of the blockchain is uploaded to the blockchain through the smart contract through the source information collection module. Once the smart contract is triggered, the transaction will be triggered. The blockchain packs the transaction information into the node of the Merkle tree through sha256 hash value calculation. The root node of Merkle tree is calculated recursively and stored in the blockchain header of the block. The root node, timestamp, random number, hash value of the previous block, difficulty coefficient, etc. in the Merkle tree form a new block[9].

Disturbance forwarding of data. For the audited data, the default data is real and secure. In order to prevent malicious attackers from damaging the blockchain architecture and malicious reading of data. Adding differential privacy noise to the data stored in the blockchain and disturbing the real value can effectively prevent malicious attackers from damaging the blockchain.

Review decisions. The data is collected through the cloud cluster, and the time sequence is recorded, and the cluster operation of the cloud cluster is monitored for abnormalities. After passing the audit, corresponding decisions are made for the results.

For the blockchain protection framework model based on differential privacy in this chapter, the following process is designed. Firstly, at the beginning of the operation of the model framework, the operation state of the current blockchain network will be detected. If it is in the initialization state, the current blockchain network needs to be created through the configuration file of the blockchain network, and the digital ID card will be issued by the CA organization of the blockchain consensus node to join the node into the network. First, the response data information is obtained from the source data acquisition module, and the data information is sent to the endorsement node in the blockchain consensus node for endorsement. If the endorsement is passed, the data information is broadcast and
recorded in the blockchain network, and the hash value and transaction timestamp of the block are generated at the same time,

4. Framework workflow
The microservice framework model is used to distribute and process blockchain requests. These functions are mainly undertaken by microservices. The internal workflow of the module is as follows.

The blockchain protection framework based on differential privacy combines the springcloud Alibaba microservice framework and blockchain technology. The system adopts micro service architecture to ensure the fine-grained division of services and service process control. The micro service architecture mode can divide the functional requirements of privacy protection applications into a group of small service groups, so that each service can run in its own process, and the communication between services adopts lightweight communication mechanism. Combined with the characteristics of the framework, the system uses Nacos for service registration and discovery component, ribbon for internal service node load balancing, sentinel for service fault tolerance component and gateway for internal gateway forwarding component. The blockchain adopts fabric super ledger technology as the blockchain technology platform. The platform is equipped with smart contracts, which can realize the automatic operation of functional contracts, so as to avoid artificial third-party tampering. Since there is a consensus node in the fabric super ledger, and the blockchain is interacted in the form of non smart contract, the request cannot be filed by the consensus node. Therefore, the platform architecture can only interact with the blockchain platform through the call of smart contract. The operation status of the smart contract and the data stored in the blockchain cannot be tampered with. Even if an attacker wants to carry out malicious attacks and data coverage against the smart contract and data, even if the forged data is submitted to the blockchain platform by means of authentication bypass, the blockchain will record the malicious operations of the user. Thus, by reviewing these submitted information and tracing the hash value of the address requested by the attacker, and searching and querying the hash address, we can quickly obtain the real identity of the attacker. In the blockchain protection framework of differential privacy, the overall architecture of combining springcloud Alibaba and blockchain fabric server is shown in figure 1.

![Blockchain system architecture](image)

Figure 1. Blockchain system architecture.

5. Analysis of test results
Firstly, relevant function tests are conducted for the user query smart contract, differential privacy noise smart contract and data uplink smart contract submitted to the blockchain environment. The chain code function test results are shown in Table 1.

| Chain code function name | Expected output | test result |
|--------------------------|-----------------|-------------|
| Query_cc                 | Data can be queried according to query criteria | Pass |
| DPrivacy_cc              | It can disturb the data | Pass |
| Insert_cc                | The blockchain browser enables you to query the changes of blocks | Pass |
Hyperledger caliper is a general blockchain performance testing framework with excellent performance. It allows users to test different blockchain solutions with customized use cases and get a set of performance test results. Caliper can test the performance of hyperledger fabric's blockchain platform. Caliper currently supports performance indicators including throughput, transaction delay, blockchain resource consumption, CPU, memory, and network io. Caliper is a service that generates a workload for the system under test and continuously monitors its response. After the test, caliper can generate a test report based on the observed kernel SUT response.

As the blockchain protection framework based on differential privacy proposed in this chapter is a blockchain architecture based on super ledger, Ethereum blockchain private chain architecture is used as a comparative test when verifying the fabric framework structure. Ethereum is selected as the comparison architecture. On the one hand, because Ethereum officials provide friendly open source solutions to help Ethereum developers better carry out the development and testing of smart contracts and run their own private chain network for testing, it has the same technical architecture as this experiment. On the other hand, if Ethereum public chain environment is selected as the comparison experiment, Submitting smart contracts on the public chain requires a certain amount of ether, and submitting smart contracts with various functions in the public chain environment will have some uncertain impact on the public chain environment. Therefore, this comparative test uses remix, an online smart contract development tool of Ethereum, to write smart contracts with the same functions and submit them to the private chain environment.

In the experiment of this chapter, 100 data submission queries were conducted for fabric super ledger architecture and Ethereum private chain architecture respectively, and the average time response statistics were conducted for the response time of the two environmental architectures. The experiment used different submitted data sizes for stress test, and the data transmission sizes were set to 1KB, 2KB, 4KB, 8KB, 18KB, 32KB and 64KB respectively, 128KB. The test results obtained are shown in figure 2.

![Comparison diagram of Ethereum and Fabric.](image)

From the response time analysis of fabric system architecture and Ethereum private architecture, the architecture based on fabric super ledger tends to be more stable. The average response time will be about 47ms when transmitting 32KB data to 64KB data, while the average response time of the compared Ethereum environment will be higher than that of fabric system architecture. However, from the perspective of average response time, the overall response of fabric meets the request requirements of most blockchains.
6. Conclusion

This chapter integrates the differential privacy algorithm into the blockchain technology architecture, faces the application scenario of the non interactive publishing framework, ensures that the final protection framework model meets the constraints of differential privacy, and greatly ensures the decentralization, traceability and tamperability of the system architecture. The blockchain based differential privacy protection framework constructed in this chapter can not only ensure data quality, but also prevent users' information from being leaked. It provides a new technical architecture and new ideas for solving a series of problems arising from the technical system in the field of information security.

References

[1] Cynthia, Dwork. Aaron The Algorithmic Foundations of Differential Privacy(Foundations & Trends in Theoretical Computer Science) pp 211–407.
[2] Acs G Castelluccia C. I have a dream! differentially private smart metering(.Springer Berlin Heidelberg) pp 118–132.
[3] Jia J J and Huang H A trajectory(k,e)-anonymous algorithm against trajectory similarity attacks(Computer Engineering & Science) pp 828-834.
[6] Wei Yinzhen and Deng Zhonghua. A scientific data security Traceability Method Based on blockchain and smart contract pp 32-38
[7] Zhu Liehuang, Gao Feng, Shen Meng, et al. Overview of blockchain privacy protection [J]. Computer research and development,( Modern intelligence) pp 2170-2186
[8] Zhao Gang and Liu Tao. Trusted storage technology of unmanned cooperative system based on blockchain [J].(Firepower and command and control) pp 141-144
[9] Weng Xiaoyong. Research on cloud computing data sharing system based on blockchain (Computer engineering and application) pp 120-124