Journal of Electronics and Information Science (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2023.080504
ISSN 2371-9524 Vol. 8 Num. 5

A survey of privacy protection in distributed systems based on blockchain

Zhuohong Zhang

Guangdong University of Science and Technology, Guangzhou, 510000, China

Keywords: Blockchain; Distributed system; Cell cipher algorithm; Homomorphic encryption algorithm; State secret algorithm

Abstract: In recent years, with the development of blockchain technology, the sharp increase in the amount of data and the improvement of user needs, various kinds of security problems occur frequently, and the application research on the privacy protection of blockchain in distributed systems is more and more extensive. This paper summarizes three types of distributed system privacy protection research methods based on blockchain, including privacy protection research based on lattice cryptography algorithm, privacy protection research based on homomorphic encryption algorithm and privacy protection research based on state secret algorithm.

1. Introduction

The emergence of blockchain technology can avoid the privacy leakage problem of centralized data to a certain extent, but there are still potential risks to user privacy and transaction information security. In recent years, network attacks and information leaks related to distributed systems have occurred frequently. For example, in 2019, EOS was attacked by a large number of hackers, and the attack means was random number cracking. In 2020, employees of a decentralized crypto derivatives exchange stole the personal information of more than 8,000 users; In July 2022, the British Army's Twitter and YouTube accounts were hacked and account information and usernames were tampered with and used to post information about cryptocurrencies and electronics. Blockchain-related security events keep happening, causing great loss and damage to the security of network systems and users' property, and the reason is that the privacy security of users in blockchain-based distributed systems cannot be guaranteed [1-2]. This paper summarizes some distributed privacy protection methods based on blockchain, and puts forward reasonable research ideas.

2. Privacy protection method based on lattice cipher algorithm

2.1 Overview

With the development of quantum computers, the digital signature used for identity authentication in most current cryptosystems is not well resistant to quantum computing hacking attacks. For example, Shor algorithm [3] uses quantum Fourier transform to solve large integer

decomposition and discrete logarithm problems with exponential acceleration. Classical computers cannot solve such problems in polynomial time, but quantum computers will solve such problems in a very short time. Therefore, for quantum computers, it is urgent to find a more secure defense algorithm.

Lattice cryptography is a kind of encryption algorithm that can effectively resist the attack of quantum computer, and is suitable for the signature authentication process of quantum computer. Blind signatures provide anonymous authentication for blockchain-based distributed systems and can be used to create untraceable payment systems.

2.2 Algorithm introduction

In view of the above problems, Li Zhaoyang [4] proposed to design a signature authentication scheme using lattice cryptographic correlation algorithm, which is divided into blind signature scheme and proxy signature scheme. In this scheme, bimodal Gaussian distribution is used to select the blinding factor and blind the original information to effectively protect the user's sensitive information. At the same time, you can set proxy signatures based on the requirements of different users, and use the proxy function through security authorization.

Compared with other schemes, the size of the public and private keys is relatively small, which reduces the signature storage space, reduces the computational complexity of the transaction signature process, and improves the efficiency of transaction execution. In terms of security, it embodies good anti-quantum security, and can solve the security problems in quantum computers to a certain extent.

The main contributions of the programme are:

(1) Considering the efficiency of the system, the private key and key are generated independently;

(2) Considering the security of the transmitted information, the transmitted information is blinded, and the bimodal Gaussian distribution is used to design a more rigorous blind algorithm;

(3) In the decryption stage, the corresponding unblinding algorithm is designed, and the signer can detect whether there is malicious attack by using the rejection mapping theorem.

3. Privacy protection method based on state secret algorithm

3.1 Overview

Zyskind et al. [5] proposed a decentralized user data management framework, including transactions for threshold management and transactions for data storage and retrieval, to ensure that the data owner has full control over the data. But the scheme requires both the owner and the visitor to be online at the same time to enable this feature.

SM2 algorithm [6] is a public key cryptography algorithm based on elliptic curve cryptosystem in China. Compared with the traditional RSA signature algorithm, SM2 is unique in the problem difficulty: the difficulty of RSA signature algorithm is based on the difficulty of decomposition of large prime numbers; The difficulty of SM2 algorithm is based on elliptic curve discrete logarithm. Compared with RSA algorithm, SM2 algorithm has a shorter key to achieve stronger password strength, and the computing cost is much lower than that of RSA algorithm with the same security level.

3.2 Algorithm Introduction

In a centralized data management system, the user's digital information is published by some

recognized trusted institutions or contributes research value in research institutions. If the user stores personal information in a centralized third-party data storage server, then the user will not be able to control the use of data on the platform, which is prone to the following problems:

(1) The data storage of a single server is vulnerable to attack, resulting in a single point of failure, resulting in the loss or leakage of user data;

(2) The control of data access lacks a trusted executor, making it difficult to achieve high sharing.

To solve the above problems, Cao Sui [7] proposed a privacy protection scheme based on the improved SM2 signature algorithm. The scheme points out that the decentralized characteristics of blockchain are used to build a decentralized access control platform, which automatically executes visitor attribute judgment through smart contracts, and then uses the improved SM2 signature algorithm to hide sensitive information in user data, so as to improve data security and computing efficiency. Figure 1 shows a concrete model of this scenario

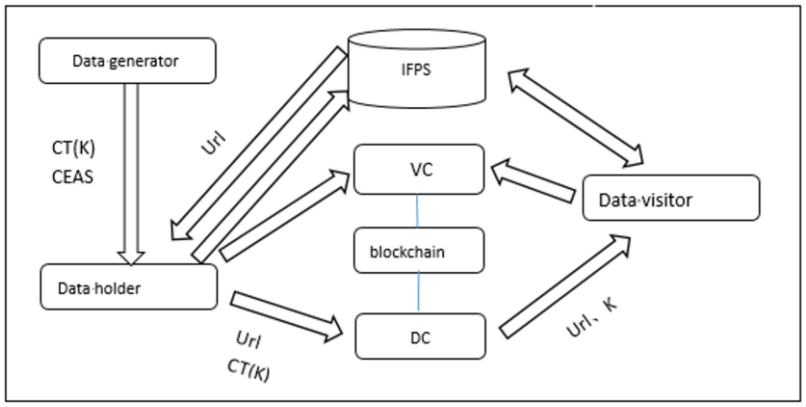

Figure 1: Scheme model diagram

The main contributions of the programme are:

(1) Considering the low security of SM2 algorithm, an improved SM2 algorithm is designed and a content interception structure is added to SM2 algorithm. The data owner divides the message and sets the content interception structure of the message to restrict the extraction range of the data owner.

(2) Considering the problem of shared data, the data holder is designed to extract the shareable message segment according to its privacy sensitivity without violating the interception rule, and an extraction signature is calculated for the extracted shared message segment set;

(3) Considering the problem of verification, a verification algorithm is designed so that data visitors can verify whether the source of the extracted signature is the data generator through the verification algorithm to ensure that the message is not tampered with.

4. Privacy protection method based on homomorphic encryption algorithm

4.1 Overview

Wang et al. [8] proposed a layered blockchain aggregation method to complete the data aggregation step and verify relevant data, so as to achieve the purpose of efficient storage aggregation and data privacy protection. Chen et al. [9] proposed a data aggregation method based on dual blockchain for data aggregation, which can effectively resist external attacks by using the two-stage consensus mechanism. However, when the data in this scheme is aggregated, the data needs to be transmitted to the data requester through the master node. In this process, it is easy to receive external attacks, resulting in data loss or damage.

4.2 Algorithm Introduction

Aiming at the privacy issues such as centralized storage and the credibility of third-party institutions caused by the characteristics of current massive data and distributed systems, and based on the current research status, Shi Xinyao et al. [10] proposed a privacy protection scheme based on blockchain. Based on blockchain and zero computing technology, this scheme designs a hierarchical distributed storage data aggregation architecture, and uses Paillier threshold homomorphic encryption algorithm to encrypt data through the addition of random value noise, so as to achieve data privacy protection and effectively resist certain external data attacks.

The main contributions of the programme are:

(1) Considering the problem of data tampering, design a distributed framework based on blockchain;

(2) Considering the delay of data transmission and the complexity of computing data nodes, a distributed aggregation framework combining blockchain and zero computing is proposed;

(3) Considering the single point attack problem, the Paillier threshold homomorphic encryption algorithm is proposed to assign the key to zero computation and data requestor, and ensure that zero node cannot be obtained during decryption, and effectively prevent the single point attack problem;

(4) Considering the authenticity of user identity, batch aggregation verification technology and bloom filter technology are proposed to design a secure anonymous signature verification mechanism to ensure the reliability of user identity.

5. Research Ideas

In the above research schemes, the algorithm privacy protection scheme based on lattice cryptography can play a role in privacy protection for some scenarios, but for complex application needs and network environment, how to design a more secure and reliable scheme needs further research. The privacy protection scheme based on national password algorithm can judge the authenticity of user attributes and data, but its time complexity needs to be reduced. The privacy protection scheme based on homomorphic encryption algorithm can meet the security requirements to a certain extent, but the decryption process after adding noise may cause decryption errors. At the same time, there is also a problem that the consensus efficiency of the blockchain network will affect the implementation efficiency of the overall privacy protection.

Based on such problems, I propose a new idea. In the distributed system based on blockchain, particle swarm optimization algorithm is adopted in the process of data clustering to optimize the clustering effect and increase the consideration of data security in edge node devices. In the process of encryption, Gaussian distribution is used to set factors to realize the authentication process of ring signature.

6. Summary

The massive data security problem after the emergence of distributed system is gradually showing its important research significance. For distributed privacy protection, a large number of scholars and researchers at home and abroad have conducted relevant targeted studies. This paper summarizes privacy protection schemes, including: The privacy protection schemes based on lattice cipher algorithm, national cipher algorithm and homomorphic encryption algorithm are summarized and their advantages and disadvantages are put forward.

References

[1] Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportunities:A survey[J]. International Journal of Web and Grid Services, 2018, 14(4):352-375.
[2] Feng Q, He D, Zeadally S, et al. A survey on provacy protection in blockchain system[J]. Journal of Network and Computer Applications, 2019, 126:45-58.
[3] Shor P W. Polynomial-time algotithms for prime factorzation and discrete logarithms on a quantum computer [J]. SIAM review, 1999, 41(2):303-332.
[4] Li Zhaoyang. Research on Privacy protection method of distributed system based on Blockchain [D]. Beijing University of Posts and Telecommunications, 2021. DOI:10. 26969/d. cnki. gbydu. 2021. 000213.
[5] Zyskind G, Nathan O. Decentralizing Privacy:Using blockchain to protect personal data [C]. 2015 IEEE Security and Privacy Workshops. IEEE, 2015:180-184.
[6] Wang Zhaohui, Zhang Zhenfeng. Overview of SM2 Elliptic Curve public key cryptography [J]. Information Security Research, 2016, 2(11):972-982.
[7] Cao Sui. Research on Distributed Privacy Data protection Technology based on blockchain [D]. Guangdong University of Technology, 2022, DOI:10. 270-29/d. cnki. ggdgu. 2022. 000400.
[8] Wang Y X, Luo F J, Dong Z Y, et al. Distributed mater data aggregation framework based on blockchain and homomorphic encrytion[J]. IET Cyber-phys Syst, 2019, 4:30-37.
[9] Siguang Chen, Li Yang, Chuanxin Zhao, et al. Double-blockchain assisted secure and anonymous data aggregation for fog-enabled smart grid[J]. Engineering, 2022, 8(1):159-169.
[10] Shi Xinyao, Wang Jingyu, Liu Lixin. Distributed data aggregation scheme for privacy protection in Internet of Things environment [J/OL]. Miniature microcomputer system: 1-9 [2023-10-14]. http://kns. cnki. net/kcms/ detail/21. 1106. tp. 20230605. 1702. 014.html