Journal of Shipping and Ocean Engineering 10 (2020) 1-4
Doi: 10.17265/2159-5879/2020.01.001

Research on Optimization Scheme of Ship Radar Information Storage Based on Big Data

Li Ning
Department of Navigational Technology, Merchant Marine College, Shanghai Maritime University, Shanghai 201306, China

Abstract: With the development of marine information technology, ship radar data increases geometrically, and the traditional local server storage architecture has become increasingly unable to meet the requirements of modern ship radar data capacity, so cloud storage has gradually become the mainstream technology of radar data storage. At the same time, because the marine communication network is more vulnerable to external attacks and environmental interference, high-density encryption technology suitable for cloud storage is needed. In this paper, a ship radar cloud storage platform based on big data is studied, and a high-density encryption algorithm CP-ASBE is designed. Finally, simulation is carried out.

Key words: Control access protocol, cloud storage platform, CP-ASBE.

1. Introduction

Cloud storage architecture is a research hotspot in recent years. It has the characteristics of large capacity, small bandwidth resources, convenient data acquisition and management, and has been widely used in modern radar data storage. At the same time, radar data is more vulnerable to external attacks and environmental interference when it is transmitted through a shared or proprietary network [1], which requires a kind of adaptive marine environment And high-density storage technology of cloud storage architecture.

In this paper, we choose a highly reliable and scalable HDFS cloud storage architecture, study the system model and security mechanism, design a high-density encryption algorithm CP-ASBE based on this architecture, and finally simulate it.

2. HDFS Cloud Storage Platform

2.1 Cloud Storage Architecture

HDFS cloud storage platform is a cluster architecture based on master-slave relationship, including a master node MasterNode and N distributed storage nodes DataNode. In order to ensure the reliability of the platform, an auxiliary node Auxiliarynodes, is configured for the MasterNode to play the role of dual machine backup.

Attribute data of ship radar is stored in MasterNode and backed up in Auxiliarynodes. Attribute data includes data block file name, starting address, data block size and other information. Specific data is stored in N distributed storage nodes DataNode, and all nodes are monitored by handshaking mechanism [2]. The architecture is shown in Fig. 1.

2.2 Access Control Process of Cloud Storage Platform

The key problem of cloud storage platform is data access security. HDFS platform carries a dual access guarantee mechanism. First, user identity authentication is carried out in the list. After the authentication is passed, the user can access the master node MasterNode or auxiliary node Auxiliarynodes. After passing the user authentication, the user does not obtain the access control right of the distributed storage node DataNode, but also needs to judge the user right in the masternode. The HD-FS cloud storage platform uses 9 bit characters to represent the

Corresponding author: Li Ning, Master, Lecturer, research fields: transportation information engineering & control.

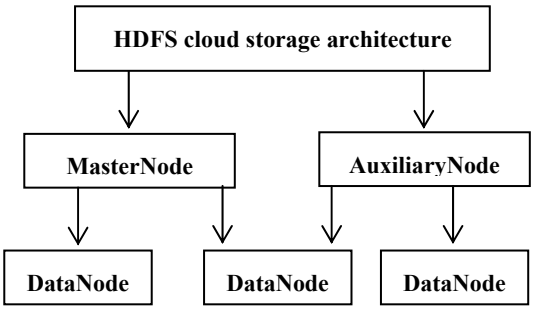

Fig. 1 HDFS cloud storage architecture.

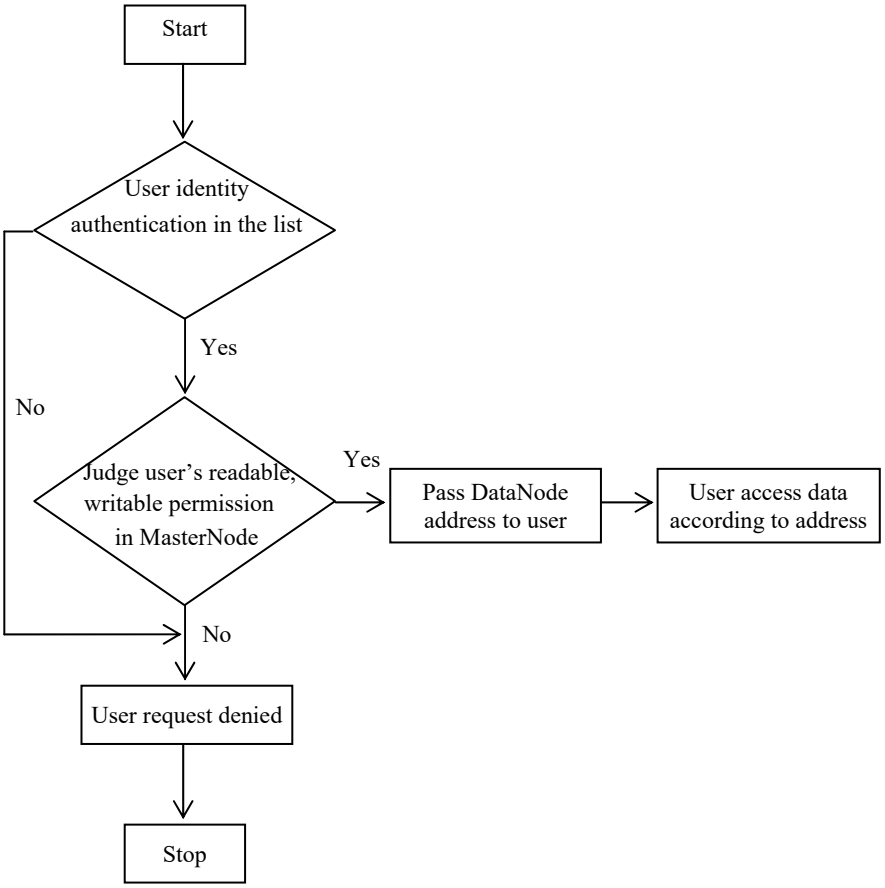

Fig. 2 HDFS control access flow.

User's readable, writable and executable permissions [3]. The whole control access process is shown in Fig. 2.

3. High-density Cloud Storage Encryption Algorithm Based on CP-ASBE

3.1 Encryption and Decryption Principle of Control Tree

The last section describes the access control process of the HDFS cloud storage platform. Although the user identity is identified at the platform level, it is vulnerable to attack at the network level where the user interacts with the data of the storage platform. CP-ASBE is an encryption algorithm based on attribute set, which does not require identity binding for user. When users access the cloud storage platform, the platform provides a specific access strategy, which corresponds to the user key one by one. Data confidentiality adopts one-to-many control tree structure.

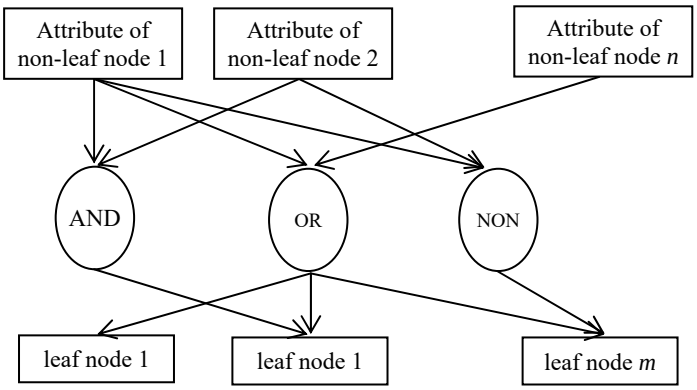

Fig. 3 Control tree data acquisition process based on attribute set.

Different attributes of ship radar data are mapped to non-leaf nodes of control tree, and data sets with different attributes are stored in leaf nodes. Assuming that the number of single attribute, that is, the number of non-node is NC_x, the number of data set, that is, the number of leaf node is NC_y, non-leaf node includes attribute threshold value k_x and the combined attributes of single attribute sets can be represented by child nodes.

Comparing the threshold value k_x with the number of single attribute NC_x: if $k_x<NC_x$, AND operation is performed between single attributes; $k_x=NC_x$, OR operation is performed between single attributes; $k_x>NC_x$, NON operation is performed between single attributes; three operations of AND, OR and NON realize different combinations between single attributes, that is, through the combination of non-leaf nodes, access to different leaf nodes (ship radar data stored at different addresses) is realized [4]. Such a complete radar data can be divided according to different attributes and stored in different leaf nodes. The client of data acquisition only needs to obtain the attribute set key to decrypt. The control tree data acquisition based on attribute set is shown in Fig. 3.

3.2 CP-ASBE High-density Encryption and Decryption Algorithm

The last section describes the principle of data encryption and decryption based on the control tree of HDFS cloud storage platform. In the actual process of ship radar data encryption and decryption, the attribute access strategy of the control tree is not a calculation, but a recursive process [5]. CP-ASBE is a strategy of recursive control tree encryption and decryption.

Supposing that the number of root node of the control tree is r, the subtree of the root node x is T_x, and the key structure of CP-ASBE is W, the whole algorithm flow is as follows:

(1) Initialization Stage

The overall public key PK and the initial key MK of the control tree T are generated and transmitted to all root nodes.

(2) Key Generation Process

The function Key Gen is used to generate keys for different users and different attributes, and transmit to users. Supposing user uid is x and the attribute set is A the function of key generation is Key Gen (MK, A, x).

(3) Encryption Process

Using Encrypt (PK, M, T) to encrypt the control tree recursively. When encrypting, using the threshold value for all non-leaf nodes of the root node to determine the encryption polynomials q_n, the degree of polynomials is the threshold value k_x minus 1; different from the non-leaf node, the degree of polynomials of the leaf node is always 1.

(4) Decryption Process

Finally, when the user obtains the private key SK, decrypting it with Decrypt (SK, T).

The whole recursive flow of CP-ASBE algorithm is shown in Fig. 4.

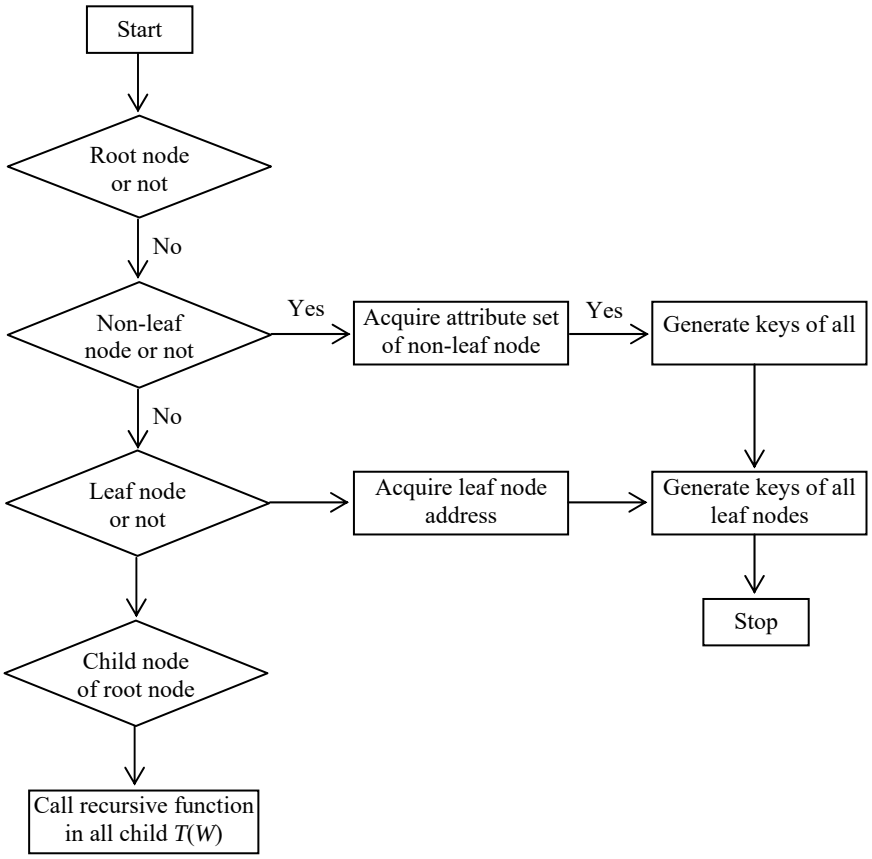

Fig. 4 CP-ASBE encryption algorithm flow.

Table 1 Simulation result.

Number of attribute set	Complexity(Recursive step)	Time-consuming for encryption /s	Time-consuming for decryption /s
10	3028	3.78	4.56
30	5620	5.29	6.09
90	6346	6.14	7.25

5. Conclusion

Based on the study of the model of HDFS cloud storage of ship radar data platform, this paper focuses on the analysis of the recursive encryptor algorithm CP-ASBE in cloud storage, and finally simulates it.

References

[1] Li Dianwei, and Fan Yundong 2016. "Design and Implementation on Cloud Document Secure Storage Management System Based on IBE Mechanism." *Netinfo Security* (12): 1-7.

[2] Li Yangai, and Zhao Huawei 2014. "PKI Based HDFS Authentication and Secure Transmission Mechanism." *Shandong Science* 27 (5): 33-41.

[3] Ruj S., Nayak A., and Stojmenovic I. 2015. "DACC: Distributed Access Control in Clouds." In: *International Conference on Trust, Security and Privacy in Computing and Communications*, 91-98.

[4] Bethencourt J., Sahai A., and Waters B. 2017. "Ciphertext-Policy Attribute-Based Encryption." In: *Symposium on Security and Privacy*, IEEE Computer Society, 321-334.

[5] Müller S., and Katzenbeisser S. et al. 2008. "Distributed Attribute-Based Encryption." In: *Information Security and Cryptology – ICISC 2008*, International Conference, Seoul, Korea, December 3-5, 2008, Revised Selected Papers. DBLP, 2011, 20-36.