Abstract

Data outsourcing in the cloud has unique advantages such as low cost, lower management overhead, and storage flexibility. The user organization is willing to use the cloud system to outsource a large amount of data to the cloud provider. With the increasing popularity of cloud storage services, how to verify the integrity of outsourced data on the cloud has received widespread attention and has become a challenging issue. The cloud outsourcing environment and its security control issues lead to the risk of exposing highly sensitive data to internal or external attacks. Traditionally, data remains encrypted and can only be decrypted by authorized authors with security. However, encrypting and decrypting large data files is computationally expensive. In addition, the existing data review mechanism cannot handle the dynamic update of data well. Therefore, this research plan proposes plans for the next three years to research and develop cloud systems with outsourced big data auditing mechanisms with security and dynamic functions.

1st year: Research and development of protecting confidential cloud proxy computing and integrating cloud storage services: Proxying encryption keys and verification information with higher computation costs to cloud storage services, reducing the burden on data owners, and establishing a complete cloud storage service system. The efficiency and effectiveness of the system are the focus of this plan. The efficiency and effectiveness quality measurement factors of a complete cloud security mechanism are as follows: 1. Computational complexity: the computation time and several operations required by the application mechanism during encryption, decryption, and verification; 2. Communication complexity: the number and length of messages required; 3. Costs: The storage space required to build a complete cloud storage service system.

2nd year: Research and development of a dynamic and efficient data audit mechanism for the divide-and-conquer adjacency list: an outsourced data review mechanism based on algebraic signatures and XOR functions, and design a divide-and-

conquer adjacency table (DAT) The data structure makes dynamic data updating more efficient.

3rd year: The research and development of the integrity verification mechanism based on blockchain cloud storage data: the third-party auditors in the traditional publicity verification model are not completely trustworthy and vulnerable to opponents' DOS attacks and bribes. This plan will propose a decentralized and tamper-resistant secure cloud storage data verification protocol based on blockchain technology.

Keywords: Cloud computing, Access control, Hierarchical key management, Cloud Storage Service, Shared key tree, Public Auditing, Public Auditing.