

The Study on Security and Audit Mechanism in Cloud Storage Service

Abstract

Cloud computing provide abundant computing ability and storage that users can accord their demand to add/cancel software/hardware requirement dynamically. These advantages let Small and Medium Business (SMB) didn't need to purchase and maintain equipments hire technical staffs for operation and repair it, only need to focus on development of system and program, and this way can reduce many kinds of cost. In Cloud, the Cloud Storage Services not only a general storage for user, but also a convenient share data service for enterprise and Data Owner (DO). But when DO want to share a specific data, especially confidential data, for specific group or users, there need to consider and include access control and key management of data.

Therefore, this project will design and implement a high efficiency access control and key management mechanism based on Cloud Storage Services to approach security and confidentiality of data stored in Cloud Storage Services. In the key management mechanism, we use hierarchical key management with Shared Key Tree (SKT) and renewed key message to achieve DO and user can only store one secret key respectively, then DO can generate all encrypt file key, and user can derive the encrypt file key which he/she has the access right, and then achieve more efficiency key update and access control.

In addition to access control and key management, when DO start to rely on Cloud Storage Service, correctness and integrity of data are also need to check and verify regularly. But DO's computing ability in Cloud scenario may no longer stronger as usual, i.e. only has browser. Therefore, reducing computing complexity of DO and data receiver is also an important issue. According to above problems, this project has been divided into three main parts: (1) Access control and key management (2) Protect privacy of public auditing data (3) Protect confidentiality of Cloud proxy computing

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