A Study of Public Key Encryption with Keyword Search in Cloud Systems (2)

Abstract

Cloud Computing can provide huge amount of computing resource and storage space for users. Moreover, users can increase their resources of software and hardware dynamically depends on their demands. Nowadays, more and more people, organizations and health institutions pay attentions on the services of Cloud Computing such as Cloud Storage Service. Cloud Storage Service can provide users virtual storage space which they can buy as their demands. Furthermore, users can access their documents store in the virtual storage space every time and everywhere. For small enterprises and sunrise industries which have less capital, buying virtual storage spaces can save lots of business cost. For health institutions and large enterprises which require huge amount storage spaces, buying virtual storage spaces can reduce organization expense. However, the action that users outsource their documents to cloud storage server will cause their documents under threatens because they cannot master the documents security and confidentiality clearly. When users request to access their file to Cloud server, the request message may be eavesdropped by outside attackers and be abused by inside attackers which will disclose the secret information of document and push personal information to danger. Therefore, this project will study and implement an efficient and high applicability Query Hiding mechanism based on Cloud Storage Service and achieve the security and the confidentiality of Query Hiding. In our Query Hiding mechanism, we will use ElGamal public key encryption system and Bilinear Map to implement one of the application and use the concepts of Batch Verification and Proxy Multi-Signature to develop two Query Hiding application and protect users identifies and their secret information. We have designed and implemented a query hiding mechanism for small mobile devices in the last project. This project is expected to continued last project to be completed: 1) to implement; to implement a multi-keyword query hiding mechanisms to narrow your search; 2) to implement a multi-user shared keyword query hiding mechanism to reduce the user cost of computing.

Keywords: Cloud Computing, Cloud Storage Service, Public Key Encryption with Keyword Search, PEKS, Public Key Encryption with Conjunctive Field Keyword Search, Security, Query Hiding, ElGamal, Proxy Multi-Signature, Batch Verification