System Analysis

Attribute-based encryption (ABE) is regarded as an effective encryption method with fine grained access control in the cloud storage. Attribute-based encryption can be divided into two types of key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE). The KP-ABE scheme refers to that the ciphertext is associated with an attribute set, and a user's secret key is associated with an access policy. A user can decrypt the ciphertext if and only if the ciphertext's attribute set satisfy the access policy of user’s secret key. The CP-ABE scheme refers to that the ciphertext is associated with an access policy, and a user's secret key is associated with an attribute set. A user is can decrypt the ciphertext if and only if his attribute set satisfy the access policy of the ciphertext.

Although attribute based encryption technology provides an effective means for data confidentiality, yet it brings another new problem that the users may find it difficult to search for interesting data from a vast number of encrypted data. This problem is called keyword search problem. One of the simplest searching methods is to download all encrypted data locally and then to decrypt it, finally to execute keyword search in plaintext. However, this method will waste huge computational resource and bring a vast cost for user to do the work of decryption.