Abstract

To maintain data integrity on the cloud, Attribute-based Encryption (ABE) with Key Policy Attribute-based Encryption (KP-ABE) and Ciphertext-Policy Attribute-based Encryption (CP-ABE) can be used with access control implementation for cloud computing. CP-ABE is a promising cryptographic primitive for secure data sharing in cloud computing. A data owner is the only charge of to define the access policy associated with his data which to be shared. In CP-ABE, each user's secret keys are associated with a set of attributes and data are encrypted with access policy on attributes. A user can decrypt a ciphertext if and only if his attributes satisfy the ciphertext access policy. In CP-ABE, the secret keys of users have to be issued by a trusted key authority that leads to key escrow problem. Besides, most of the existing CP-ABE schemes cannot support attribute with an arbitrary state. In this paper, weighted-attribute data sharing scheme is proposed to solve the key escrow problem and also improve the expressiveness of attribute, so that the resulting scheme is friendlier to cloud computing applications. An improved two-party key issuing protocol guarantees that neither key authority nor cloud service provider can compromise the whole secret key of a user individually. The
concept of weighted-attribute not only enhance the expression of an attribute binary to arbitrary but also reduce the complexity of access policy, so that storage cost of ciphertext and time cost in encryption can be reduced.

References


Index Terms

Computer Science Distributed Systems

Keywords

Cloud Computing, Attribute-based Encryption, Secure Data Sharing, Weighted-Attribute