REVOCABLE IDENTITY-BASED BROADCAST PROXY RE-ENCRYPTION FOR DATA SHARING IN CLOUDS

ABSTRACT:

Cloud computing has become prevalent due to its nature of massive storage and vast computing capabilities. Ensuring a secure data sharing is critical to cloud applications. Recently, a number of identity-based broadcast proxy re-encryption schemes have been proposed to resolve the problem. However, the IB-BPRE requires a cloud user who wants to share data with a bunch of other users to participate the group shared key renewal process because Alice's private key is a prerequisite for shared key generation. This, however, does not leverage the benefit of cloud computing and causes the inconvenience for cloud users. Therefore, a novel security notion named revocable identity-based broadcast proxy re-encryption is presented to address the issue of key revocation in this work. In a RIB-BPRE scheme, a proxy can revoke a set of delegates, designated by the delegator, from the re-encryption key. The performance evaluation reveals that the proposed scheme is efficient and practical.

INTRODUCTION:

Cloud computing has become a solution for data maintenance due to its flexibility and effectiveness. However, cloud computing has been suffering from security and privacy challenges. Encryption can be a straightforward approach to ensure data confidentiality and Identity-based encryption is one of the promising representative secure mechanisms because it has a concise public key infrastructure. When storing the identity-based encrypted data to the cloud, the data owner would like to share the data with others in particular scenarios. For example, a set of volunteers upload their genome data to the cloud in a genome record cloud system for the scientists to collaboratively conduct medical research. If IBE is adopted into such a medical system, the genome data should be encrypted before uploading to the cloud as Enc(m, id), where m is the genome data and id is the recipient's identity. A researcher Alice with the identity id from the genome research institute may want to share the volunteer's genome data with a list of her colleagues with identities id1, · · ·, idn in the same research group. So it could be a potential approach to address our research question as embedding proxy re-encryption into cloud also leverages the benefit of cloud computing not only is the data saved on the cloud but the cloud server also can play a role as a proxy to do complex re-encryption computations.