A survey of proxy re-encryption for secure data sharing in cloud computing

Never before have data sharing been more convenient with the rapid development and wide adoption of cloud computing. However, how to ensure the cloud user’s data security is becoming the main obstacles that hinder cloud computing from extensive adoption. Proxy re-encryption serves as a promising solution to secure the data sharing in the cloud computing. It enables a data owner to encrypt shared data in cloud under its own public key, which is further transformed by a semi trusted cloud server into an encryption intended for the legitimate recipient for access control. This paper gives a solid and inspiring survey of proxy re-encryption from different perspectives to offer a better understanding of this primitive. In particular, we reviewed the state-of-the-art of the proxy re-encryption by investigating the design philosophy, examining the security models and comparing the efficiency and security proofs of existing schemes. Furthermore, the potential applications and extensions of proxy re-encryption have also been discussed. Finally, this paper is concluded with a summary of the possible future work.