Ph: 9585554590, 9585554599
Email: support@salemsmartreach.com
URL: www.salemsmartreach.com

Identity-based remote data possession checking in public clouds

Abstract:

Checking remote data possession is of crucial importance in public cloud storage. It enables the users to check whether their outsourced data have been kept intact without downloading the original data. The existing remote data possession checking (RDPC) protocols have been designed in the PKI (public key infrastructure) setting. The cloud server has to validate the users' certificates before storing the data uploaded by the users in order to prevent spam. This incurs considerable costs since numerous users may frequently upload data to the cloud server. This study addresses this problem with a new model of identity-based RDPC (ID-RDPC) protocols. The authors present the first ID-RDPC protocol proven to be secure assuming the hardness of the standard computational Diffie-Hellman problem. In addition to the structural advantage of elimination of certificate management and verification, the authors ID-RDPC protocol also outperforms the existing RDPC protocols in the PKI setting in terms of computation and communication.