**ABSTRACT**

In proxy re-encryption schemes, users delegate their encrypted files to other users by using re-encryption keys, which elegantly transfers the users’ burden to the cloud servers. Moreover, one can adopt conditional proxy re-encryption schemes to employ their access control policy on the files to be shared. However, we recognize that the size of re-encryption keys will grow linearly with the number of the condition values, which may be impractical in low computational devices. data security has become a critical issue in various kinds of applications. Users may prefer storing their files in an encrypted manner and delegating decryption rights efficiently. In order to protect the files stored in the clouds, the owners can encrypt the files by using their keys before uploading the files to the clouds. Still, a user needs to be online to share her encrypted files because she needs to send her keys to her friends. It is extremely inefficient because of the heavy overhead on the user. Fortunately, proxy re-encryption schemes, enable users to share their encrypted files with other users by using re-encryption keys.

A Cloud storage system, consisting of a collection of storage servers, providing long term storage services over the internet. Storing data in a third party’s cloud system causes serious concern over data confidentiality. To keep sensitive user data confidential against untrusted servers, cryptographic methods are used to provide security and access control in clouds. As the data is shared over the network, it is needed to be encrypted.