**INTRODUCTION**

Nowadays data have become important resources, sharing is now considered to be an inevitable trend to improve the value of data resources. With the help of cloud service, users can enjoy high quality sharing services while saving a lot of local infrastructure investment. Data sharing in the cloud, however, has a series of privacy and security risks as the cloud is out of the trust domain of the data owner.

There are many practical scenarios for data sharing. Consider the members of a research institution want to store and share their research data with each other. In order to reduce management and storage overhead, they store and share data in the cloud. But some research projects include sensitive commercial or national secrets. To protect data confidentiality, files are often encrypted before uploading to the cloud. Furthermore, users prefer to share data anonymously for preserving identity privacy. In addition, some projects may need to be completed together by multiple research institutions, and data may need to be shared among different groups, but each institution usually has its own encryption and access control mechanism, thus, data sharing for multiple groups presents some challenges.

First, the identity privacy of users is an urgent issue to be considered. On the one hand, they must be authenticated by the cloud to access the data. Without privacy preservation, the cloud may collect their identity information. On the other hand, if the identity privacy of users is unconditionally protected, accountability is difficult when they upload maliciously faulty shared data. Second, the multi-group access control is a thorny problem. To preserve data privacy, data owners usually encrypt their data, and then upload the ciphertexts into the cloud.

It is necessary to consider not only the access rights management within a group, but also the access control of sharing among multiple groups. Since each group has its own encryption mechanism, when users want to access the data of other groups, they need to request the decryption key from the data owner or key manager of the group, which undoubtedly increases the communication cost and calculation cost, so it is not feasible in the real scene. Furthermore, group members are often dynamically changed. Therefore, it is necessary to ensure that the revoked users can no longer access any data in the cloud.