**PROPOSED SYSTEM**

To realize data sharing of security and privacy protection for multiple groups in the cloud, we combine group signature, attribute-based encryption of ciphertext policy and broadcast encryption technology to realize conditional privacy protection and efficient access control. The group manager is responsible for key management within the group, and the key involved in cross-group data sharing is generated by the key generation center. The data owner does not have to manage all the visitors and be online all the time to authorize them.

A. System Construction This section describes the details of our scheme for the system construction, including system initialization, key distribution, file generation, file access and user revocation.

1) System Initialization

System initialization is performed by the key generation center and the manager of each group. The key generation center generates the system public parameter PK and the master key MSK by algorithm AttSetup. The manager is responsible for the initialization within his own group. The group public parameter GPK and the group master key GMK are generated by algorithm GroupSetup.

2) Key Distribution

First, the group manager generates a set of attributes S for the group, and uses algorithm Sign(m, Ksigሻ to generate the group signature σs for message m = (IDgroup, S), where Ksig denotes the key of the group signature. Then he sends the message (IDgroup, S, σs) to the KGC, where IDgroup stands for group identification. KGC runs algorithm Verify(m, σs, GPK) to verify whether the signature is valid, then runs algorithm AttKeyGen(PK, S, MSK) to generate the corresponding attribute key AttKey and send it to the group manager. After that the group manager runs the algorithm UserKeyGen(GPK, GMK, IDi ) to generate the user key SK for each group member, and saves (IDi, SK) into the group user list. Finally, the group manager computes the proxy key PXK and uploads it into the cloud. PXK = (׊IDięRL: PሺIDiሻ, Ai, x)