**EXISTING SYSTEM**

Some schemes were proposed to ensure secure data sharing. In these encryption systems, the data owner encrypts the data and specifies authorized visitors who can access the encrypted data. In, the cloud converted ciphertext from one encryption system to another encryption system via proxy re-encryption to realize the data sharing among different encryption systems. However, an important issue is the privacy of user identity. The data visitor needs to submit the identity to obtain the decryption key. In addition, the data owner needs to stay online to authorize visitors of other groups.

Liu et al. proposed a multi-owner group data sharing scheme, in which identity-based dynamic broadcast encryption (IBBE) achieves flexible access control, the group administrators are responsible for key management of all users. with respect to the group signature technology, it protects user identity privacy and realizes anonymous and tractable data sharing. However, the scheme requires the identity of all data visitors and is usually only applicable to data sharing within a group. Shen et al.proposed an anonymous traceable group data sharing scheme, which generates shared session keys through multi-person key negotiation to reduce the burden of key management brought by centralized distribution to the central controller, but it can only realize data sharing within the same group.