Project Title : MobiShare

Short description :

Today distributed cloud services have become very popular for storing and processing of user data. However, currently cloud users must have full trust in the correct handling of their data by the cloud services. For instance, that the data is encrypted while residing in the cloud service.

This project aims at decoupling the key management from the cloud server by performing a decentralised file encryption key management that is in control of the user. This is achieved by performing an independent, **distributed key management** between the user's own devices and also among users who share content with each other through other communication channels like NFC, Barcodes, Local networks etc.,.

The work concerns with design and implementation of protocols and algorithms that can perform the distributed key management among the users who share data. It also involves mobile devices due to their popularity and a proof-of-concept implementation on Android platform for some of the popular cloud-services like Dropbox, Google Drive and Microsoft OneDrive. The proposed protocols should work without involving any additional intermediary services. In addition, the protocol must also be secure - in the sense that it never leaks unencrypted data or the encryption keys to anyone other than the users who are authorised for file sharing.

The work involved in this project can be broadly categorised as **Security in Distributed Systems**.