Assignment No. 11

Data Security

Objective:-

Create chatting app with Cloud and providing Data security

Description: -

The objective of this assignment is to secure the data stored on the chat application. The idea is to encrypt the user and chat data stored on disk, and decrypt the data for retrieval and update.

This is achieved by encrypting the database using SQL Cipher, a version of SQLite that is available for iOS and android. The database is encrypted with a 256-bit AES key. Rather than storing this key with the database, I have instead provided the key with every operation from a Client of the content provider, providing the key as a query parameter in the URI specified for the operation. An activity saves this key, and passes it to any manager objects it creates for accessing the content provider. The manager object in turn caches the database key when it is created. When an operation is invoked, the manager then adds the database key as a query parameter to the URI used to identify the content being accessed. The database is initialized with the encryption key the first time that a database operation is performed. The device's camera is used to read this QR code and parse it for the database key.

All messages are uploaded by the client and stored in its content provider that have not yet been uploaded to the server. A sequence number is provided to the last message that it receives, along with its own UUID and client identifier to identify itself.

These messages are added to the server and adds to its own database, assigning each message a unique sequence number. The server responds with a list of all of the registered clients, and a list of the messages that it has received since it last synchronized with the client. The list of chat clients is replaced with the list received from the server. Assuming one is using server-assigned client identifiers as primary keys for clients in their content provider, you will be able to maintain the correct relationships between clients and messages in your content provider.

I have implemented google play services in order to work with Location Awareness. It uses the API to obtain the pin code of the location where the phone is located. It also displays latitude and longitude of the device along with the message sent by the user. The sender can be changed by clicking on Settings.

Conclusion: -

In this way I have successfully created Chat App and saved messages on to the cloud along with location awareness and encrypted the database using SQL Cipher.