**ENCAPSULATE**

**Title:** Encapsulate

**Purpose:** The purpose of this project is to develop a cross-platform application that will help users to store their secret words, such as password, locally or on server securely.

**Need of the Application:** Today, in our day to day life we use many online services such as Social Networking Website, EMail and many more digital nodes or extensions of our physical life. Even a simplest person has more than one EMail to keep Personal and Professional life separate. To all these accounts we associate a password. It’s hard to manage this many password and it’s even more foolish to keep same password everywhere. The magnitude of this problem grows exponentially when we start to manage our Bank Accounts online. The password of these bank accounts have to contain some special type of character to keep it strong and it’s very foolish to write this password in some file or on some page. Same goes with DigiLocker Account, an initiative by GoI within Digitalization Revolution of India. So, there is a huge need of a cross-platform solution that will help users to store their multiple passwords securely so that they neither forget them nor store them unsecurely.

**Solution:** Think of a “cross-platform” software that enables user to save their password. There are lots of such software. But hey, why should I know secret word of my user. So, think of a “cross-platform” software that enables user to encrypt their secret word using their own secret key and store all of them at one place. The Secret Word Vault does this.

**Development:** The development of a “cross-platform” application take a lot of hard work and dedication for a really long time. So, we have divided the project into phases:

1. **Phase I: Android Application**
   1. In this phase, we have focused to develop an android application due to a huge market capture. To develop Android Application we have subdivided tasks into different sub phases and assigned each task to some person.
   2. **Sub-Phase I: Android UI:** At first we have to make a layout for our app using android studio. This design or layout will used to take input from user and give user output. Hence, at first we have to make a rough layout of UI and implement it.
   3. **Sub-Phase II: Database:** To store user’s key and encrypted secret words we need a database. There are two databases:
      1. **Local Database:** This database is on user’s local storage. The chances of loss of this data due to user’s error (format device) is high. Also, once user’s log in to his/her account, a copy of all server data will be made on user’s local database to minimize bandwidth use of internet.
      2. **Server Database:** The server database centrally stores all the information of user’s profile, user’s keys and user’s encrypted passwords. It’s user’s decision that if he/she wants to keep his/her secret on server (ensures persistence of data) or locally only (high risk of data loss).
   4. **Sub-Phase IV: Connecting Server Database to Android using jSON and PHP:** Our Server database will be on remote server. For an Android device to communicate with the database, there will be a need of internet. Also, to ensure safety of server, we can’t write database USER ID and Password in android application. Hence, we will be using PHP to communicate with database.
      1. **Step I:** Android device will store all data into a jSON array.
      2. **Step II:** This array will be posted to our server url using POST (PHP) method.
      3. **Step III:** PHP will extract data out of jSON array and do operations with it such as encryption and storing into database.
      4. **Step IV:** Based upon need, PHP will also create a jSON array that will contain reply from server (maybe failure or success or list of some data from database).
      5. **Step V:** Android application will get this jSON array as soon as post of data is complete on same server url to which it posted data and then android application will operate on this reply.
      6. **Step VI:** User will get the reply / data it requested for.
   5. **Sub-Phase V: Encryption/Decryption:** The encryption/decryption will happen on our online server. For this we will be using PHP.
   6. **Sub-Phase VI: Design & Finalizing:** As the last step of Phase I, we will put everything together and give the UI a professional design. Post this, Android Application will be ready.
2. **Phase II: Web Portal**
3. **Phase III: Windows / Linux (PC) Application using Python**
4. **Phase IV: iOS Application**