Thought Bubble Diary

Abstract:

The objective of this paper is to present a personal diary application, which implements AES-256 to encrypt diary entries and SHA-1 for user authentication. Every entry made to this app is secured using the encryption algorithm. The users are first brought to sign up to store their credentials. They can then create entries which are stored in Android's SQLite database in encrypted form. These entries can be read and modified by the user.

Introduction:

It is often necessary for someone to maintain a journal to record life's highs and lows only to remember later how they have been through and embrace the present. This necessity can only be served by a personal diary, which also helps to secure one's thoughts. The thought bubble diary is an application where one can save their thoughts. Users can make entries every day and their entries are encrypted. The encryption cipher used is AES and the user entries are encoded before they are inserted into the database. To view these entries, they are decrypted before presenting them to the user.

Background

There are many applications on play store that implements a diary application, but there are a limited number of applications that store the user data encrypted. Some of the journaling applications also include image journaling which makes it convenient to journal on the go. Several journaling applications have their proprietary cloud storage which sometimes takes away user's control over their data. They can be made better if the application were made more secure and perhaps made available across various platforms. A multitude of APIs can be used in order to make the app more compatible with other applications.

Existing System:

There are many diary-making apps for android that notably lacks security of the data. Android OS by itself is well-known to be devoid of stability concerning safety, though it is improving with time. Such systems need an added layer of security to protect data. Some of the existing features like the fingerprint can be compromised using third-party applications that spoof fingerprint data.

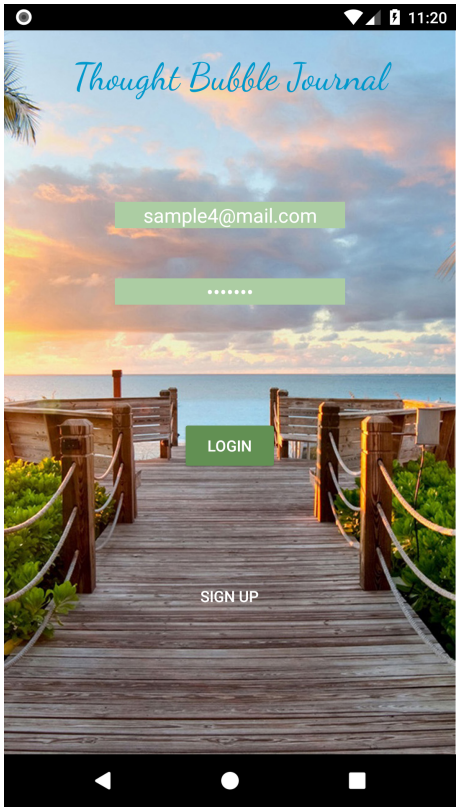
Thompson Rajan
CWID:20082947

Proposed System:

The Thought Bubble Diary was built with a motive to encourage users to create an alphanumeric password. This passcode is converted to the SHA-1 signature which will be used to encrypt user entries using AES-256 where the SHA-1 signature plays the role as the key to the cipher. The users can log in and make entries after registration. The entries are encrypted and are then stored in the SQLite database. The users can manage entries, make changes or read them.

Methodology

- Initially, the application was modeled so as to identify what components should be created and where they would go. It started with the Android activity (Sign-Up Activity) that takes the user credentials.

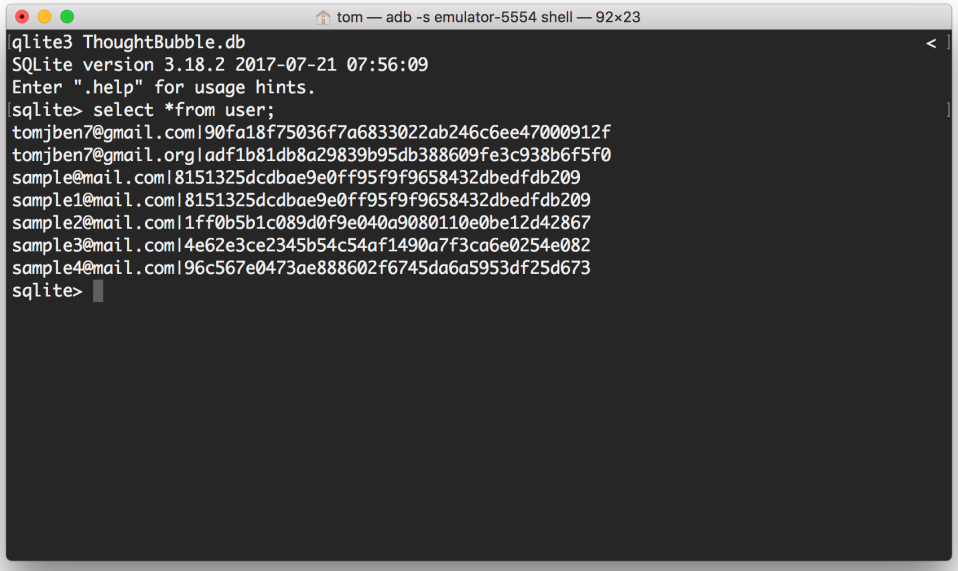


Thompson Rajan
CWID:20082947

- The credentials are validated to ensure data have their proper format.

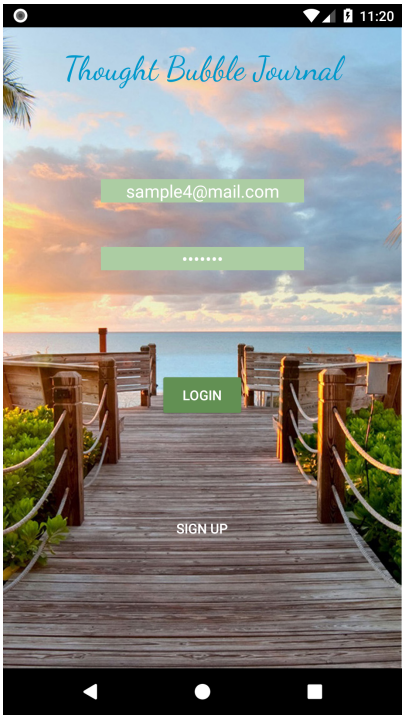
- The database was created as the backend for the application with one table holding the user credentials and another table to store user entries with the primary key being user's email address, which is most probably a Gmail address.

- The SHA-1 signature is created for the user password and is then with the other details are stored into the user table.

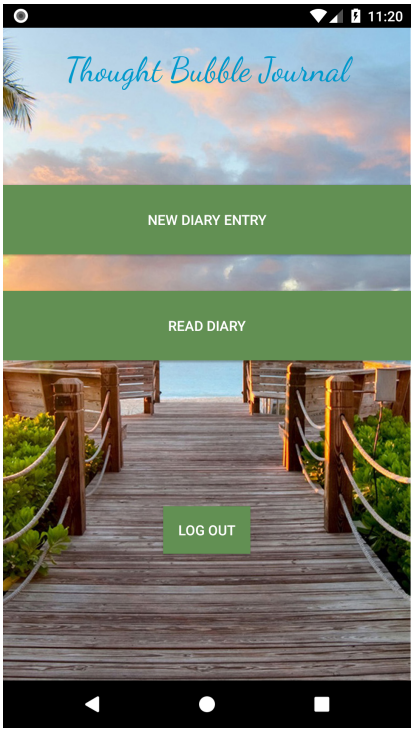


- The user is then directed to log-in using the email and password, where the SHA-1 signature of the password is generated.

Thompson Rajan
CWID:20082947



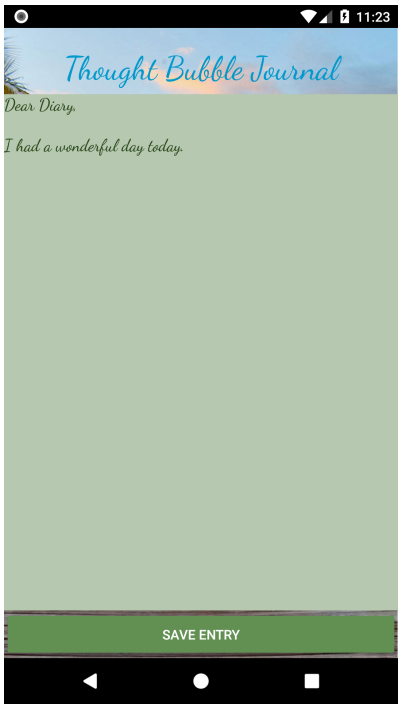
- This signature is compared with the signature from the user table. If they match, the user is directed to the app menu



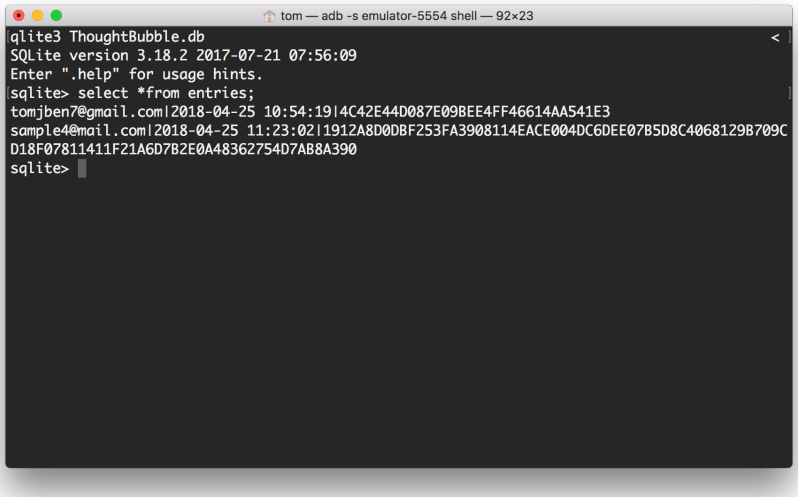
- From the app menu, the user can create new entries and make pages in the diary.

Thompson Rajan
CWID:20082947

- When the user saves the entry, the contents of the diary page is encrypted with AES-256.

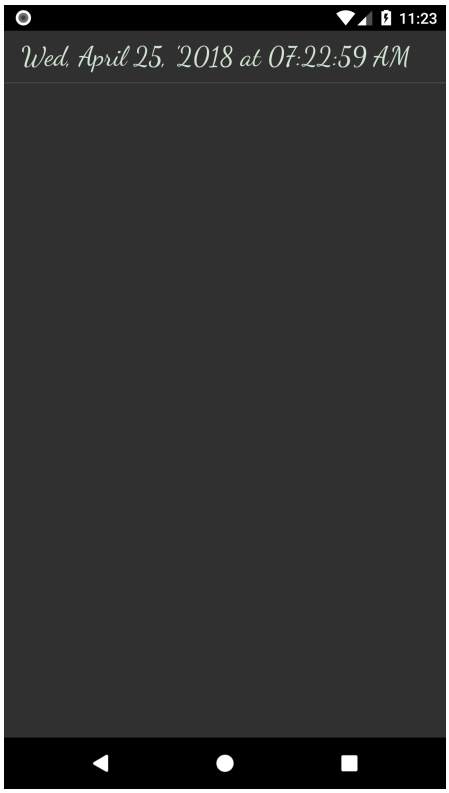


- For the input key to the AES cipher, the user's signature is used. And so, the encrypted data is stored into the entry table



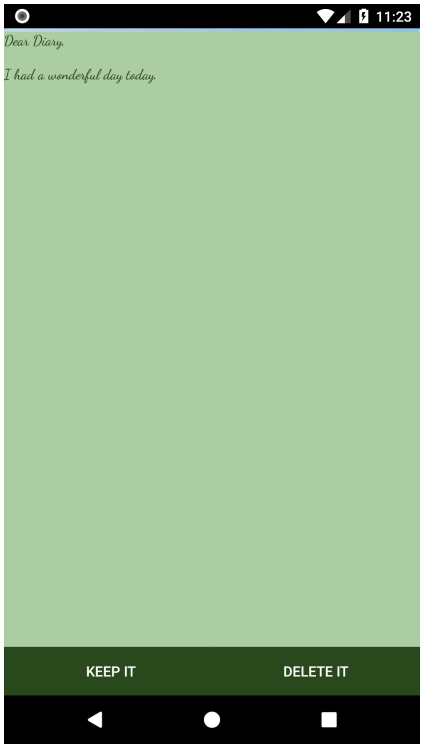
Thompson Rajan
CWID:20082947

- From the app menu, the user can read the entries through the ‘read entry’ button which will direct to the list activity which lists all the entries created by the user.



- The user can click on any entry to view them, which will retrieve the time stamp and the encrypted entry from the database. This entry is then decrypted and is rendered on the test panel where the user can see the contents.

Thompson Rajan
CWID:20082947



Experiments

- Most of the trials were made to verify if the data is being stored in the database. Android's ADB shell was used to gain access to the database files and lookup data stored in the tables using general SQL queries.
- When the query data was retrieved, significant effort was made to make this data available to all intents (Activity) so that they were operable throughout the application.

Discussions / Future Scopes:

Using the ADB shell to verify the tables enabled to progress toward creating the user login activity and authenticate users against their credentials. This also ensured that the user was able to make entries so that they are recorded as is in the entries table. When the database is well populated with user data, the application was able to create files from the individual entries from the entries table. Furthermore, the app data can be pushed to cloud through the Google Drive API. Certain methods to create files from the database also need to be implemented so that they can be pushed to the cloud

Thompson Rajan
CWID:20082947

Conclusion

A habit of journaling is a fun way to record blissful events, which can help connect clues to answer one's journey of life. And these personal records must be kept safe, secure and conveniently accessible. The cloud diary app serves these necessities. The algorithm used to encrypt user entries is AES. This algorithm is used to encrypt user entries and is then stored in the database. The app stores the user data in Android's default database SQLite. The entries make the individual files in the local directory which is then pushed to the cloud. All entries made by the user is encrypted and stored in the database. While the user views the entries, the respective encrypted copy of the entry is brought in to be decrypted before presenting to the user. The cloud diary makes use of Google Drive to store user data so that it can be accessed across devices.

References

1. Cahya, Risky & Made, I. (2016). *Data Exchange Service using Google Drive API*. International Journal of Computer Applications. 154. 12-16. 10.5120/ijca2016912187.
2. Roussev, Vassil & Barreto, Andres & Ahmed, Irfan. (2016). *Forensic Acquisition of Cloud Drives*. Greater New Orleans Center for Information Assurance (GNOCIA)

Thompson Rajan
CWID:20082947