User data security

* Use internal storage for sensitive data

Every Android app has an internal storage directory associated with it whose path is based on the package name of the app. Files inside this directory are very secure because they use the MODE\_PRIVATE file creation mode by default. This means the files cannot be accessed by any other app on the device.

* Encrypt data on external storage

The internal storage capacity of an Android device is often limited. Therefore, at times, you might have no choice but to store sensitive data on external storage media, such as a removable SD card.

Data on external storage can be easily accessed by users and other apps, so it is important to store it in an encrypted format. One of the most popular encryption algorithms used by developers today is AES.

* Use HTTPS

All communications between app and servers should be over an HTTPS connection. By using HTTPS, as long as the server is configured with a certificate issued by a trusted certificate authority, you can be sure that your network traffic is secure against attacks.

* Avoid asking for personal data

Unless having a good reason and a very secure infrastructure to collect user information, we must avoid directly asking for it in your apps.

A better approach to user authentication and user profile information look up on Android is through the [Google Identity Platform](https://developers.google.com/identity/). Google Identity Platform allows users to quickly sign in to your app using their Google account. After a successful sign in through the platform,