Problem Statement

**a) What is the difference between Internal Storage & External Storage?**

**Internal storage:**

\* Unlike external storage, internal storage is always available, but generally has less free space

\* Files are not accessible to the user (unless the device has root access)

\* Files are automatically deleted when your app is uninstalled (or with the Clear Cache/Cleanup File option in the App Manager)

External storage:

\* The device may not have external storage or it may be inaccessible (such as when it's connected to a computer)

\* Files are accessible to the user (and other apps) without requiring root access

\* Files are not deleted when your app is uninstalled (unless you use getExternalFilesDir() to get app-specific public storage)

**b) For how long the data resides in the cache?**

Ans. Data resides in cache until it is cleared by user or the application gets uninstalled by the user.

**c) What are the critical Permissions and Normal Permissions? What are the examples of each?**

System permissions are divided into several protection levels. The two most important protection levels to know about are *normal* and *dangerous* permissions or critical permissions :

* *Normal* permissions cover areas where your app needs to access data or resources outside the app's sandbox, but where there's very little risk to the user's privacy or the operation of other apps. For example, permission to set the time zone is a normal permission. If an app declares that it needs a normal permission, the system automatically grants the permission to the app. For a full listing of the current normal permissions.eg., ACCESS\_LOCATION\_EXTRA\_COMMNDS, ACCESS\_NETWORK\_STATE, ACCESS\_WIFISTATE.
* *Critical or Dangerous* permissions cover areas where the app wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps. For example, the ability to read the user's contacts is a dangerous permission. If an app declares that it needs a dangerous permission, the user has to explicitly grant the permission to the app. eg., READ\_ALENDER, WRITE\_CALENDER, READ\_CONTACTS,WRITE\_CONTACTS.