|  |  |
| --- | --- |
| Internal Storage | External Storage |
| It will be always available. | It’s not available always as the user can mount and Unmount the SD card storage whenever he opts for it. |
| Files , the data stored here are only accessible to the application | Its World-readable data stored (Files) can be accessed by anyone of our control |
| When we uninstall the application , the system removes all the application file from Internal storage | When we uninstall the app ,the system will not remove all the files , but it can be done if we save them in the directory getExternalFilesDir() |
| Internal storage is best when you want to be sure that neither user nor other apps can access our files | It’s best when files don’t require access permission and restrictions that we want to share with other people or try to access via computer. |

1. What is the difference between Internal Storage & External Storage?

Ans---

1. For how long the data resides in the cache?

Ans----

Data in the cache are will be available in the Memory until we go and deledte it in settings in android .

If the cache data is stored in the server then we can specify in our application such that for how long it should be available in the memory ie:we need to write in the code

1. What are critical Permissions and Normal Permissions? What are the examples of each?

Ans:----

1. Normalpermissions 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, see Normal permissions.

Eg:

* ACCESS\_LOCATION\_EXTRA\_COMMANDS
* ACCESS\_NETWORK\_STATE
* ACCESS\_NOTIFICATION\_POLICY
* ACCESS\_WIFI\_STATE
* BLUETOOTH
* BLUETOOTH\_ADMIN

1. Criticalpermissions 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 Critical permission, the user has to explicitly grant the permission to the app.

Eg:

* READ\_CALENDAR
* WRITE\_CALENDAR
* CAMERA
* READ\_CONTACTS
* WRITE\_CONTACTS
* GET\_ACCOUNTS
* ACCESS\_FINE\_LOCATION