**ASSIGN 14.1(Saving Data & Working with System Permissions)**

**Q:14.1(a) What is the difference between Internal Storage & External Storage?**

**Answer :** **Internal Storage**: Stores private data on the device memory. You can save files directly on the device's internal storage. By default, files saved to the internal storage are private to your application and other applications cannot access them (nor can the user). When the user uninstalls your application, these files are removed.

**External Storage**: Stores public data on the shared external storage. Every Android-compatible device supports a shared "external storage" that you can use to save files. This can be a removable storage media (such as an SD card) or an internal (non-removable) storage. Files saved to the external storage are world-readable and can be modified by the user when they enable USB mass storage to transfer files on a computer.

**Q:14.1(b) For how long the data resides in the cache?**

**Answer:** You can clear the catch at any time when you feel your phone is bit lagging and space is low. it does not have a specific time.

**Q:14.1(c) What are the critical Permissions and Normal Permissions? What are the examples of each?**

**Answer**: **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, see Normal permissions.

Eg:Bluetooth, NFC, Set\_Alarm.

**Critical 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: Cameras, Read\_Contacts, Send\_sms, Receive\_sms.