**ACADGILD Session 14:**

**Saving Data &**

**Working**

**with System Permissions**

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

* When building an app that uses the internal storage, the Android OS creates a unique folder, which will only be accessible from the app, so no other app, or even the user, can see what's in the folder.
* The external storage is more like a public storage, so for now, it's the SDcard, but could become any other type of storage (remote hard drive, or anything else).
* External Storage has two types:

**Primary External Storage:** In built shared storage which is "accessible by the user by plugging in a USB cable and mounting it as a drive on a host computer". Example: When we say Nexus 5 32 GB.

**Secondary External Storage:** Removable storage. Example: SD Card.

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

* Caching is the process of saving data temporarily so the site, browser or app doesn't need to download it each time.
* You can clear the cache on Android, to free up phone space for example, in Settings. Go to "Apps" (or "Applications", depending on your device) in the menu, find the app want to clear the cache or data for and tap on "Storage." The buttons for clearing the cache and app data will become visible and you can see how much storage is being used, and clear it.
* When the user uninstalls the app, cache files are removed.

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

* The purpose of a permission is to protect the privacy of an Android user. Android apps must request permission to access sensitive user data (such as contacts and SMS), as well as certain system features (such as camera and internet). Depending on the feature, the system might grant the permission automatically or might prompt the user to approve the request.
* Normal permissions are permissions which are deemed harmless for the users privacy or the operation of other applications. For example, the permission to set the time zone. Normal permission are automatically granted to the application.
* Critical permissions affect the users private information, or could potentially affect his data or the operation of other application. For example, the ability to read the users contact data. Dangerous permissions must be granted by the user at runtime to the app.
* Examples of **Normal Permissions**:   
  android.permission.ACCESS\_NETWORK\_STATE  
  android.permission.ACCESS\_NOTIFICATION\_POLICY  
  android.permission.ACCESS\_WIFI\_STATE  
  android.permission.BLUETOOTH  
  android.permission.INTERNET
* Examples of **Critical Permissions:**

android.permission.READ\_CALENDAR

android.permission.ACCESS\_FINE\_LOCATION

android.permission.ACCESS\_NETWORK\_STATE

android.permission.READ\_SMS

android.permission.BODY\_SENSORS