Advancement In Android Operation

Akshit Jaggi

Student, Dronacharya College of Engineering, Gurgaon.

Android is an operating system. It is an open source code. You can enjoy more than 700,000 apps and games, millions of songs, thousands of movies, etc. on your Google Android device. It is full of features like widgets, instant notifications, multi-tasking, voice recognized commands, screen rotation, brightness control and easy data sharing. In present time, the devices come with processors more than single core like dual-core, quad-core and the latest octa-core which uses minimum of 1GB RAM. After getting loaded by thousands of features, the Android devices still lags at many points. This review will provide detailed information about the Android operating software along with its point of lag and will even provide the steps that can overcome many problems and will reduce its lagging problems.

Keywords

Operating system, applications/apps, malwares, widgets, interface, Google Play and sandbox.

Introduction

Android is an operating system used primarily for touch-screen mobile devices such as smart-phones and tablets, based on Linux. It is open source and its code is released under Apache License by Google. There is no other software quite like Android with millions of applications, games, songs and videos available with Google Play. Its every version is named after a desert like jelly bean, donut, éclair, kitkat, etc.

Applications of Android, that extends the functionality of these devices, written primarily in java programming language but in a customized way.

Android devices consist of many internal hard-wares like accelerometers, gyroscopes and proximity sensors which are used by many applications to respond to the actions of user. For example, screen rotation from portrait to landscape depending on device orientation. Its response is based on swipping, tapping, pinching and reverse pinching on the screen, which is now-a-days capacitive while in olden days it was resistive.

Android devices also have Sandbox comprised in the device internal circuit. The Sandbox is an isolated area of the system. Rest of the system's resources does not have access to this area unless accessible permissions are granted by the user while installation of applications. Android Devices are user friendly which gives the user an ease of access. User can access all Google stuff like Gmail, photos, etc. quickly and easily just after signing in to the device, either it's a phone or a tablet, with Google. The user can enjoy all favorite entertainment and stuff without using wires and even without syncing. More than 700,000 apps and games, millions of songs, thousands of movies and TV shows, the world's largest collection of eBooks, and a growing selection of magazines, the user can enjoy all of these favorite stuff via Google play very easily.

Features

Widgets

The users can interact with their favorite apps from their home page directly with the help of widgets. They can view their favorite photos, check weather, see the latest sport scores and even peak at their inbox without leaving the home page.

Notifications

Quick access to calls, incoming texts and new mails in a non-intrusive way just by using the notification tray.

Multi-tasking

You can quickly access to other applications at a single time without leaving other applications. It has been never easier before on a mobile device for juggling multiple tasks at once.

Voice Commands

The Android device can be operated on voice commands in different languages. The system supports more than 30 languages.

Data-(photos and videos)

User can take every special moment by capturing it in high definition pictures and videos. Users can explore their shots and can even quickly share their favorite data in any way that they want.

Special Features

IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013
ISSN: 2320 - 8791
www.ijreat.org

Android was the first operating system which introduced features like face unlocking (which uses facial recognition to let the user unlock their device), Android beam (which lets the user to share contacts, data and more by touching two devices together) and Google Now (which brings the latest updates before the user asks)
Versions

Version	Code Name	Release Date
1.0	Android	23/Sept/2008
1.1	Android	09/Feb/2009
1.5	Cupkake	30/Apr/2009
1.6	Donut	15/Sept/2009
2.0/2.1	Éclair	26/Oct/2009
2.2	Froyo	20/May/2010
2.3/2.3.2	Gingerbread	06/Dec/2010
2.3.3/2.3.7	Gingerbread	09/Feb/2011
3.1	Honeycomb	10/May/2011
3.2	Honeycomb	15/Jul/2011
4.0.3/4.0.4	Ice Cream Sandwich	16/Dec/2011
4.1.1/4.1.2	Jelly Bean	09/Jul/2012
4.2.1/4.2.2	Jelly Bean	13/Nov/2012
4.3	Jelly Bean	24/Jul/2013
4.4	KitKat	--/--/----

Main Problems

1. Soft-wares or security firms, such as McAfee, AVG Technologies, etc. are ineffective due to applications of Sandbox which limits their ability to scan deeper system for threats.
2. Many applications that are not compatible to certain devices can even be installed by user.
3. Very low percentage of Android Malware or bugged applications is reported from Google Play store.
4. Through the online interface of Android devices, the user can be easily tracked or located.
5. It is worldwide known that many organizations have access to the user data in Iphones, Blackberries and as well as Android Devices.
6. Many applications still use to run after closing them manually which occupies unnecessary RAM space. This results in not so quick response while operating heavy applications.
7. Many Android devices create online backup data, of pictures, videos, music, texts, etc., by using the user's account without informing the user.
8. Many applications store the ids and passwords of user's commonly accessed accounts and many users does not even aware of it.

Points to be implemented:

1. Soft-wares or security firms, such as McAfee, AVG Technologies, etc. are ineffective due to applications of Sandbox which limits their ability to scan deeper system for threats. For this problem and to make device more stable, an inbuilt application must be provided in order to prevent the device from viruses and malwares as well as aware the user about the threats and how it can be prevented in future, when that application may not work properly. The application must register, with unique serial numbers for different devices, when the installation of Android interface took place. It should not be uninstall and will be updated itself after a required time period.

2. Many applications that are not compatible to certain devices can even be installed by user. Some user gets successful in installing certain applications which are not compatible with the device by any un-fare means. The android should be protective enough to prevent the device from these applications by increasing the protection. This can be done by providing Android interface an in-built brain to tackle the applications either by un-installing itself or resist the application's working.

3. Very low percentage of Android Malware or bugged applications is reported from Google Play store.

Android can be expanded very much and that is its advantage but the problem arises with it as its expansion leads to many drawbacks and it should work more efficiently in the field of malware and virus protection.

4. Through the online interface of Android devices, the user can be easily tracked or located. Mostly the applications available for android are bugged and can lead to the device's tracking or hacking with their installation.

IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013
ISSN: 2320 - 8791
www.ijreat.org

Android must be aware of these and final warning should be given by the device for every bugged application.

5. It is worldwide known that many organizations have access to the user data in Iphones, Blackberries and as well as Android Devices.

Many Governmental or Non-governmental organizations crack in to many of the I-phones, blackberries and android devices.

Due to the expanding quality of android, many organization crack into it and they can use the user's personal data without the user's consent. This is due to the account login in Android to secure the device but the device rather may lose the information on the user's internet profiles on various Social sites as well as other mailing and personal sites. This can be prevented by making authorized login in Android devices through a secondary Identity and that ID can use the personal ID only when user need to and still it should ask for several permissions.

6. Many applications still use to run after closing them manually which occupies unnecessary RAM space. This results in not so quick response while operating heavy applications.

This is one of the most common problems in every Android Device. The Android Operating System developer should make his working in such a way that background activities should be close when the user manually stops it or quit the applications.

7. Many Android devices creates online backup data, of pictures, videos, music, texts, etc., by using the user's account without informing the user.

The operating System must not allow the online applications to store the data itself. This can be done when there must a provision given in the system to make a virtual boundary between the user's personal data and cloud storage.

8. Many applications store the ids and passwords of user's commonly accessed accounts and many users does not even aware of it.

The system should remind the user before installation or working of application that it can store essential data itself by extracting from the device.

Conclusion

Android devices are loaded with many features based on many high technologies but still it is unable to perform perfectly at times. Android Devices should be comprised of many essential features just to make the device more stable, protective and to prevent lagging in the devices. The application/s must be of lower data memory space in order to occupy less space on permanent memory of the device. The application should work on the principle of Device protection and security leak prevention principles, so that it can be used without being an utter of getting cracked or hacked by anyone and even the user will be got benefited of its lag-free interface. The background processes should be reduced and also the leakage of personal data through unnecessary online backup should ask for permissions first

Acknowledgment

References

[1]en.wikipedia.org

[2]www.android.com

[3]www.wikihow.com

[4]androidtrickz.com