*International Journal Of*

**Recent Scientific Research**

**ISSN: 0976-3031**

**Volume: 7(4) April -2016**

# DESIGN AND IMPLEMENTATION OF MOBILE PHONE CLONING

**Mahalakshmi V., AntoBennet M., Aravind S and Jayavignesh B.S**

THE OFFICIAL PUBLICATION OF
INTERNATIONAL JOURNAL OF RECENT SCIENTIFIC RESEARCH (IJRSR)
http://www.recentscientific.com/ recentscientific@gmail.com

ISSN: 0976-3031

*Available Online at http://www.recentscientific.com*

*International Journal of Recent Scientific Research*
*Vol. 7, Issue, 4, pp. 9979-9981, April, 2016*

**International Journal of Recent Scientific Research**

**Review Article**

# DESIGN AND IMPLEMENTATION OF MOBILE PHONE CLONING

**Mahalakshmi V[1]., AntoBennet M[2]., Aravind S[3] and Jayavignesh B.S[4]**

[1,2,3,4]Department of ECE, VELTECH, Chennai, India

**ARTICLE INFO**

***Article History:***

Received 05th January, 2015
Received in revised form 08th February, 2016
Accepted 10th March, 2016
Published online 28st April, 2016

***Keywords:***

Smart phone, Short Message Service (SMS), Subscriber Identity Module (SIM).

**ABSTRACT**

The usage of smart phones among people is increasing rapidly. With the phenomenal growth of smart phone use, smart phone theft is also increasing. This paper proposes a model to secure smart phones from data loss even when the phone was stolen by someone and also it provides options to access a smart phone through other smart phone via Short Message service (SMS). The data loss can be prevented by retrieving the important data from the phone such as contacts, word documents and media files. This paper also includes the location identification of the theft mobile phone when the call is made through the mobile phone after the Subscriber Identity Module(SIM) was changed in that mobile phone.



## INTRODUCTION

Nowadays, usage of mobile has become a vital part of day-to-day activities of people. We can refer the current time as the era of Smart phones. Suppressing all other traditional communication purpose, smart phones are now at the peak of popularity in their usage of accessing the internet which includes mail access, social networking, mobile shopping and mobile banking. Smartphone usage of people is studied in [1]. Smart phones contains critical and sensitive data of user like automated call records, photos, videos and saved passwords of WebPages. So loosing the smart phone means a very high amount of irrecoverable data loss which may not be affordable in many cases. Few surveys [2][3][4] about mobile theft in various countries has been studied. This claims the need of an intelligent application to be run in mobile to eradicate mobile theft and track the mobile even after change of the SIM also.

### *Android*

Android delivers a complete set of software for mobile devices: an operating system, middleware and key mobile applications.

Figure 1 shows the architecture of the android application. The bottom layer of android architecture is Linux - Linux 2.6 with approximately 115 patches. This provides basic system functionality like process management, memory management, device management like camera, keypad, display etc. On top of Linux kernel there is a set of libraries including open-source Web browser engine WebKit, well known library libc, SQLite database which is a useful repository for storage and sharing of application data, libraries to play and record audio and video, SSL libraries responsible for Internet security etc. This is the third section of the architecture and available on the second layer from the bottom. This section provides a key component called **Dalvik Virtual Machine**[5] which is a kind of Java Virtual Machine specially designed and optimized for Android. The Application Framework layer provides many higher-level services to applications in the form of Java classes. Application developers are allowed to make use of these services in their applications. The applications are at the topmost layer of the Android stack. An average user of the Android device would mostly interact with this layer (for basic functions, such as making phone calls, accessing the Web browser etc.).

### *Android activity life cycle*

Activities in the system are managed as an *activity stack*. When a new activity is started, it is placed on the top of the stack and becomes the running activity -- the previous activity always remains below it in the stack, and will not come to the foreground again until the new activity exits.

Figure 2 depicts the activity life cycle of the android application. An activity has essentially four states:

**Corresponding author: **Mahalakshmi V***
*Department of ECE, VELTECH, Chennai, India*

- If an activity in the foreground of the screen (at the top of the stack), it is *active* or *running*.
- If an activity has lost focus but is still visible (that is, a new non-full-sized or transparent activity has focus on top of your activity), it is *paused*. A paused activity is completely alive (it maintains all state and member information and remains attached to the window manager), but can be killed by the system in extreme low memory situations.
- If an activity is completely obscured by another activity, it is *stopped*. It still retains all state and member information, however, it is no longer visible to the user so its window is hidden and it will often be killed by the system when memory is needed elsewhere.
- If an activity is paused or stopped, the system can drop the activity from memory by either asking it to finish, or simply killing its process. When it is displayed again to the user, it must be completely restarted and restored to its previous state.


**Fig 1** Android architecture

### *Proposed System*

In the proposed system, the entire project is going to be installed in the android mobile just like an application similar to games, web browser, etc…Within that application the predefined number (i.e. mobile number of family or friends)has to be stored once the application is installed and the modules necessary for us must be enabled with the passkey.

### *Module I*

In the first module the message will be send to the predefined number that has been already stored in that mobile phone when the SIM was changed in the theft mobile phone.

### *Module II*

In the second module the important data such as contacts, files and pictures in media files can be retrieved from the stolen mobile phone without the knowledge of the person who has stolen the mobile phone.

### *Module III*

In the third module we can delete the retrieved data in the stolen mobile phone by sending the notification. After receiving the notification, the data will get erased.

### *Module IV*

In the fourth module the location of the theft mobile phone can be identified once the call is made from that phone to any number through different SIM.

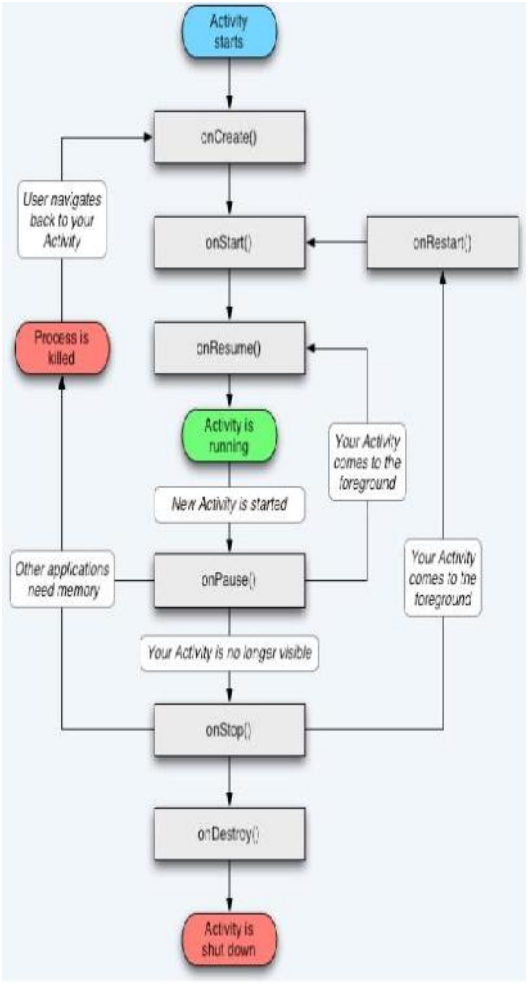


**Fig 2** Activity life cycle

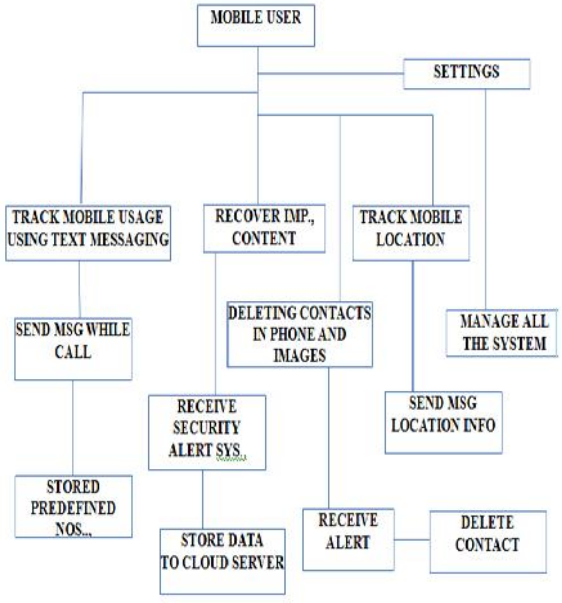


**Fig 3** Architecture of the proposed system

**Fig 4** Debugging of android application

**Figure 4** shows how to debug the android application.

## CONCLUSION

The remote data retrieving and wipe services are necessary to protect against the private data disclose. At the same time, it must prevent the malicious user from launching DoS attacks that's ends such commands to the normal users intentionally. We also demonstrated our implementation and test result of the proposed system running on Android smartphone.

## Reference


1. Hossein Falaki, Ratul Mahajan Srikanth Kandula, Dimitrios Lymberopoulos, Ramesh Govindan, Deborah Estrin: Diversity in smartphone usage, Proceedings of the 8th international conference on Mobile systems, applications, and services, ISBN: 978-1-60558-985-5
   Survey about mobile theft in UK:
2. http://news.bbc.co.uk/2/hi/uk_news/1748258.stm
3. Survey about mobile theft in USA: http://www Symantec.com/about/news/release/article.jsp? prid=2 0110208
4. Survey about mobile theft in India:http://asiarelease.asia/norton-survey-reveals-1-in-2-indians-is-avictim-of mobile phone loss or theft/
5. stack overflow.com/…/how - an- android application is executed on dalvik


*******


**How to cite this article:**

Mahalakshmi V., AntoBennet M., Aravind S and Jayavignesh B.S.2016, Design and Implementation of Mobile Phone Cloning. *Int J Recent Sci Res.* 7(4), pp. 9979-9981.

TSSN 0976-3031