International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Index Copernicus Value (2015): 62.86 | Impact Factor (2015): 3.791

# Advanced Authentication System for Android Smartphone

**Rachana Ghongade[1], Supriya Gondkar[2], Nikita Gunjal[3], Varsha Hon[4]**

Department of Computer Engineering, S.R.E.S's College of Engineering, Kopargaon, City-Kopargaon, SPPU, India

**Abstract:** ***Developed by the Open Handset Alliance (visibly led by Google), Android is a widely anticipated open source operating system for mobile devices that provides a base operating system, an application middleware layer, a Java software development kit (SDK), and a collection of system applications. Android mobile application development is based on Java language codes, as it allows developers to write codes in the Java language. Mobile Development India has worked extensively on projects ranging from gaming software, organizers, media players, picture editors to go-cart devices and more. Most of the devices used in IT services are rapidly changing from PCs and laptops to tablets and smart phones. Since these devices contain important personal information, better security is required. Major problems could occur if the mobile is lost. So proper authentication system is very important. Different authentication schemes are available with both advantages and disadvantages. The authentication schemes must be made by keeping in mind the requirements of the users and the android architecture.***

**Keywords:** Android, security, hacker, Authentication

## 1. Introduction

Googles operating system Android is now becoming more and more popular because it is open source ,user friendly. that why most of the mobile device manufacturers move towards android .Today everyone is having android smart phone in his pocket. As the popularity of android smart phone is increasing day by day it is become very important to provide security to the smart phone.

Already many systems are developed to provide security to the smart phone,but each system is having some drawbacks. So we are going to develop a system that will provide better security as compared to others. The proposed system contains a circular screen lock pattern to unlock the phone in which each circle can be retouch seven times and it will changes its color at every touch, unlock phone using random number, generate system backup, receive notification of Subscriber Identity module change which is able to support authentication for the user's convenience and provide a good security system for smart phones. The proposed system is used to provide "Advanced Authentication For Android Smartphone" .This system consist of circular lock screen pattern to unlock the phone in which each circle can be retouch and it will changes its colour seven times. When smart phone is lost or gets stolen then the proposed system can enable to unlock phone using random number, taking system backup via email, receive notification of SIM change, tracking incoming calls and messages.

## 2. Literature Survey

To provide security to the android smart phone a circular screen locking application is provided. This application provides various features like unlock phone using random number, taking system backup via email, receive notification of Subscriber Identity module change via message, track incoming calls and messages when our smart phone is lost or stolen. This helps user to know who is calling and sending messages on their device. Hence this application satisfies the need of today's users and applications.[1]" An upgraded Lock Screen system, which is able to support authentication and provide a good security system for Android smart phones has been presented in Users convenience has also been taken into account. For user convenience two modes are provided: User Mode and Guest Mode. In User mode, we can do everything with our mobile phone, but in Guest mode, we can only do the operations that are authorized by the User. Guest mode can be entered by simply shaking the mobile phone whereas password can be entered for entering into the User mode [2]. A Secured Authentication in Android Phones Using 3 D password. The proposed system is a multi-factor authentication scheme. It can syndicate all prevailing authentication schemes into a single 3D virtual environment. This 3D virtual environment comprises some objects or items with which the user can interact. The user is obtainable with this 3D virtual environment where the user navigates and interacts with numerous objects. The categorization of actions and interactions toward the objects inside the 3D environment constructs the users 3D password. The 3D password can conglomerate most existing authentication techniques such as textual password scheme, graphical password scheme, and various types of biometrics scheme into a 3D virtual environment [3].

## 3. Existing System

There are some system which are already in existence such as

1) Slide Unlock
2) Face Unlock
3) Finger Print Scanning
4) Keypad lock

**a) Slide Unlock**

Slide lock is one of the locking system provided by the smartphone companies. In this locking scheme screen is provided with a circle with a lock inside and user to slide that circle outside of one large circle. one of major drawback of that system is that even if phone is unlock one can still access all notifications on his screen. There is no need to fully unlock the phone.

**b) Face Unlock**
To unlock the phone using this system user has to first place his face inside a face shape ring of dots using front camera. If system decides that its enough to unlock the phone then phone will be unlocked.

**c) Finger Print Scanning**
Now-a -days most of the mobile phones are coming with this feature i.e. finger print scan. No matter it provide good security but low speed and overlapping processes are the main drawback of this system.

**d) Keypad Lock**
This scheme require a four-digit password so it provides key space from 0 to 9999. Repititive input touching is required, it become one of the inconvenience factor.

## 4. Proposed System

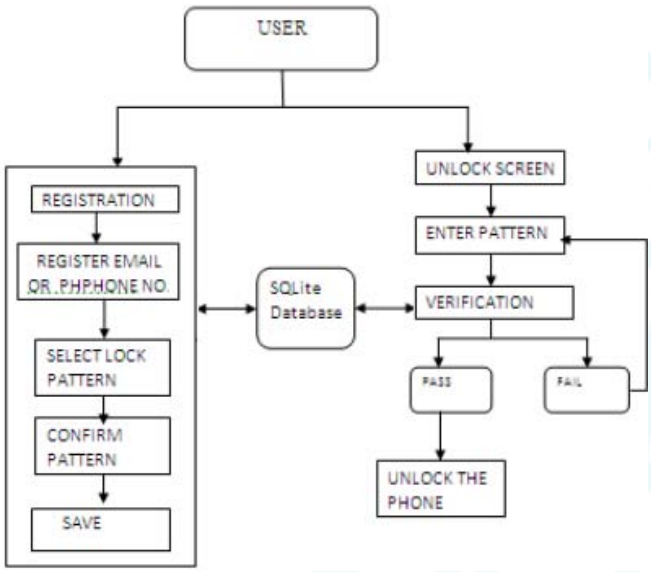



**Figure 1:** System Architecture

The above Architecture is giving us the details about the process of setting the lock pattern to unlock the phone & how to unlock the phone using that set pattern. When user is going to register for the application he/she has to enter his/her email-id,one or more phone numbers as a reference.

When actually user is going to set pattern that set pattern will be stored in database. At the time of unlocking the phone using that Pattern that pattern entered by user & one which is stored in database gets verified if match is found phone get's unlock otherwise not.

If user fail to unlock the phone using that pattern in three attempt system will generate RANDOM NUMBER that random number will be send to the registered Email or reference phone number. For that random number also user has only three attempt .Even in this three attempt user fails to unlock system start to take backup of the phone &store it on the cloud or send it to the registered number.

IN case if the mobile phone is get stolen and the one who has stolen that phone insert a new SIM card in that in that case all SIM details, contact message will be send to the authorised user.

**Workflow of the System**

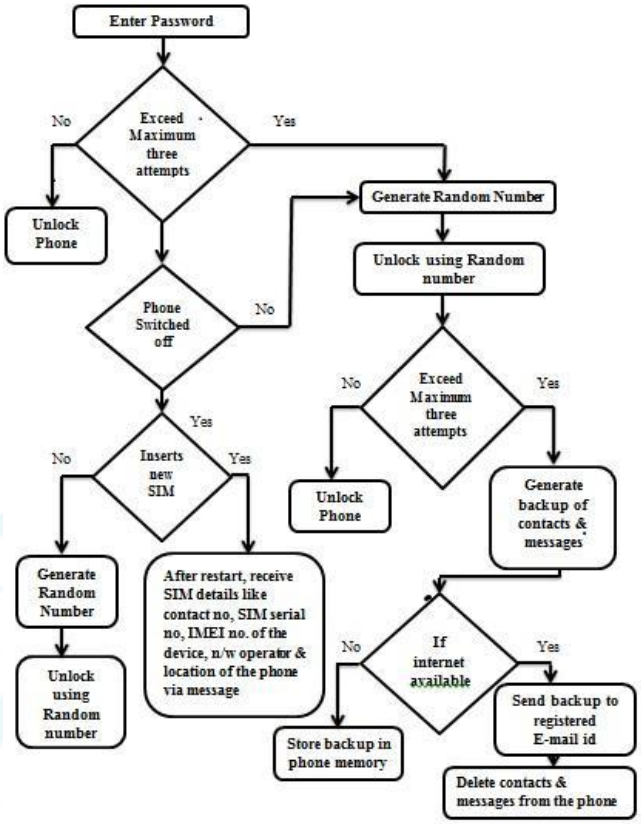


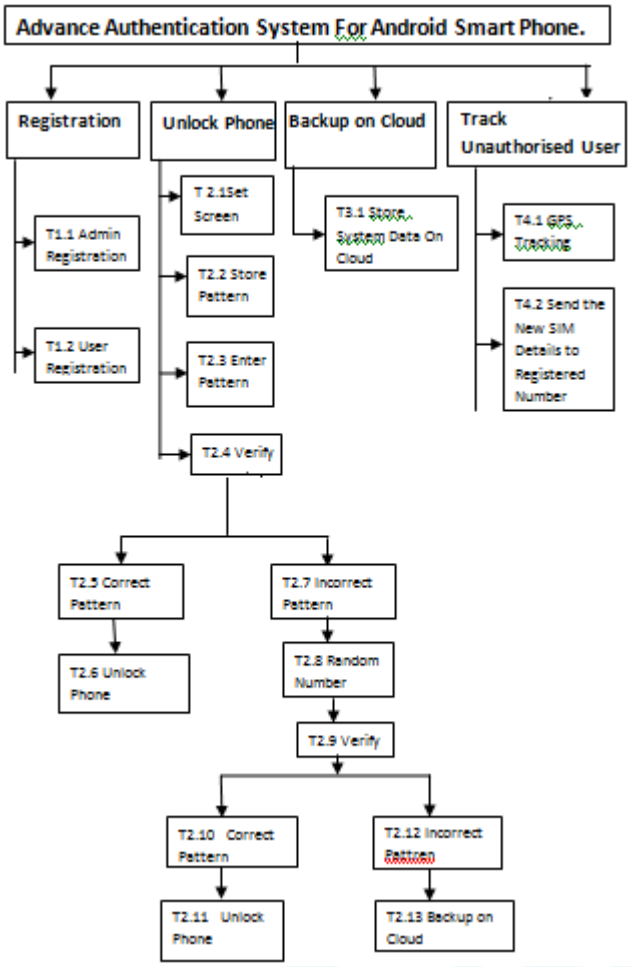

**Figure:** Workflow of the System:

## 5. Proposed System Workflow (Implementation)

**A) Registration**
In this module, registration of admin and user will be done for authentication and privacy.

**a) Admin registration**
In this task admin should give his details for registration. For registration admin need to enter name, email address, phone number etc. he can access the users details as well. He can verify the details of registered user.Registration details are stored on database for further verification.

**b) User registration**
In this task registration of user will be done. For registration user need to enter name, reference email address,reference one or more phone number etc. Registration details are stored on database for further verification.




**B) Unlock Phone**
In this module, process of unlocking the phone is describe.

**a) Set lock screen pattern**
In this task user has to set the lock screen pattern for future use to unlock the phone. System consist of circular screen lock, each circle changes its colour maximum of seven times by retouching the circle. The circles are touch randomly by the user, once pattern is entered user should confirm it by clicking on ok button. And then internally the password string is generated and this string is use for unlocking the phone.

**b) Pattern stored on database**
The patterns set by the user are stored on SQLite database for further verification.

**c) Enter pattern to unlock screen**
For unlocking the phone user has to enter the pattern which is already set by the user. Maximum three attempts are given to user in case of wrong pattern.

**d) Verification**
Firstly user enter the pattern for unlocking the phone, matching of pattern are done by using already stored pattern in database. But user has maximum three attempts to enter the pattern. If pattern are match then phone will be unlock. After failing three attempts application will generate random number & that number will be sent to registered reference phone numbers and email address. By using this random number the phone can be unlocked. Verification of random number also required. Random number also has maximum three attempts. If user fails to unlock the phone using random number system starts to take backup and send it to cloud.

**C) Backup on cloud**

**a) System data stored on cloud**
After failing to unlock the phone using random number system starts to take backup and simultaneously important data of system like contact, messages and other data will be formatted from the system and send it to cloud.

**D) Track unauthorized user**

**a) GPS Tracking**
If phone is lost or stolen, the location of phone will be find via GPS tracking and it will be send to authorized user.

**b) Send the New SIM Details to Registered Number**
When the user phone are stolen and new SIM is inserted by unauthorized user or the SIM card is changed in the phone, the SMS will be sent from a new SIM which is placed by the person, who changed it, and using that phone number the network provider can be contacted and location details can be inquired. This SMS contains information of new SIM number, SIM serial number, IMEI number of the device & the network operator.

## 6. Acknowledgement

We gratefully acknowledge H.O.D of computer engineering department of our college for their kind support for this project. We also thank our project guide and co-guide for highlighting our path and their gracious guidance. In last we like to thank all the friends who had given some valuable contribution for this system.

## 7. Conclusion

In this thesis, we analyzed problems in the current security system for smartphones and we are going to suggest the advanced authentication system for android smartphone. Praposed system will improve security and privacy of user by providing the function like backup an cloud and track unauthorized user. System provide the protection of personal information.

## References

[1] Swapnil Waghmare,Satish L.Varma, Madhumita Chatterjee Authentication System for Android smartphones ,International Journal of Computer Applications (0975 8887) Volume 87 No.5, February 2014.
[2] Kwang Il Shin, Ji Soo Park, Jae Yong Lee, Jong Hyuk Park Design and Implementation of Improved Authentication System for Android Smartphone Users,26th IEEE International Conference on Advanced Information Networking and Applications Work-shops,2012.
[3] SECUDROID - A Secured Authentication in Android Phones Using 3D password Ms. Chandra Prabha K M.E.

Ph.D.1, Mohamed Nowfel2 E S, Jr., Gowtham V3, Dhinakaran V4 Department of CSE, K.S.Rangasamy College of Technology, Tiruchengode 637215 India, Tamilnadu, India1.