A Simple Face-based Mobile Security System Design for Android Phone Protection

Alabi A. A.
Adjunct Lecturer,
Computer Science Department,
Oduduwa University Ipetumodu
Osun State, Nigeria

Ogundoyin I. K.
ICT Department,
Osun State University, Oshogbo,
Osun State, Nigeria

ABSTRACT

The advent and use of mobile phones have added a lot to the world's social lives as technology keeps evolving on a daily basis but also face a bit of challenges such as info theft, misrepresentation, impersonation etc. with a view to causing mayhem; a scenario that calls for a more secured mode of phone access for protection sake. A unit of functionality provided by the system was demonstrated with the aid of a Use-Case diagram and the procedural flow of control between the various class objects involved was illustrated using the Activity diagram. The code was written in JAVA on a platform called "Android Visual Studio" and the required tools and Texts were built with the aid of the Android In-built Controls; which generate their own codes when utilized thus providing the needed field for entering E-mail and some other required parameters. The design was made in such a way that security info was sent to a designated Email for necessary action whenever an illegal attempt is noticed on the mobile phone. The expected intruder's face captured and the registered phone location due to the provision of incorrect security codes (while attempting to log in on the phone) were sent to the phone's rightful owner inform of alert via a preset Email. This research guaranteed privacy in addition to exposing intruders no matter their motives. It also educates the masses with the basic knowledge of privacy, protection from unauthorized access and the core importance of mobile phones security.

Keywords

Security, Face, Mobile Applications, Android Phones, Java Programming

1. INTRODUCTION

The advent and use of mobile phones have added a lot to the world's social lives as technology keeps evolving on a daily basis. These days, more and more users employ different forms and make of phones not only as communication tools, but also as a means of planning and organizing work and private life. Within companies, mobile technology is constantly causing profound changes in the organization of information systems and improvising of certain technology-related needs. This has also become a source of new risks as its potentials grow. For instance, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of probably a company or government-owned institution. Many smartphones are preferred targets of attacks these days. These attacks exploit weaknesses related to smartphones that can come from means of communication such as Short Message Service (SMS) also known as "Text Message", Multimedia Messaging Service (MMS), Wi-Fi networks, Bluetooth and GSM (the de facto "global standard for mobile communication"). There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users thus causing the unthinkable. In view of this, different security counter-measures are being developed and applied to smartphones configurations, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps. Mobile Phone users are today exposed to various threats ranging from theft to unauthorized access of his/her phones with a view to causing mayhem. These threats are considered very serious in the sense that victims and stakeholders in this could suffer from end effects such as illegal transmissions of their classified info, misrepresentation, impersonation and the likes. Although, some of these mobile phones come with some inbuilt security functions which are in most cases in default form easily bypassed by people conversant with the workings of such phones. This scenario calls for a more secured mode of preventing illegal access which could also provide an undeniable form of identification should in case such negative acts take place. Mobile security today is a very important part of security scheme that required prompt and implicit attention. Aside the fact that our mobile devices (i.e. Phones) host the larger aspects of our bio-data and other forms of records, they represent the best and most available communication devices for most of our day-to-day correspondence. In the same vein, a lot of risks comes with the use of mobile phones and so serve as constraints if not cons to the pros expected to be associated with having them. One of such problem is the increasing complexity of mobile intrusion, mobile theft etc. It is therefore paramount to invest lots of interests and resource in curbing this menace for a free and safe communication system. The result of this study could serve as a breakthrough towards decreasing the stakes as stressed above with a view to maximizing the good involved. In short, the new system should be capable of eliminating some problems inherent in the existing system such as an increased guaranty of the mobile phone's security, provision for easy tacking of the phone if lost or stolen and easy capturing of intruders face and location. This article is targeted at developing a Face-Based Security System for Mobile Application with a view to exposing and neutralizing any form of threat emanating from accessing one's phone as a result of the activities of intruders. Expected goals here include gathering and analyzing of information making up records about mobile phone systems in terms of user and system data; developing a face-based security system for managing and securing those records as well as the phone's functions and evaluation the developed system.

2. RELATED WORK

Security today has become a globally challenging issue touching virtually every facet of life. In line with this, many forms of security systems have been developed to address the menace for a better appreciation of the so-called Information Communication Technology (ICT) dominated world. Many houses these days are burgled mainly by means of illegal entry by force, such as breaking a window or slashing a screen or by entering through an unlocked door or open window [1]. Also, many mobile phones owners fall victims of impersonations, information etc. as a result illegal access to victims' mobile phone records. Meanwhile, research in security has brought about many different ways of tackling most security issues reducing those of mobile applications to some extent. This is as a result of the increasing number of makes and brands coming up as ICT evolves. Most applications are pre-installed on phones during manufacturing platforms, or delivered as web applications using server-side or client-side processing (e.g., JavaScript) to provide an "application-like" experience within a Web browser. According to findings [2], the language you choose for mobile development can be the difference between great success and tremendous frustration. However, there are options but only if you know which path you're on. For instance, Java has been around for twenty years but still maintains its firm position in the family of programming languages. The language today is, according to most ways of measuring such things, the most popular programming language in the world [3]. Three broad parameters need to be taken into consideration when examining the subject area of mobile security. This is as a result of the fact that securing one's phone security (especially Android Phones) isn't only about the use a PIN lock [4]. The mobile phone is a key technology in an increasingly mobile and connected world. Growing technological convergence and ubiquitous networking leave behind a continuous and lasting trail revealing information about those involved in the communication. Picking up on this electronic trail makes it possible to identify the location of communication devices and individuals are indirectly locatable by carrying their mobile phone. In some cases, the location information supplied by a mobile phone can be very specific, depending in cell size and cell shape. Location-based services (LBS) for mobile phones are predicted to grow in the near future [5]. The mobile phone as a location technology helps in the area of identification of the approximate location of a cellphone both on a continuous basis and in real-time. Android phones for example, are made up of operating systems that give room for designing and developing security-based applications [6]. Unfortunately for some classes of phone users, new research into the security and manageability of mobile phone operating systems shows that the two most popular - Android and iOS - both pose major risks to users and their employers [7]. Another type which makes use of a SIM548C quad band GSM module which supports GPS technology for satellite navigation does exit [8]. Android is a marriage of the Linux operating system and a Java-based platform called Dalvik, which is an off-shoot of the popular Java platform. Essentially, software developers write their apps in the Java programming language and then using Google tools convert their resulting Java programs to run on proprietary Dalvik platform on Android devices. Once converted, such an app can run on any Android device [9]. Many security applications have seen the light of the day in a move to improve the workability and efficiency of most Android phones security-wise. For instance, [10] developed a Semantically-Rich Application-Centric Security in Android; a Secure Application INTeraction (popularly known as "Saint") which is a modified infrastructure that governs install-time permission assignment and their run-time. This was seen to be very effective in the sense that it provides necessary utility for applications to assert and control the security decisions on the platform. In [11], a programmable Interface for extending Androids security which was based on a framework known as Android Security Modules (ASM) was developed by studying the authorization hook requirements of recent security enhancement proposal. The application provides a programmable interface for defining new reference monitors for Android. Also, a technique for differentiating malicious and benign mobile App behaviour using context was proposed in [12] as a security measure to tackle the effect of malware on mobile App such as Android. This brought about an AppContext of a static program analysis that extracts the contexts of security-sensitive behaviours that assists App analysis in differentiating between malicious and benign behaviour. It was thereby observed that the maliciousness of a security-sensitive behaviour is more closely related to the intention of the behaviour than the type of the resources accessed. Recent research [13] centered on guaranteeing secrecy in smartphones operating systems such as Android OS. A technique made up of context-sensitive DIFC enforcement via lazy polyinstantiation and practical and secure network export through domain declassification was introduced in this regard. This brought about a practical and secure DIFC enforcement on Android. However, mobile phone users can potentially have their geographical location and movements traced at any time or all the time. In addition, a log of all data generated by a mobile phone is stored by the mobile phone service provider and potentially shared based on legal framework relevant to mobile phone location data. This makes the mobile phone unique in comparison to other location identifying technologies, such as CCTV or RIFD, particularly as a mobile phones tends to be carried by one person on a regular or sometimes even continuous basis. CCTV for instance, can track individuals in real time but never continuously, RFID tags can also reveal location information but tends not to do this in real-time or on a constant basis. WiFi (Wireless Fidelity) networks can also be used to locate the positions of devices that share links with wireless network. However, this is limited to the size and the geographical area covered by this network. Whatever the form of evolvement of current technology, privacy is also an important issue that needs proper address in security systems. The difficulty of defining the concept of privacy is often used as an introduction to reviews of security privacy. Understanding privacy as an interest individuals have in leading a life free from inference by others. Despite this apparent slipperiness of the notion of privacy, numerous scholars have not ceased to provide their thoughts on this subject over the last several decades: such as regarding the impact of technologies on privacy [14]. Whatever the case, applications involving face images seem of more relevance today for some forms of identification owing to the fact that the human face as we all know, is used for expression, appearance and identity purpose among others [15].

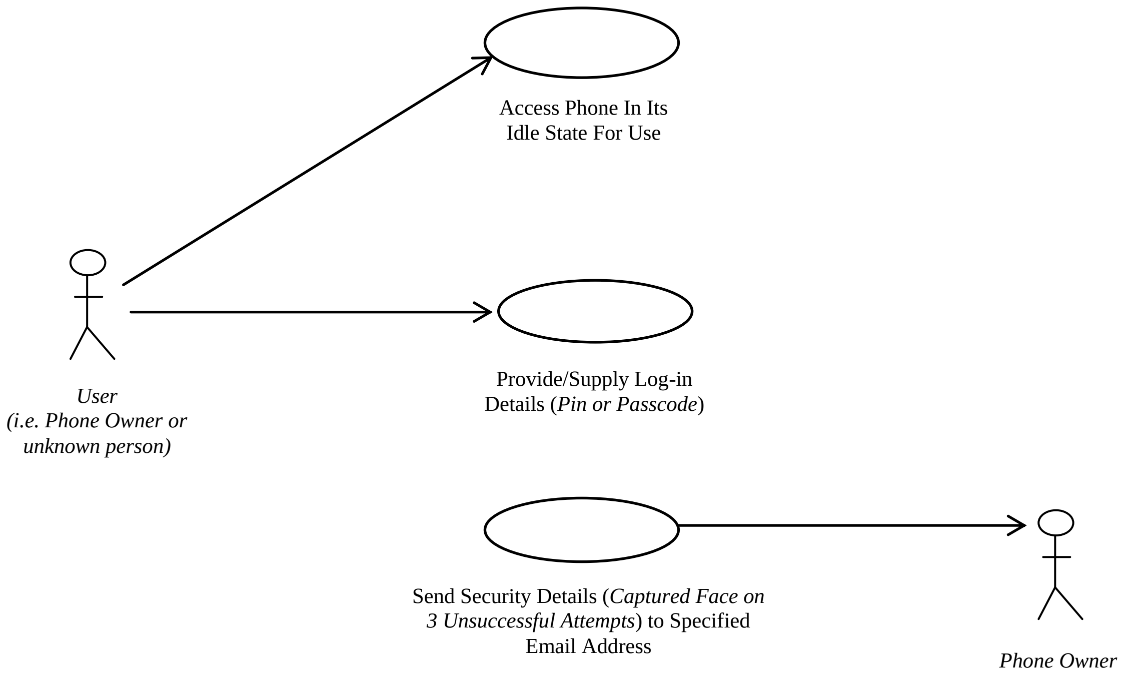
3. METHODOLOGY

The detailed parameters employed in the configurations of Android phones were identified and analyzed accordingly in terms of functions and efficiency as regards to their security measures. A unit of functionality provided by the system was demonstrated with the aid of a Use-Case diagram and the procedural flow of control between the various class objects involved was illustrated using the Activity diagram. The various elements in this were properly considered in the development of the required program for running the needed security functions on mobile phones (Androids). The code was created using JAVA programming language. Since the code is designed to be implemented on mobile phones, a Universal Serial Bus (USB) was used to facilitate its transfer from the computer system on to a mobile phone for implementation.

4. DETAILS OF THE DESIGN

The program was developed on a platform called "Android Visual Studio" which allows the development of applications to be run solely on phones with Android Operating Systems. The required tools such as Interface, Location Settings (Mode) and the Texts were built with the aid of the Android In-built Controls; which generates its own codes when utilized thus providing the needed field for entering E-mail and some other required parameters. Other aspects of the program design include the sending of data captured (i.e. pictures, location, date&time) to E-mail, Reading of the Cache memory and the ability to activate the phone's front camera for automatically capturing user's face when malicious act is been detected. With the aid of the touchscreen, data input to the system was made possible giving room for entering the pre-conceived password or pin. Also, an activity screen for face capturing is provided for face unlock; which was also incorporated with a voice application for recording the user's voice for the unlocking process. Lastly, the design made use of a nine-dot screen for drawing needed pattern for either locking the phone and at the same time unlocking it where necessary. Meanwhile, the program, following the system specifications were coded and developed using JAVA and XML codes on Android Studio package and Eclipse.

The system model is thereby represented in forms of the Use-Case Diagram (Fig.1) and the Activity diagram (Fig.2). The Use-Case diagram presents makes us understand that the system lets the phone user *(i.e. a particular person holding the phone at the moment with the intension to use it)* access the phone idle state and supply the expected security code (i.e. log in information which could be either *pin* or *password*). In connection with this, there is provision for an alert system which comes in form of reporting the existence of incorrect log-in info. In this case, the system makes it possible for the sending of the said user's details *(captured face)* to a designated email for awareness and to take necessary measures as regards to the person attempting to use the phone. The Activity diagram makes us see the various instances of log-in info *(PIN/Password)* validation and the results/consequences in each case in addition to the scenarios highlighted in the case diagram. For instance, the said security alert gets activated whenever the log-in info *(PIN/Password)* is incorrect but the user gets the full access to the phone when the log-in info is correct. Meanwhile, the logic behind the entire system performance is highlighted in the form of a flowchart as shown in figure 3.


Access Phone In Its Idle State For Use
Provide/Supply Log-in Details (*Pin or Passcode*)
User (i.e. Phone Owner or unknown person)
Send Security Details (*Captured Face on 3 Unsuccessful Attempts*) to Specified Email Address
Phone Owner

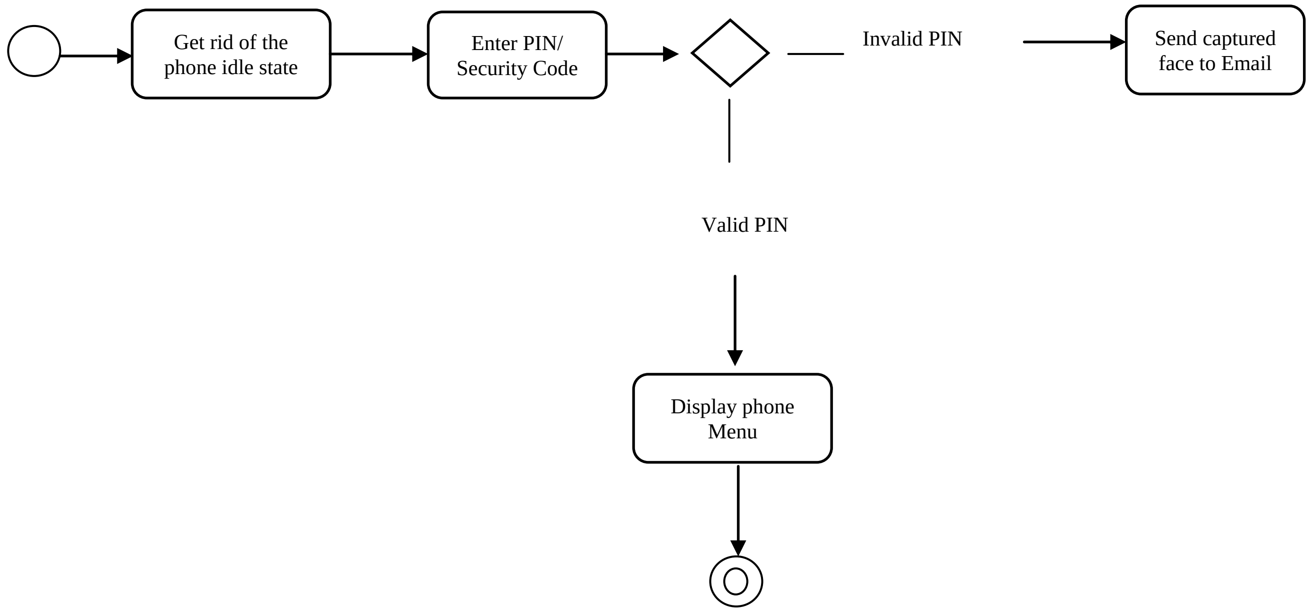


Figure 2: Activity Diagram

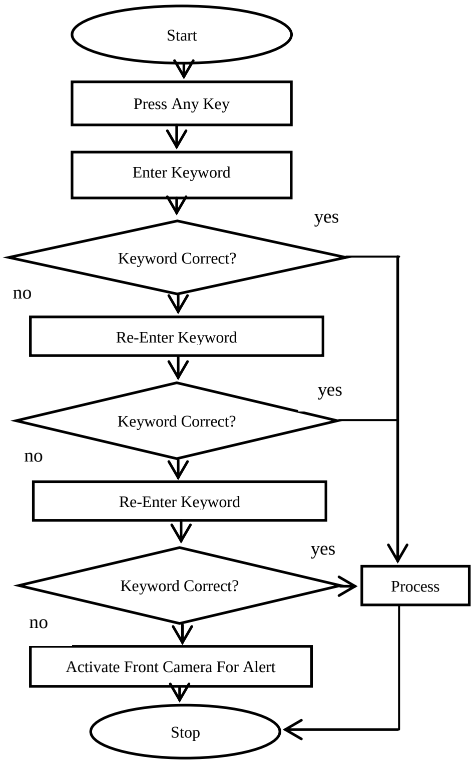


Figure 3: System Test Logic

4.1 Input Design and Specification

Security system is designed in such a way that sometimes it is called GIGO – denoting that what Goes In Goes Out. The input specifications are designed generally based on the necessary data that needs to be entered into the application. The data are captured through the mobile phone's touchscreen keyboard and the front camera and stored in the phone's integrated database which is known as SQLite.

4.2 Output Design and Specification

The output was based on inputs. The result generated gives a meaningful output to the user. The system designed generated the following results.

1. Face captured when wrong password is typed in specific times
2. Provides number of unlock attempts before capturing.
3. Phone location also automatically stored when this happens.
4. Sending of Email of the inputs generated *(picture and location)* due to the wrong attempt is activated.
5. However, some of the parameters of interest that could be considered as areas of significance in this study include the following;

- **Exposure** - It eliminates the consistent loss of mobile phone by exposing intruders with the information about him/her (face and location) sent to the provided email.
- **Assurance** - This study saves one the stress of or fear losing his/her phone adding more to the beauty and confidence of phone usage.

5. SYSTEM IMPLEMENTATION AND EVALUATION

The data gathered were processed into a more meaningful format for entry into the system. The following parameters; the voice, password, pin, captured pictures, and pattern were processed using the SQLite database built solely for mobile applications. The output of the system is generated from the processed data, it is been derived from the mobile database where it's been stored. For instance, when an initial password is been set to lock a phone, it automatically save into the database, to unlock the phone the pre-conceived password is required to be type anything contrary would introduce "wrong password" string.

The implementation of the program was possible through the design and coding which produced an error free result output. The design concept of the system initially started with the design of the interface, labeling and naming of the activities before the important aspect which is the coding. The on-screen interface was firstly coded to totally lock down the phone screen and keys excluding the volume keys, for it to strictly stick on the notification panel which cannot be discarded. The concluding functions of the system were coded a little bit different from the initial on-screen interface.

5.1 The Workings of the New System (Procedural Steps)

Stage 1: Launching the code

Launching the developed code takes the user to the phone's security settings (As shown in figure 4). This shouldn't be a problem because most android phones share the same form of tools on them. Some of the options available here include the following;

Swipe

Face unlock

Face and voice

Pattern

Pin

Password

None

Then, select *"Password"* to lock the phone and enter your desired password twice; i.e. the first is for *the main password* section while the second is for *confirmation*. Hence select *"ok"* to get back to the screen's security.

i. Press or Hit *"back"* on your phone to go back to the application
ii. Click on *"turn on high accuracy location mode for best results" t*o get to the location mode
iii. Turn on the "*location mode"*. Also press *"back"* to get back to the application.
iv. Select *"Send alert email"* to get to the device administrator where the activation of the code for security execution on your phone shall be done.
v. Click on *"activate"* to activate the code. On completion of the listed steps, the phone's setup will automatically display a form a report saying *"the application has been successfully activated"*.
vi. The next thing is to specify the exact number of password attempts before the phone's front

camera starts capturing; to do that; Select *"Number of unlock attempts"*.

An example of a maximum of *three attempts specification* should give us the following display;

1 attempt
2 attempts
3 attempts

This determines the number of wrong password entered before the application prompts the phone's front camera to capture the face of the user in question. This last step listens to the phone's cache memory to search for the owner's email address if available, if not it provides a field for it to be entered.

vii. Click on the *"email should be sent to"* to enter your personal E-mail and then select *"ok"* and finally close the application and allow the screen to either dim-off or be in idle mode.

Stage 2: Testing the codes;

First, get rid of the phone's idle state

viii. Key in your phone security keywords *(password, pin etc.)*, i.e. the security parameters employed by the user while locking the phone.

Condition;

- If the entered keyword *(password, pin etc.)* is correct, then the phone opens smoothly giving the user the room to proceed with using it.
- Else, if the entered keywords *(password, pin etc.)* is incorrect (i.e. user attempts entering a wrong password), then the user's details *(i.e. face as well as location)* shall be automatically sent to the E-mail set while configuring the system. The various scenarios in this system are shown in figures 5 and 6.

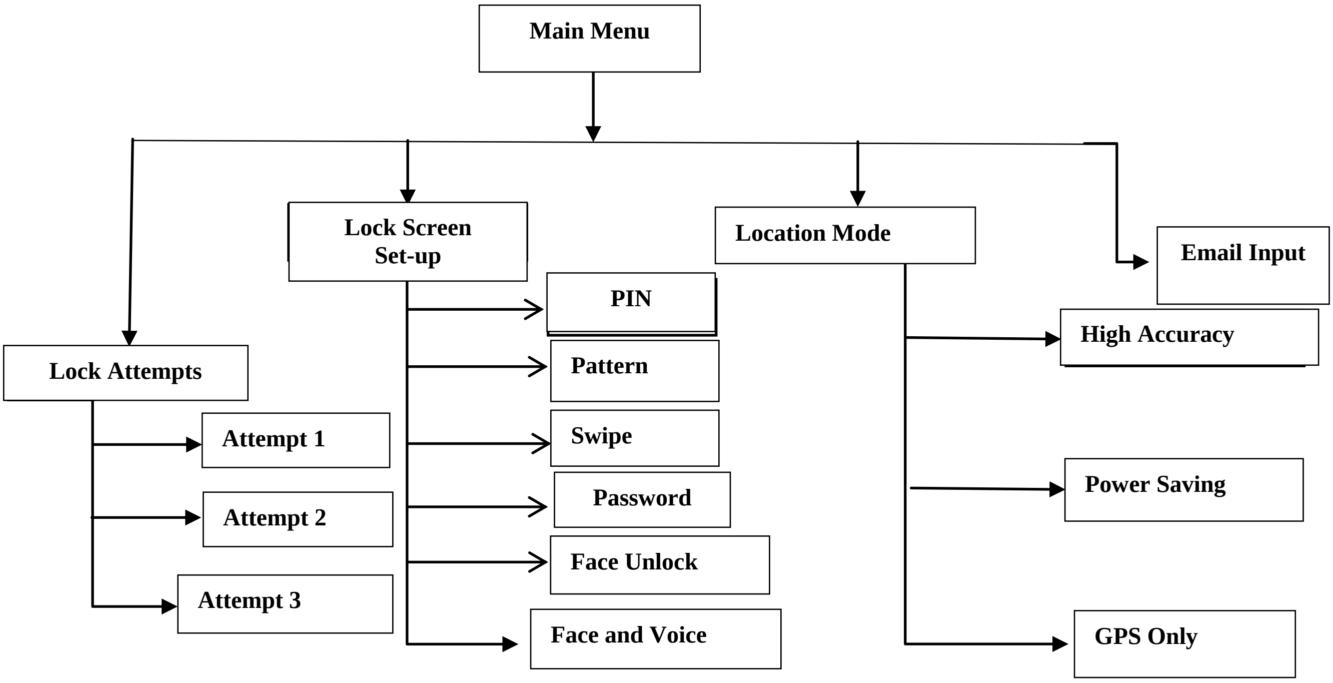
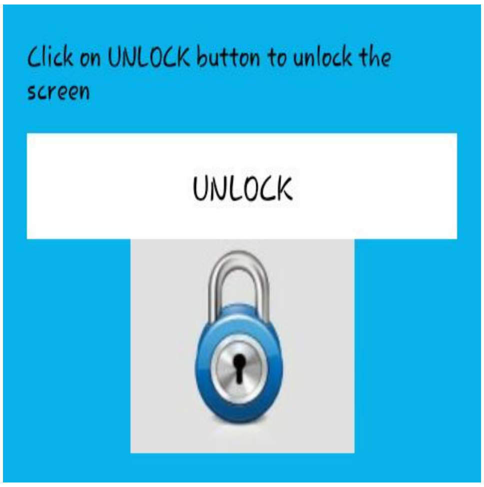
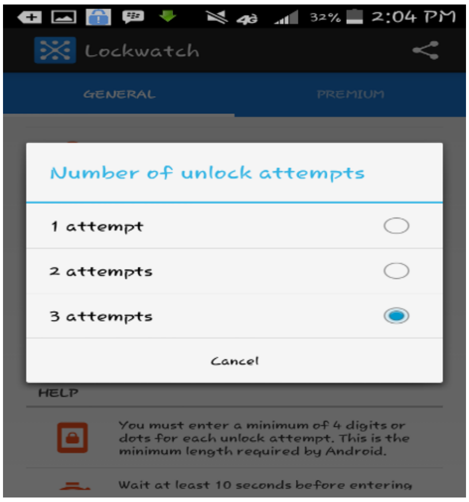


Figure 4: Procedure Chart


Click on UNLOCK button to unlock the screen

UNLOCK

Figure 5: Lock Screen Interface


2:04 PM

Lockwatch

GENERAL PREMIUM

Number of unlock attempts

1 attempt ○
2 attempts ○
3 attempts ●

Cancel

HELP

You must enter a minimum of 4 digits or dots for each unlock attempt. This is the minimum length required by Android.

Wait at least 10 seconds before entering

Figure 6: Unlock Attempt Interface

6. DISCUSSION

The scope of this study is limited to the development of security system for mobile phone in Android platform. The actual area of interest in terms of limitation is that the system is simply set to forward what has been captured *(user's face)* while attempting to enter the security keywords but not to actually process and identify the captured image as to whether it is a face or not. Meanwhile, it is expected that a user *(phone owner or intruder)* is to have his/her face facing the phone's screen while attempting to perform the expected function required to prompt for any security measures. At any rate, the system here is programmed to work in a secured mode; meaning that the intruder whose face is to be captured is likely not to have a prior knowledge of its existence before embarking on its usage. A person's mobile phone represents his/her secret life info which are to be well secured; thus making the security of the phone paramount in all ramifications. It is recommended that a phone user is expected to have it in mind that his/her phone is owned by him/her and nobody else. Therefore, no one, unless of course you give permission of free access, is to access it for any reason(s). Also, your phone is your life style in soft form, so your lifestyle should be kept discreet, confidential, private and protected; especially for efficient functionality of security-related application of such phones.

7. CONCLUSION

This research work does guarantee safe usage of one's personal phone in terms of privacy in addition to exposing true identities of intruders, who give themselves access to operate and explore someone else's private life through their mobile phones. It also educates the masses with the basic knowledge of privacy, protection from unauthorized access and the core importance of mobile phones security. For efficiency sake, several observations were carried out on the existing security functions of mobile security with a view to study the shortcomings and make necessary improvement when implementing the current system to eliminate the disadvantages. Unlike other methods, searching through the cache memory at installation to collect user's registered mail address (if any) is made possible in this system thus saving the user some stress instead of entering the email address. The design here made it possible for an intruder's face to be captured and referenced for detection and possible recognition in case of intrusion and theft.

8. REFERENCES

[1] A. Elfasakhany, J. Hernandez, C. Garcia, M. Reyes and F. Martell, "Design And Implementation Of A House-Mobile Security System", Scientific Research. *http:// www.SciRP.org/journal/eng* (2011).

[2] C. Franklin, "6 Top Programming Languages ForMobile Development", InformationWeek, Interop.Las Vegas, (2015).

[3] C. Franklin, "9 Java Programming Myths Busted"InformationWeek, Interop, Las Vegas, (2016).

[4] Brewis. "How To Secure Android: 14 Tips For Securing Your Android Phone or Tablet",www.pcadvisor.co.uk, *(2016).*

[5] L. Peruso, K. Michael and M. Michael , "Location-Based Services and The Privacy-SecuritymDichotomy", School of Information Technology and computer Science Faulty of Informatics,University of Wollongong, Northfields Avenue,Wollongong, NSW, 2500, Australia, 2006).

[6] G. Anjaneyulu, M. Gayathri and G. Gopinath, "Analysis of Advanced Issues In Mobile Security In Android Operating Systems "Archives Of Applied Science Research 7(2), India, (2015).

[7] G. David, "Research Reveals That Android is Least Secure Mobile Phone Operating System",*www.Ibtimes.co.uk,* (2012).

[8] J. Bangali and A. Shaligram, "Design and Implementation of Security Systems For Smart Home Based On GSM Technology" International Journal Of Smart Home. Vol 7, No, 6, (2013).

[9] N. Carey, "A Window Into Mobile Device Security", Symantec Security Response, USA, (2011).

[10] M. Ontang, S. McLaughlin, W. Enck and P.McDaniel, "Semantically Rich Application-Centric Security In Android" Security and Communication Network, Volume 5, Issue 6 Pages 658-678, (2012).

[11] S. Heuser, W. Enck, A. Nadkami and A. Sadeghi,"ASM: A Programmable Interface For Extending Android Security", In *Proceedings of the 23rd USENIX Security Symposium*. San Diego, CA , USA, (2014).

[12] W. Yang, X. Xiao, B. Andow, S. Li, T. Xin and W Enck, "AppContext: Differentiating Malicious and Benign Mobile App Behaviours Using Contex", International Conference on Software Engineering, Austin, TX, (2015)

[13] A. Nadkarni, B. Andow, W. Enck and S. Jha, "Practical DIFC Enforcement on Android", In Proceeding of the 25th USENIX Symposium, Austin, TX, USA, (2016)

[14] F. Ben and E. Kathering, "The Right Of Privacy In Florida In The Of Technology And The Twenty-First Century: ANeed For Protection From Private And Commercial Intrusion", Florida State University Law Review. Vol. 25:25, (1997).

[15] A. Alabi, "A Modified Principal ComponentAnalysis Technique For Recognizing African Bust" The International Journal Of Engineering And Science, Volume (2), Issue (9), Pages (116-129) SSN (e): 2319 – 1813ISSN (p): 2319 –1805 , (2013)