Design and Evaluation of accelerometer based user authentication methods

by

Priyanka Bhide

LiTH-ISY-EX—17/5020-- SE

Supervisor: Andreas Ehliar, Biträdande universitetslektor (Assistant Professor)

Department of Electrical Engineering, Linköping University

Examiner: Jan-Åke Larsson, Universitetslektor (Associate Professor)

Department of Electrical Engineering, Linköping University
Abstract

Smartphones’ usages are growing rapidly. Smart phone usages are not limited to the receiving/calling or SMSing anymore. People use smartphone for online shopping, searching various information in the web, bank transactions, games, different applications for different usages etc. Anything is possible by just having a smartphone and the internet. The more usages of the smartphone also increase keeping more secret information about the user in the phone. The popularity is increasing and so is different ways to steal/hack the phones. There are many areas which require further investigation in the field of smartphone security and authentication.

This thesis work evaluates the scope of different inbuilt sensors in smartphones for mobile authentication based techniques. The Android Operating system was used in the implementation phase. Android OS has many open source library and Services which have been used for the sensor identification using Java Android platform.

Two applications using Accelerometer sensor and one using Magnetometer sensor were developed. Two foremost objectives of this thesis work were- 1) To figure it out the possibilities of sensor based authentication technique. 2) To check the end user perception/opinion about the applications.

Usability testing was conducted to gather the user’s assessments/vision of the applications. Two methods which were used for usability testing are named Magical move and Tapping. Users (Most of them) have shown interest and inclination towards tapping application. Although, some users were also expressed inhibitions using both sensor based methods.
Preface

This master thesis report is carried out in the field of mobile security. This is the result of last stage of my education of becoming an engineer in computer science. This thesis was executed at Linköping University Valla Campus in the department of Electrical Engineering (ISY) division.

Linköping, Sweden, December 2015

Priyanka Bhide
**Title:** "Design and Evaluation of accelerometer based user authentication methods".

**Table of Contents**

Acknowledgement ....................................................................................................................... 8

1. Introduction .................................................................................................................................. 9
    1.1 Goals of the Thesis .................................................................................................................. 11
    1.2 Tools used and delimitation ................................................................................................... 11
    1.3 Research Question .................................................................................................................. 12

2. Background ................................................................................................................................... 13
    2.1 Android Framework ............................................................................................................... 13
    2.2 Android Sensors Types ......................................................................................................... 14
    2.3 Previous Works ..................................................................................................................... 19
    2.4 Different Authentication Methods ......................................................................................... 22
    2.5 Security Threats ..................................................................................................................... 23

3. Methodology and Application Development ............................................................................. 24
    3.1 Methodology ......................................................................................................................... 24
    3.2 Application Development ..................................................................................................... 24
    3.3 Obstacles faced ..................................................................................................................... 30

4. Usability Evaluation .................................................................................................................... 31
    4.1 Goals of Usability Testing ...................................................................................................... 31
    4.2 participants and duration ....................................................................................................... 32
    4.3 Result Analysis and Interpretation ........................................................................................ 32

5. Survey Results ........................................................................................................................... 32

6. Discussion and Conclusion .......................................................................................................... 36

7. Bibliography / References ......................................................................................................... 38
List of Figures:

Figure 1.1 A picture showing the shoulder Surfing
Figure 1.2 A picture showing of smudge attack
Figure 2.1 A picture is derived from Android Framework
Figure 2.1 Sensor Coordinate system of accelerometer sensor
Figure 2.3 Magnetometer Compass showing the directions.
Figure 2.4 A picture of partial shoulder surfing safe technique
Figure 2.5 A picture of pattern recognition using grids.
Figure 2.6 A picture of Hybrid PIN entry method.
Figure 3.1 A picture of different stages of the workflow
Figure 3.2 A picture of methodology used during application development.
Figure 3.3 A picture of the first application.
Figure 3.4 A picture of the second application.
Figure 3.5 A screenshot showing the PIN entry using magnetometer.
Figure 5.1- Showing the test result in a pie chart
Figure 5.2- Showing the testing result in a pie chart.
Figure 6.1- Showing the Two way authentication.

List of Tables:

Table 2.1- A table of Android Sensors Description.
Table 2.2 A table showing the return values of coordinates.

APPENDIX A. Accelerometer detection
APPENDIX B. Magnetometer detection
APPENDIX C. Tap detection and Vibration detection
APPENDIX D. Magnetometer values detection
Acknowledgement

This thesis would not have been completed without the direction and support of several individuals who have contributed their valuable thoughts, guidance and encouragement to complete the work.

First and foremost, my gratitude to Prof. Jan Åke Larsson, who has been encouraging and inspiring throughout my thesis time. He has been examining my work regularly and guided me towards the right direction. He has also given some useful inputs of various standards and guidelines that need to be followed. Assistant Professor Andreas Ehliar, who has been supervising the progress. He has given his key inputs and some positive ideas to overcome my hurdles during implementation phase.

My husband Ameya Bhide for the encouragement and support ever since he came into my life. My beloved parents (aai and baba), for all the love, blessings and moral support through thick and thins and strength right from my childhood. My brother Prateek for his love. My In-laws for all the support. My close friends in Linköping for advising me. Last but not the least my beautiful daughter Tanaya for giving priceless moments of happiness, love and smiles. A special thanks to Naga Umapathi Rao for his advice and backing during my thesis work. Also, to my friend Seror Shubbar for the time we shared during my masters in Linkoping university.

Every milestone I have accomplished so far personally and professionally wouldn’t be so special without all of them.

Linköping, August 2015
Priyanka Bhide
1. Introduction

This chapter provides a brief introduction to the thesis, outline of the work, research questions and delimitations.

Standard old phones were used only for limited usages in older days. They had no Wi-Fi connections or primitive Operating systems or any other smart features. Smartphones on the other hand are extremely popular and in demand nowadays [30]. They are easy to handle and intuitive compared with Standard old phones for end users. Approximately 2 billion people are using smartphones all over the world and that explains the popularity of these phones [31] [32].

Standard phones are more secure since it has no application and hence less outbreak prospects compared to a smartphone. Smartphones have more security issues. Each person who owns a smartphone tries to use one or many smart features such as using internet for reading mails, bank transaction, online purchasing etc. An easier way to remember all the passwords or PIN numbers is to store them in the phone. Nowadays, smartphone users store many secrete credentials such as passwords, bank account numbers and pin codes in the phone. These are useful for instant logging in to their bank accounts, for online purchasing, for bill payments, checking emails etc. This gives more attention and motivation for the stealers to steal the phone. They can not only get the smart phone but also get secrete information of that user like credit card details and this can lead into more crimes.

An observer just need to stand next to the person before stealing the phone. He/she can easily peep over when the user is typing his/her password. People are generally careless while typing their password/pin code or drawing a pattern on public forums [25]. This scenario of getting and knowing the information is called shoulder surfing [2]. Shoulder surfing and record monitoring are two techniques where an attacker/observer can get the passwords or PINs by just looking over the shoulder of a user. Record monitoring is performed through concealed cameras but this technique has not been investigated further in this thesis work.
There are other ways to observe the password if there is no possibility to stand next to the person. An attacker can just carefully observe user’s fingerprints on the screen [26]. This is called smudge attacks. There are mainly two popular ways user can lock the phone- By typing four-digit pin code or drawing a pattern. The stolen phone can be carefully observed by an attacker. For pin entry unlocking, attacker can try all permutations for 4 pins. This will eventually unlock the phone. Similarly, for drawing pattern an attacker can guess it by repeating the pattern in different directions and manner. Above two are general security threats for the smart phone users. According to the source [33] typing a PIN is more secure than drawing a pattern but it is still not very tough to guess or observe.
1.1 Goals of the Thesis

First of all, the intention was to check whether it is possible to make authentication methods using different in-built smartphone sensors. Background study of these sensors took handful of time because of the lack of knowledge in the area of smartphone sensors and the technique these sensors work. The objective of this thesis was also to investigate some different techniques and approaches to reduce the fingerprint observation attacks on smartphones. Furthermore, to investigate the usability of the newly made sensor based methods in comparison with popular authentication methods. This study opens up new research ideas from the users’ liking and disliking towards the methods.

1.2 Tools used and delimitation

The following tools are used while Designing and implementation of three sensor based Android applications. These tools have been selected after the background study of tools used in different research papers, online materials, web information and different applications available online.

Development Tool used- Eclipse IDE, version- Luna
Implemented on- Android based smartphones,
Tested on- Nexus 5 and Samsung S4.
Sensors used- Magnetometer, Accelerometer
Supported tools- Android-SDK using Java SE
Usability testing tools- Google forms (Task based approach)
Android versions- 4.9 to 5.1
Analysis tools- adb Logcat shell command
Emulator has also been used in the initial phase before the real testing was conducted. Most of the testing is done through task based usability testing approach. More information will be available in section 4 ‘Usability evaluation and Results’. To understand first and implementation later in Java Android using eclipse tool were not tranquil and that took time more than expected. Only a handful of work has been done in the related area hence collecting information also took some extra time.

“Sensor Manager” public class has been used to access the sensors which is an Android hardware abstract class hence it puts a limitation that these applications cannot be used on any other Operating System. Author is also not sure whether these applications can work on old versions of Android OS as many new classes and packages have been introducing every now and then. Building two successful applications and one unsuccessful application and setting up all the environment was time consuming and maximum efforts was applied in learning Java Android and developing the methods.

**Delimitation**
Some improvements are still needed to be able to make the applications more stable, reliable and professional. Additionally, we have not tested any age group other than 18-35. Testing was only done on Nexus 5 Mobile phone by different users and no other mobile has been used for Usability testing.

**1.3 Research Question**
The research questions highlight overall objectives of the thesis work and represent the relationships between theories and concept and the approach. These research questions will also sum up the significant issues about the research. The following questions are answered in various chapters of the thesis report.

1. **What is the reason behind the developed methods?** The elaborated answer to this question is described in the Chapter 1.1 ‘Goals of thesis’.
2. **How many sensors are available for developing these Applications?** The elaborated answer to this question is described in the Chapter 2.2 ‘Sensor Types’.
3. **Which security types can be trusted in this Applications?** The elaborated answer to this question is described in the Chapters 5 and 6.
4. **Which is the best method that we can rely on according to survey?** The elaborated answer to this question is described in the Chapter 4.3 ‘Result Analysis and Interpretation’.
2. Background

This section gives background of Android framework, different sensor types and sensor description which are used in this thesis for developing the applications. Furthermore, this will describe a short summary of similar earlier work and advantages and disadvantages of each technique.

2.1 Android Framework

The thesis implementation is based on Android operating system for mobile device. Android is the most used mobile operating system in the world, has more users, more phones and more tablets worldwide than any other mobile operating system. Apart from popularity of the phones, open source code is available for everyone for free to use. The below figure is the description of Android framework.

![Android Framework](image)

*Figure 2.1 A picture is derived from Android Framework [37].*

As it illustrated in Figure 2.1, the bottom layer is a customized embedded Linux system which interacts with the phone hardware and contains hardware drivers of camera, keypad etc. The next level is for all the libraries set such as SQLite database, Web browser webkit, etc. Above this is a set of Java based libraries. In the same layer one section is reserved for Android Runtime which provides a component called DVM. DVM enables each Android application to run on its own process and instance. It also provides some libraries which allows developers to write code using Java language. Second last layer or the layer second from the top is Application framework which gives high level Java class services to applications such as Activity manager, Resource manager, Notification manager, Content provider. More information about these services can be found in Android Interfaces and Architecture open source material. The
top most layer is Android Application layer. All the applications are written to install in this layer. e.g., phone dialer, address book etc.

2.2 Android Sensors Types

Most of the modern smartphones devices are equipped with a variety of sensors like accelerometer, gyroscope, magnetometer, gravity, light, GPS, etc. A sensor is a converter that could measures a physical quantity and converts it into a signal which can be read by a user or an instrument. It could be hardware-based sensor which is a physical component built into the device and it obtains its data by directly measuring specific properties like Accelerometer or Gyroscope sensors. Gyro sensor mainly detects the earth’s gravity and based on that one can determine phone’s orientation. This is a free rotating disc which is mounted on the spinning wheel. It could also be a software-based sensor sometime called virtual sensor and it obtains the data from one or more hardware-based sensors such as gravity sensor.

Android platforms support mainly three different sensors [34]-

a) **Motion sensors**- Motion sensors are primarily used to monitor the motion of the device. These sensors can be hardware based or software based. Hardware based sensors are gyroscope and accelerometer sensor. On the other hand, gravity, linear acceleration and rotation vector sensors can be either hardware based or software based sensors. Motion sensors are very useful for detecting the shaking, rotation, swing and tilting movements. Motion sensors are generally used with some other type of sensors such as position sensors to show the relative position frame of reference.

b) **Position sensors**- Position sensors are primarily used for determining device’s physical position. There are two types of sensors- geomagnetic field sensor and orientation sensors. The geomagnetic sensor is a hardware based sensor while orientation sensor is a software based sensor and it derives its data from hardware based sensors such as geomagnetic sensor and accelerometer sensor.

c) **Environment sensors**- Environment sensors are hardware based sensors and these are not available in all the devices. These are mainly of four types- ambient humidity, illumininance, ambient pressure and ambient temperature. These sensors are used to measure the environmental pressure, humidity, air temperature etc. These sensors are not used in this thesis hence not very elaborative description has given for this type of sensors.
The above description will provide the information to the programmer about the sensor framework like what type of sensor a particular device has, how powerful it is (range, power requirement and rate of which the data comes). ‘Sensor Manager’, ‘Sensor’, ‘Sensor Event’ and ‘SensorEventListener’ are some of the classes which are being used during the implementation of the applications. More information about these sensor classes can be found here [20].

Motion sensors and Position sensors both are used during the development. The below table has shown Position sensors and Motion sensors description which are used to develop the applications.

This table’s contents are derived from the open source Android developer guide. [28]

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Type</th>
<th>Description</th>
<th>Common Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE ACCELEROMETER</td>
<td>Hardware</td>
<td>Measures the acceleration force in m/s·that is applied to a device on all three physical axes (x, y, and z), including the force of gravity.</td>
<td>Motion detection (shake, tilt, etc.).</td>
</tr>
<tr>
<td>TYPE GRAVITY</td>
<td>Software or Hardware</td>
<td>Measures the force of gravity in m/s·that is applied to a device on all three physical axes (x, y, z).</td>
<td>Motion detection (shake, tilt, etc.).</td>
</tr>
<tr>
<td>TYPE_GYROSCOPE</td>
<td>Hardware</td>
<td>Measures a device's rate of rotation in rad/s around each of the three physical axes (x, y, and z).</td>
<td>Rotation detection (spin, turn, etc.).</td>
</tr>
<tr>
<td>TYPE_LINEAR ACCELERATION</td>
<td>Software or Hardware</td>
<td>Measures the acceleration force in m/s·that is applied to a device on all three physical axes (x, y, and z), excluding the force of gravity.</td>
<td>Monitoring acceleration along a single axis.</td>
</tr>
<tr>
<td>TYPE_MAGNETIC_FIELD</td>
<td>Hardware</td>
<td>Measures the ambient geomagnetic field for all three physical axes (x, y, z) in μT.</td>
<td>Creating a compass.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Type</td>
<td>Description</td>
<td>Common Uses</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>TYPE_ORIENTATION</td>
<td>Software</td>
<td>Measures degrees of rotation that a device makes around all three physical axes (x, y, z). As of API level 3 you can obtain the inclination matrix and rotation matrix for a device by using the gravity sensor and the geomagnetic field sensor in conjunction with the getRotationMatrix() method.</td>
<td>Determining device position.</td>
</tr>
<tr>
<td>TYPE_ORIENTATION</td>
<td>Software or Hardware</td>
<td>Measures the orientation of a device by providing the three elements of the device's rotation vector.</td>
<td>Motion detection and rotation detection.</td>
</tr>
</tbody>
</table>

Table 2.1- A table of Android Sensors Description.

Accelerometer Sensor: The accelerometer is one of the hardware sensors provided from Android platform in the category of motion sensors. The hardware sensor is based on sensor motion and it lets the user monitor the motion of the device. It measures how quickly the speed of the device is changing in a given direction. It also monitors the device movement, such as tilt, shake, rotation, or swing and checks the velocity of the device which is moving in a particular direction. The movements are usually linear movements in three dimensions for example- side-to side, forward-and-back, and up-and-down. The figure is derived from [35] source.
This orientation is measured in all three (x, y and z) axes like it is pictured in above figure. While Accelerometer measures linear acceleration of movement, Gyroscope sensor measures the angular rotational velocity in degrees per second. Accelerometers are sensitive to the linear acceleration of the sensor and the local gravitational field. The values are always shown as positive x, y and z in the log data. The linear acceleration is always aligned in the same direction of these axis and gives positive values of X, Y, Z axis. The gravitational field is also aligned in the same axes but shows the negative values of X, Y, Z axis [42]. These axes have been used to measure the static acceleration and find the angle at which device is tilted due to the gravity. Furthermore, it measures the dynamic acceleration to analyze the direction in which the device is moving [41].

The accelerometer can be measured in portrait or landscape mode in all three axes (X, Y, Z). Portrait mode setting is used in this thesis. When a device moves, the return values of (X, Y, Z) are translated into (0, 1, 2) respectively that defines specific angles as described in Table 2. The changes in acceleration along with these axis of the coordinate system measured in m/s². The method - public void onSensorChanged (SensorEvent event) notifies whenever there is any change in accelerometer values. The code snippet shown in APPENDIX detects the accelerometer in a device. This table showing the return values of different coordinates is derived from source [41].
<table>
<thead>
<tr>
<th>Constant Name</th>
<th>Index/value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROTATION_0</td>
<td>0</td>
</tr>
<tr>
<td>ROTATION_90</td>
<td>1</td>
</tr>
<tr>
<td>ROTATION_180</td>
<td>2</td>
</tr>
<tr>
<td>ROTATION_270</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 2.2 A table showing the return values of coordinates.

Magnetometer Sensor: Magnetometer sensor is one of the position sensors which is used to measure the direction of magnetic field stand-in in any device. A magnetometer is an instrument used to measure the strength and/or direction of the magnetic field in the surrounding area of the instrument. Magnetometer is surrounded often with another sensor like Accelerometer. Magnetometers can be divided into two basic types: Scalar magnetometer and Vector magnetometer. Scalar magnetometer measures the total strength of the magnetic field to which they are subjected. Vector magnetometer has the capability to measure the component of the magnetic field in a particular direction, relative to the spatial orientation of the device. Vector magnetometer has been used to develop one application in the thesis. Digital compass which is based on magnetometer sensor provides mobile devices with orientation in relation to the earth magnetic field, so the mobile phones always know where the Magnetic North is for example [37]. Magnetic north is different from Geographic north and the difference between them is called ‘Magnetic Inclination’. Code snippet shown in APPENDIX recognize in any device whether the magnetometer sensor is available or not.
2.3 Previous Works

A literature study [1—15] on various sensor based techniques was performed where the special stress was given on accelerometer and magnetometer based techniques. The pros and cons of existing techniques were analyzed. The other sensors besides Accelerometer and Magnetometer have also been studied to get the fundamental knowledge of other sensors like gyroscope sensor. However, to the best of author’s knowledge gyroscope has always been used with some other sensor type such as Accelerometer and Magnetometer for different mobile authentication methods. Most of the work has been done on accelerometer sensor.

Given below are some of the examples of mobile authentication solutions using various powerful techniques. These methods have provided many ideas for the development of this thesis work.

a. **Gesture based user authentication** [5,7]: The gesture based user authentication using a hand gesture is the objective of this thesis work as an alternative method to knowledge based authentication techniques. Using 3 dimensional Accelerometer and 3 dimensional gyroscope, user can choose one gesture which he/she will use it for authentication. Gestures only in terms of hand/arm movements have been used. Different algorithms of machine learning have been used to make the application such as DTW (Dynamic Time Warping), HMM (Hidden Markov Model) etc. Linear interpolation to normalize the sampling frequency. It needs more feasible and user friendly approach.

*Figure 2.3 Magnetometer Compass showing the directions.*
The algorithms used in the thesis are very complex and mathematical based. The algorithms need to be refined and further user studies for multiple dimensions’ mechanism are also required. The combination of both the sensors makes the hand movement measurements more precise. User doesn’t need to look at the device while performing the gesture and hence more useful for blind people.

b. **Partial shoulder surfing [10]** - Another technique for smartphone authentication was used by partially shoulder surfing safe method. This method has advanced security for especially human shoulder surfing safe methods. The numbers are displayed in two colors (white and black) on the screen. User needs to press either white or black key according to the color of the numbers displayed on the screen. This technique is easy and fast and takes around 8 seconds to complete the process. But according to the survey conducted for the analysis of the work shows that if the process takes more time it is easier to guess the password for an attacker. Below is the figure displaying the steps for the application-

![Figure 2.4 A picture of partial shoulder surfing safe technique](image)


c. **WYSWYE [3]** - WYSWYE stands for ‘What You See is What You Enter’. This idea was based on simple pattern identification which is an alternative solution for knowledge based authentication mechanism. This is a simple shoulder surfing based defense technique. User has to recognize N password in a MxM grid. There will be two different grids available- Challenge grid and Response grid. User needs to select rows of the N passwords and maps them to the response grid. Both the grids have different sizes so user first eliminates the extra grids. The following figure will present the concept of how the pattern identification is done using different size of grids.
Figure 2.5 A picture of pattern recognition using grids.

The technique is very simple to understand and easy to use. However, the whole process takes more time to perform compared to other techniques. Moreover, concentration can be lost by doing the repetitive process. In this method no sensors have been used but the reason for mentioning this work here is that the work has created different ideas for this thesis and it can also be implemented in the future work and can be really interesting to see the results.

d. **Hybrid method** [13]- This concept is very similar to digital lock method and the author has combined gesture based technique and PIN entry notion together. This is a hybrid technique combining tapping and four key gestures. This technique was mainly used to reduce smudge attacks on smartphones. The idea is that users are asked to input the randomly generated password through tapping and gestures. The password is generated using random numbers from 0 to 9, four arrow keys-up, down, left and right and a dot for tap. Below is a figure demonstrating the application.

The password contains Right arrow for number 4, a tap for the number 5, Right arrow for number 8 and a tap again for number 3. This is how the phone will be unlocked through this gesture based hybrid method. User needs to make a right gesture on number 4, then a tap on number 5 and the process continues until all the four PINs are successfully unlocked. This work has generated the idea to the author that tapping can be used using sensors in the phone.
Although this method was simple to look and use but was shown a higher error rate during testing. It was also confusing to perform the gestures and hard for users to memorize the randomly generated password.

There were many more authentication methods were found during the literature study phase like - Unlocking Smart Phone through Handshaking Biometrics [4], Gesture based User Authentication for Mobile Devices using Accelerometer and Gyroscope [5], Some thesis works [6],[7],[8] and some papers, presentations like [9][10][11][12][13][14][15] were also referred to get the idea

2.4 Different Authentication Methods

a) Two Factor Authentication: There are mainly three categories of credentials which can be used for identity verification in the system. something a user knows e.g.- password, something user has e.g.- passport and something user is like fingerprint. Combination of any of two authentication methods mentioned above is called Two Factor Authentication. Two Factor Authentication is a powerful way of preventing security attacks. Something a user is (fingerprints) and Something a user knows (Pin Codes/Passwords) can be used in the future work.
b) *Multi Factor Authentication*- Multi Factor Authentication is an extension of Two Factor Authentication. Using more than two authentication methods is called Multi Factor Authentication. Multi factor Authentication can be more expensive and time consuming hence this method is used only where the top secret security is essential.

c) *Certificate based Authentication*- Certificate based Authentication is based on Asymmetric cryptographic technique. This technique is very difficult to falsify. For more information about Asymmetric cryptographic technique please refer to [43].

d) *Risk based Authentication*- Risk based authentication is based on various levels of strictness for authentication in the system. This technique is also depending upon different users, locations etc. For example- While accessing the bank account from different geographic location system sometimes ask users more security questions than usual.

### 2.5 Security Threats

There are three types of components which are considered the base line of any security related area. Smart devices are prone to theft and whenever there are possibilities of an attack, one or more of the following three types of data breaching could be possible- Confidentiality, Availability and Integrity. A brief about these three components are-

- **Confidentiality**- It is an alternative word for Privacy. Prevention of sensitive information by unwanted people and making sure that the most desired person would get it. In this thesis work the most focus has been given on the Confidentiality factor.

- **Integrity**- Integrity contains the consistency or accuracy of the system/data. The data can be changed by only authorized people and redundancy should be available to restore it from any given point. For example- Version control, Access control are some of the examples.

- **Availability**- The availability is mainly focused on the hardware part of the system so the system is always available to use. Maintaining hardwares, system upgrades, OS etc. are some of the examples of it.

The methods presented in this thesis work has mainly concentrated on Confidentiality and Integrity components. The magic move and Tapping applications represent the Confidentiality in terms of Privacy. Only authentic user can set the number of taps or set the directions for Magic move. Similarly, in case of new changes in the applications or implementing new things can be possible only by authorized users.
3. Methodology and Application Development

This chapter describes the workflow of different stages, methodology used during thesis time, the applications development process and application description in detail. This also gives the solutions to the questions asked in section 2.

3.1 Methodology

Figure 3.1 shows an overview of the different stages of the basic workflow of the stages. As the figure shows the first stage started with reading previous similar works. The second phase or stage was to generate different ideas through prototyping and finalize the applications to be made. The third stage was to implement the applications. The fourth stage includes the testing of the applications and the fifth stage includes the result and future work of the applications.

![Figure 3.1 A picture of different stages of the workflow.](image)

3.2 Application Development

All the applications are developed using Java Android in Eclipse Luna IDE. All the applications are installable on Android platforms as (.apk) file package. The applications might not be supported on any other OS other than Android operating system. The methodology is used during the thesis
time is Agifall methodology. Agifall methodology is used when combining loose waterfall process in agile method to increase the speed and quality and decrease the cost (in this case- the time). The reason behind using Agifall methodology was to get the best from both Agile and Waterfall models. The continues development and improvement of the applications were going on until the final solutions were built. The requirements were gathered initially and the development and testing phases came in later stage of the development cycle. Below is the diagram of the work cycle using Agifall methodology in the figure 3.2 below.

Figure 3.2 A picture of methodology used during application development.

**Application description:** - Three applications have been implemented during the implementation phase. Two applications using accelerometer sensor and one using magnetometer sensor. However only two applications have been tested by the end users in testing phase. The brief about these applications are described below-

a) **Tapping**- The meaning of ‘Tap’ is to hit something gently and/or repeatedly. As described in the Section 2 that the sensor recognizes the movement by different gestures such as shaking, moving etc. The taps get registered through accelerometer sensor. The first screen shows the reading instructions of using the application. User needs to tap number of times behind/underneath the phone to register the tapping. After each tap user will get the ‘Toast’ on mobile screen that the tap is registered.

**Note** [ A ‘Toast’ is a simple popup message to give a feedback of a particular event. It disappears after a particular timeout.]

Users can choose (n) number of taps of their own choice. This is the secret shared between an authenticated user and the device. Users then need to remember the number of taps which they had used for authentication to unlock it in the next step. To unlock the phone, user has to tap it again on the back side of the device. Every time user taps behind the phone he/she will get the vibration indicating that the tap is now un-registered. To understand the process correctly there is a minimum of five seconds pause time between each tap. Registering and un-registering the tap should match the number of taps otherwise
the device will not be unlocked. If the user cannot perform the tapping in 30 seconds, then the process is reset and user has to start the tapping from the beginning.

Figure 3.3 A picture of the first application.

A small code snippet of the tap registration is described in the Appendix. The code describes that if the time between two tapping is greater or equal to two seconds then a toast is displayed and the last shake is updated. During the unlocking process the device also vibrates indicating the user an indication that the tap is unregistered even if he/she misses the Toast for some reason. If both the tap counts are equal, then using Android “Power Manager class” the device is unlocked.
b) **Magic Move**: Magic wave is the second application which was developed. This application has a novel concept of moving and unlocking the phone. This application has also used accelerometer sensor for the implementation part like the previous one. This concept is based on the orientation of the device. The accelerometer sensor recognizes the orientation in the phone. For example, there are six different orientations possible in the phone (Positive x, y and z and negative x, y and z). The concept is based on password entry method which is very popular in smartphones. In the password entry method, user needs to enter four different digits/symbols to unlock the phone. Similarly, in this application user position the phone in any of the given directions for four times instead of typing the password. The secret which is shared between an authenticated user and the phone is the orientation pattern. To register the number of orientations, user needs to move the phone four times in the user’s choice directions. User has the liberty to place the phone in the same or different directions of his/her own choice. User needs to hold the phone for three seconds to get it registered successfully and once it is registered a ‘Toast’ will appear that the registration is successful in a particular direction.

**Note**: [A ‘Toast’ is a simple popup message to give a feedback of a particular event. It disappears after a particular timeout.]
Figure 3.4 A picture of the second application.

The key point here is that user needs to remember the direction and consecutiveness of the all four orientations which have been used initially. In any circumstances user forgets the orientations then there will be 45 seconds of waiting time before user starts the process again. Phone will not be unlocked until the correct pattern of all the directions have not been completed.
c) **Application 3** - The third application was built using magnetometer sensor. The idea was to ask users to write 4 different PINs in the form of degrees such as 30 deg, 170, 90, 320 degrees in a ‘Textbox’. User needs to remember the degrees to open/unlock the phone. This is shown in a below picture.

![PIN entry using magnetometer](image.jpg)

*Figure 3.5 A screenshot showing the PIN entry using magnetometer.*

Move the phone and it checks the correct degrees and eventually unlocks the phone. However, this idea was not successful. There were many reasons that it failed to show the correct results. The detailed description will be given in the section 3.3. The fetching of magnetometer values is described in the source code in APPENDIX. This application was not included in the testing part as the application was not successfully developed.
### 3.3 Challenges faced

Accelerometer values- Getting the accelerometer range was tough as the accelerometer values range is dependent upon device. Every hardware sensor has different limitations. Saving the log data into a file- The log data when using eclipse depends on the size of the buffer and in the system which was used during the implementation could only save maximum two minutes of data. Every two minutes the new log data takes place and it automatically removes the previous one. Storing the log files from starting till the end was another hurdle faced. The testing needed at least 20 minutes of buffering of the logdata files.

Magnetometer sensor is in general very sensitive to any interference material. Materials like electric cables, steel furniture, magnetic objects or even a vehicle passing by can interfere the sensor. Calibration is another issue in magnetometer sensors. Sensor can actually stop working and user needs to calibrate the device again for the correct or accurate direction.

Magnetometer calibration- The magnetometer application was not successful as discussed in the previous chapter. The main cause behind that is the code used for getting Magnetometer sensor directions was giving false directions. So for example, The Z axis was always showing wrong values. It was always needed to be calibrated and that is not possible once the application is started. It also had serious jitter problems. The magnetometer sensor is very sensitive comparative to other sensors. Another issue which was faced is the speed. The magnetometer could not update the directions fast enough to match with user’s hand movement speed. The other concern was to remember the angles properly for example- 135, 78, 320 etc. As the degrees are not easy to remember, users tend to forget the numbers easily.

Above mentioned magnetometer obstructions’ reasons are not identified as there is not so much information in the form of source code is available on the net. This can be a hardware issue or driver issue or the source code problem. Due to time limitation and lack of knowledge the concentration moved towards getting the other two applications correct. The author believes that using magnetometer for authentication in smartphones can be a very good solution.
4. Usability Evaluation

This chapter discusses different user testing techniques and the extracted data analyzation results.

*Concept of usability:* - Usability testing is performed to test the applications. Usability meaning quality. The quality of the product should be good. There should not be frustration while using the software. The more frustration the less usability of the product/software is.

There are different techniques and methods to perform the usability of a system or product nowadays such as Ethnographic design, walkthroughs, paper prototypes, participatory design, heuristic evaluation, Usability Testing etc. The fundamental use of Usability Testing is evaluation and assessment of a system. The main goal of Usability Testing is to know that the product (in this case it is an application) is useful for the targeted users and is easy to use and learn. Usability Testing is cheap to perform and comparatively quick in comparison with other methods of usability.

*Different attributes of Usability:* There are four major attributes of usability.

**a. Usefulness** - Usefulness depicts how keen user is to use the product and achieving his/her goals while using the product. The Usefulness of any product is a key attribute of the usability. The user agrees with the product maker of the usefulness of that product.

**b. Efficiency** - Efficiency depicts how quick a user can achieve his/her goals is all about efficiency.

**c. Effectiveness** - Effectiveness is in a way related to efficiency. It defines error rate of a particular task and the result depends upon quantitative analysis.

**d. Satisfaction** - Satisfaction depicts the user’s experience after using the product. This usually captures via oral conversations with the user or by filling out multiple choice questionnaires.

4.1 Goals of Usability Testing

There are number of methods which can be used to measure and investigation of the task. For example- SUS (System Usability Scale), QUIS (Questionnaire for User Interface Satisfaction), CSUQ (Computer System Usability Questionnaire) and PSSUQ (Post-Study System Usability Questionnaire) are available for these kind of testing. We have used the SUS method as it is appropriate for this thesis study.

SUS method is very simple to understand and use. It covers variety of questions. It has a 1-5 rating scale for each questions asked during the testing. User testing brings out the usability perspective of the tested application as some usability perspective might get miss from the developer sometime. This testing is done by end users those are nowhere associated to the application. Usability testing can also be used to expose design errors, logical errors. There will be a Task based approach for the evaluation of these applications and based on the outcome the success rate has been measured in the evaluation phase.
4.2 participants and duration

All the participants were chosen from Linköping University and all of them are students studying/working in the university. All the participants are aged between 20-35 yrs.

The duration of the test was approximately 30 mins for each user. The test was conducted individually in various places in Linköping. Each applications’ rules were written clearly and also explained orally by the author in the beginning of the test. In total fourteen participants tested the applications. We started off with three pilot tests first. During the testing, the author of the applications was present and available to help. Each user has given a set of questions to answer and give the feedback of the applications after testing of applications. For the feedback and evaluation “Google form” has been used. The google forms were created for the questionnaire. There were total 11 different multiple choice questions for each participant to fill and one feedback column was available for those who want to give the feedback as well. The log data of each test has been saved in a file. By talking to all the users, verbal feedback was also taken after the test has been completed.

Two applications were tested one after another. Each application’s log data is saved in a text file for the analyzation part. The ‘adb logcat command’ has been used to save the logdata for the accelerometer values for each method.

4.3 Result Analysis and Interpretation

There are two ways to analyze the data- qualitative and quantitative [22].

Quantitative analysis- When all the numerical statistics can be analyzed using numbers such as number of users participated, number of tests performed, number of tasks which were successful etc.

Qualitative- Qualitative analyzation gives the emphasis on the eminence of the test performed such as user selection criteria, their satisfaction rate from the test, efficiency to use the applications etc.

In this thesis both approaches have been used and combined for the best results.

Why test Analysis

There are three primary reasons to test these thesis applications.

- The accelerometer data is showing the accurate values and in a stable condition while locking and unlocking the phone.
- The audience or participants accept the concept of locking/unlocking the phone through accelerometer values and not the traditional ways like drawing pattern or typing PIN.
- If the above two are accepted by the users and giving good results, then can this thesis be extended in future for more research and can be implemented in real life.
5. Survey Results

This chapter summarizes the work and highlights the results and future work.

This thesis work has shown positive response from the participants. Some of the participants were really thrilled by the concept of Sensor based authentication methods and some of them were reluctant for the change. The applications developed in this thesis work are

However, all the participants were interested in knowing the new concept. Between Tapping and Magic move about 80 percent of the participants liked the tapping application above Magic move. The reason behind liking the Tapping application was given that it was more user friendly and easy to use in comparison to Magic move. While 17 percent people liked the standard pin code application and did not want the variations in it. Below is a picture showing the result in a graph.

![Pie chart showing survey results]

6. Which application of entering a pin did you like the most?

- Enter pin-code by moving the phone: 0%
- Standard Keypad Pincode: 16.7%
- Tapping the phone: 83.3%
- Not sure: 0%

7. Why did the above mentioned application of entering a pin you like the most?

- Easy to remember: 0%
- Easy to use: 100%
- Not easy to use: 0%
- Not sure: 0%

8. Was it difficult to enter the pins when the device was vibrating continuously?

- It was easy to guess: 0%
- Not easy to guess: 16.7%
- Confusing: 66.7%
- It was ok: 16.7%

*Figure 5.1 - Showing the test result in a pie chart.*

While taking the feedback from the participants, they were in the opinion that the Magic Moves has more potential in the future. The applications are in pilot stage and some improvements are needed to make it more professional. For example- in case of any mistake while unlocking the
phone by the user, almost 60 percent of the participants felt that the application was confusing and not easy to use (unlock) it again. The reason behind the confusion was that the phone vibrates continuously while using the application and users quickly lose concentration of the directions in case of a mistake.

3. The instructions "How to use the App" was clear enough to understand.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0%</td>
</tr>
<tr>
<td>2</td>
<td>0%</td>
</tr>
<tr>
<td>3</td>
<td>20%</td>
</tr>
<tr>
<td>4</td>
<td>80%</td>
</tr>
<tr>
<td>5</td>
<td>0%</td>
</tr>
</tbody>
</table>

4. I would imagine that most people (between age group 20-40) would learn to use the application quickly.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0%</td>
</tr>
<tr>
<td>2</td>
<td>0%</td>
</tr>
<tr>
<td>3</td>
<td>20%</td>
</tr>
<tr>
<td>4</td>
<td>60%</td>
</tr>
<tr>
<td>5</td>
<td>20%</td>
</tr>
</tbody>
</table>

5. Was it easy to re-enter the pin codes in case of any mistakes?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Not easy</td>
<td>50%</td>
</tr>
<tr>
<td>Easy</td>
<td>33.3%</td>
</tr>
<tr>
<td>Not made any mistakes</td>
<td>0%</td>
</tr>
<tr>
<td>Confusing</td>
<td>16.7%</td>
</tr>
</tbody>
</table>

*Figure 5.2- Showing the testing result in a pie chart.*

Although, the users like the concept of tapping more than the other method, but the tapping is easy to guess in case of an intruder tries to attack. Magic move on the other hand is not easy even if the intruder tries to unlock the phone. The reason is that in the tapping case- An intruder just needs to tap the phone and waits till the n number of hits matches with the authentic user’s number of taps. This process is not so hard to repeat. On the other hand, in case of Magic Move there are 4x4 different permutations for the intruder to guess and every cycle has a waiting time before he/she can start guessing again.

The Tapping application needs improvisations and given below are some ideas which could be used for the next version of this application-

- Instead of tapping anywhere in the back side of the device, a specific spot could be introduced which is not easy to find/catch. For example- a place in the left or right corner of the device which is not easily recognized.
• Two Factor authentication is a good alternative to combine two methods for authentication for more security.
• The tapping should be more firm to be recognized by the accelerometer sensor. Alternative method would be that the gesture based recognition can be introduced along with the tap stroke.

Magic move seems more secure than tapping but this also needs improvements. For example—
• The speed in which the accelerometer recognizes the values can be improvised to a faster hand gesture.

General observations from both the applications are—
• To improve the set of instructions- One user could not understand the set of instructions given on the device before testing it so in future improvised set of instructions can be introduced.
• More user friendly applications as in the GUI (Graphical user interface) of the applications can be improved such as- Easy to navigate, more intuitive and effective error handling in case of a mistake etc.
• The professional touch- The applications can be improvised to more professional and skilled way so that any age group can use the applications.

This is the first time users tried these applications and according to the analysis most of the users liked the concept. These applications have a very new concept which was not implemented and tested by common users before in real life. This will reduce the fingerprint attack on smartphones. It also opens up one more notion and idea towards improvising the security of smartphones. The whole idea of the thesis was to identify whether users are giving positive response to the new concept and will they be able to adapt it in the future.

Users appreciated the idea of using the sensors on the phone for unlocking. However, they were doubtful and hesitant whether this new concept will get the same amount of popularity as pattern based or pin based unlocking the phone in real world have it already. Overall, majority of the participants liked the concept but are still skeptical of using the new techniques. The future work includes enhancement of the functionalities of the applications and the remaking of applications according to users’ feedback.
6. Discussion and Conclusion

The applications developed during this thesis work come under ‘Knowledge based authentication’ method. Knowledge based authentication is a very popular method of authentication which is based on the concept of what user knows. This method gives high security against guessing attacks as long as the secret used (password/Pin codes etc.) for authentication is not easy to guess by others. Generally, users are not careful while choosing the passwords. Users tend to choose easy passwords such as names, date of birth, house address which are vulnerable to guessing attacks. The guessing probabilities increase when the secret shared between a user and the device are easy to predict or shoulder surf by an intruder/attacker. According to a survey in a Norwegian University, 44 percent of people start their pattern based authentication from Top left corner of the mobile phone, so approximately 30% of the guess is completed without even try by the attacker. This shows that the attacker can easily guess the remaining pattern by randomly drawing different shapes in very short time. The attacker can either guess the remaining pattern or use the prior knowledge about that user which he might have gained after using different shoulder surfing techniques for example. Users are generally more inclined and interested to choose any authentication credentials such as passwords/Pin codes/Patterns which are easy to use, remember and less time consuming. While choosing a secret of any kind, user also needs to think about the probability of guessing the secret by the attacker in case of an attack. Ease to decipher a secret is directly proportional to the hardness of authentication security. The more harder the security is the more difficult it is to decipher/crack it.

There can be many alternatives to make a system harder to intrude. A user can opt for different authentication methods to use. For example- one technique is to combine one or more authentication methods one after another. The combination not only gives the double protection against the threat but also provides the duel security in cases of one type of authentication fails. The knowledge based authentication method can be combined with other two authentication methods such as Token based and Biometric based authentication. Using two or more authentication methods is called ‘Two Factor Authentication’. Two Factor Authentication is a two-step verification process which is generally used in high security areas. In Two Factor Authentication method, a user provides two different category of credentials. There are various categories such as passwords, Non text passwords, Digital certificates, smart cards, hardware tokens, biometrics etc. for authenticating a device. The combination of Password/Patterns and a sensor based method implemented in this thesis work (Taping/Magic-Move) can be used as one type of combination. One method after the other to add more security in smartphone authentication. This strategy can be a very robust to protect the smartphones from the threats mentioned in the thesis work. A picture represents the two factor authentication is shown below.
The flip side of using two factor authentication though is, that the process can be cumbersome and time consuming for users. Users who do not want to spend too much time on the authentication part will not use this technique.

Authentication of smartphones should be user friendly and at the same time robust and secure. The aim of this thesis report to offer a new technique and show some different routes along with some existing ones to increase and enhance the authentication of smartphones. Users can use the new methods implemented in this thesis work as either add a layer of security with the existing methods or can replace them with the new ones. This thesis work needs more improvements and many more feedback from different users to advance the quality of the applications in the future.

**Figure 6.1- Showing the Two way authentication.**
7. Bibliography / References

2. What is shoulder surfing http://robertsiciliano.com/blog/2015/05/15/what-is-shoulder-surfing.
12. Reducing shoulder-surfing by using gaze-based password entry dl.acm.org/
15. Zhi Xu et al. TapLogger: Inferring User Inputs On Smartphone Touchscreens Using On-board Motion Sensors. cse.psu.edu
17. What is Usability Testing and its benefits to users, istqbexamcertification.com
18. Step by Step approach of Usability testing, NNGroup nngroup.com/courses/usability-testing/
19. How to perform Usability testing nngroup.com/reports
20. Sensors overview developer.android.com
21. Agifall, Mark Fromson slideshare.net
22. Qualitative and Quantitative Research atlasti.com
23. What is the Difference between Qualitative Research and Quantitative Research? snapsurveys.com
24. Qualitative Data Analysis, Tilahun Nigatu slideshare.net/1895136
25. 10 Common security problems to attack in mobiles. www.pcworld.com
27. 3.1 million smart phones were stolen in 2013, pressroom.consumerreports.org
28. The compass is not working on my Android phone stonekick.com
29. Smartphone Popularity Around the World [business2community.com/mobile-apps/0574672]
30. 1 billion smartphones shipped worldwide in 2013 Tim Hornyak [pcworld.com/article/2091940]
32. Who’s Winning, iOS or Android? All the Numbers, All in One Place [techland.time.com]
33. which-is-more-secure-a-password-or-a-pattern-lock [makeuseof.com]
34. A quick tutorial on coding Android's accelerometer, William J. Francis [techrepublic.com]
35. Emulator sensors [doc.qt.io]
36. Magnetic North vs. Geographic North, gisgeography.com
37. serious magnetometer issues [forums.androidcentral.com/general-help-how/294734]
40. Sensors [gsmarena.com]
41. Tegra Android Accelerometer Whitepaper [developer.download.nvidia.com]
42. Tilt Sensing using three-axis accelerometer [cache.freescale.com]
Appendix A- Accelerometer detection

```java
if (sensorManager.getDefaultSensor(Sensor.TYPE_ACCELEROMETER) != null) {
    // Success! We have an accelerometer.
    accelerometer = sensorManager.getDefaultSensor(Sensor.TYPE_ACCELEROMETER);
    sensorManager.registerListener(this, accelerometer, sensorManager.SENSOR_DELAY_NORMAL);
    vibrateThreshold = accelerometer.getMaximumRange() / 2;
} else {
    // Fail! Do not have an accelerometer!
}
```

Appendix B- Magnetometer detection

```java
mSensorManager = (SensorManager) getSystemService(Context.SENSOR_SERVICE);
if (mSensorManager.getDefaultSensor(Sensor.TYPE_MAGNETIC_FIELD) != null) {
    // Success! There's a magnetometer.
} else {
    // Failure! No magnetometer.
}
```

Appendix C- Tap detection and Vibration detection

```java
if (currUpdate - lastShake >= interval) {
    Toast.makeText(cxt, "Tap registered", Toast.LENGTH_SHORT).show();
    tapCount++;
} 
lastShake = currUpdate;

Similarly, the same tap is recognized for the unlock the application.

if (force >= 5.0 && force <= 8.0 && accelerationSquareRoot >= 2.5)
if (currUpdate - lastShake >= interval) {
  Vibrator v = (Vibrator)
  this.getSystemService(Context.VIBRATOR_SERVICE);
  v.vibrate(200);
  tap_count++;
}

// Power manager to unlock the device screen
if (ServiceLock.tapCount == tap_count) {
  PowerManager manager = (PowerManager)
  getSystemService(Context.POWER_SERVICE);
  PowerManager.WakeLock wl = manager.newWakeLock(
    PowerManager.SCREEN_BRIGHT_WAKE_LOCK,
    PowerManager.ACQUIRE_CAUSES_WAKEUP, TAG);
}

Appendix D - Magnetometer values detection

// fetch the magnetometer values
if (event.sensor.getType() == Sensor.TYPE_MAGNETIC_FIELD) {
  //mag_values = event.values;
  mag_values = lowPass(event.values.clone(), mag_values);
  Log.i(TAG, "mag azimuth pitch roll " + mag_values[0] + " +mag_values[1]" + mag_values[2]);
  magValue = (float) Math.sqrt(mag_values[0]*mag_values[0] + mag_values[1]*mag_values[1] + mag_values[2]*mag_values[2]);
} // fetch the gravity data
if (event.sensor.getType() == Sensor.TYPE_GRAVITY) {gravity_values = event.values;
  Log.i(TAG, "gravity azimuth pitch roll " + gravity_values[0] + " +gravity_values[1] +" + gravity_values[2]);
}

private void registerListenerMagnetometer() {
  sensorManager.registerListener(this,
    sensorManager.getDefaultSensor(Sensor.TYPE_MAGNETIC_FIELD),
    SensorManager.SENSOR_DELAY_FASTEST);