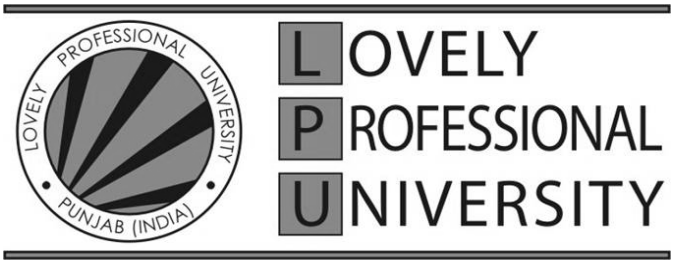

Smarter method for user authentication in mobile system

A Dissertation submitted

By

Malika Verma

(11011460)

to

Department of Computer Science And Engineering

In partial fulfilment of the Requirement for the

Award of the Degree of

Master of Technology in Computer Science and Engineering

Under the guidance of

Mrs. Monica Sood

Assistant Professor, Lovely Professional University

(May 2015)

PAC Approval Page

LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

School of: LFTS (Lovely Professional University)

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Malika Verma
Registration No: 11011460
Batch: 2010-2015
Roll No: RK2006B33
Session: 2014-2015
Parent Section: K2006
Details of Supervisor:
Designation: AP
Name: MONICA
Qualification: MTECH
U.ID: 14858
Research Experience: 4 years

SPECIALIZATION AREA: Mobile System Security (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Smarter method for user authentication in mobile systems
2. Behavioural Biometric based authentication system
3. User Authentication on swipe pattern behaviours

Monica SOV
Signature of Supervisor

PAC Remarks:
first topic approved, publication expected

APPROVAL OF PAC CHAIRPERSON: Signature: Date: 30/9/14

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)
*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.
*One copy to be submitted to Supervisor.

ABSTRACT

User authentication is an important issue that needs to be taken seriously especially in case of smart phones where the statistics say that almost half of smart phone users use no authentication system since they need to unlock their devices quite frequently and that complex passwords are difficult to remember and time consuming while entering each time they need to log in. Other issues such as unauthorized access in case of password hack also need to be considered for better security. Biometrics claim to be more secure way for authentication purposes as physical and behavioral traits of a user are difficult to imitate just like writing your signature of fingerprints.

This report discusses the existing user authentication methods for smart phones, and current statistics of user authentication in smart phones explaining the reason why people do not like to have any authentication mechanism on smart phones despite having sensitive data and other confidential accounts logged in. A new user authentication method based on graphical password and behavioral biometrics has been discussed in this report which is reliable, easy, secure and fast at the same time.

CERTIFICATE

This is to certify that Malika Verma has completed M.Tech dissertation titled Smarter Method for user authentication in mobile system under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation has ever been submitted for any other degree or diploma.

The dissertation is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech Computer Science & Engg.

Date: Signature of Advisor

Monica Sood
14858

ACKNOWLEDGEMENTS

It is not until I undertake the topic like this one that I realize how massive the effort it really is, and how much I must depend on efforts and working help of others. There are many who helped me in finding this topic for further research, and I want to thank them all from the core of my heart.

Most importantly I offer my sincerest appreciation to my mentor, Mrs. Monica Sood, who has underpinned me throughout my thesis with her tolerance and learning whilst permitting me the room to work in my own specific manner. She always helped to clear all doubts generated during different parts of this literature review and formulation of statement for my research work. Her guidance is also a motivation for me to do work on time. Her guidance was crucial for formulation of problem statement. I attribute the level of my Master's degree to her consolation and effort and without her this proposal, would not have been composed.

I am also very thankful to our Computer Department for all their valuable technical advices. I would like to thank my friends, who were always willing to help and give their best suggestions. My research would not have been possible without their help.

Finally, I would like to thank my parents. They were always there to cheer me up and stand by me through the good times and the bad.

DECLARATION

I hereby declare that dissertation entitled, "Smarter method for user authentication in mobile system", submitted for the M.Tech degree is entirely my original work and all ideas and references have been fully acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

Malika Verma

11011460

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1
INTRODUCTION

In digital world, the key to open any lock or a door is traditionally a password. Theoretically, it provides high security, as the only place to keep this secret key is user's mind. But, in practice, human mind is an awful place to remember complex passwords. People usually forget complex passwords. More the complexity more is the security but at the same time, more are the chances to forget. To recall, some people write down their passwords at places or use same password for multiple accounts. Even if the password is complex, attacks like key logger, social engineering or shoulder surfing are commonly being used.

1.1 Graphical Passwords

When it comes to smart phones, graphical passwords are also very common. They are designed to make passwords more memorable. They serve as a solution to the remembering problem of traditional passwords. These include methods like drawing a pattern, locating some images, etc. They are easier to remember and recall as compared to traditional passwords.

1.2 Biometric Passwords

Biometric passwords are based on the concept of what a user possesses. Unlike knowledge based, which includes traditional and graphical passwords, this type of password work on user's physical characteristics or habits that are unique to a person and are very hard to imitate. It is very difficult to find similar biometric characteristics in different persons. They focus on "Who you are?" as every person has unique traits and qualities and habits that do not match with any other person. These can be broadly classified as:

1.2.1 Physical biometrics

It includes the physical characteristics of a user like fingerprint, face recognition, iris scan, voice, size of palm etc. There usually require special hardware to be implemented for scanning and recognizing a user's physical traits. It focuses mainly on "Who you are" physically i.e. physical parts of a human that are unique to itself like iris, voice etc.

1.2.2 Behavioral Biometrics

It includes the behavior and habits of the user like the speed of typing, walking, speaking etc. These are just like writing your signature. It is difficult to write someone else's signature. It focuses on "who you are" by means of habits of a person that are not common in all with another person.

1.3 Security Habits of Smart Phone Users

The number of smart phone users is increasing swiftly, worldwide. Whether it comes to social networking, online banking, storing private data, the frequency of the usage of smart phones grows the call for stronger device protection method.

According to Info Security Magazine Report in 2012, More than half of Smartphone and tablet users did not perform the most basic security protection measure, such as password-protecting their devices, despite having them connected to sensitive online accounts and applications. This clearly shows that security does not coincide with usability when it comes to mobile devices.

1.3.1 Available authentication methods

Android provides various types of authentication methods in its devices by default in different devices. Apart from the default available authentication schemes, many other are available in the form of android apps on Google play store. Some of the commonly used schemes have been discussed below:

a) Slide lock-This lock screen is provided by android Operating System and it provides no security. Users simply slide horizontally to unlock the screen.

b) Glass lock- This lock screen is provided by Samsung. It also serves no security and is similar to slide lock but is not just restricted to slide horizontal. Users can make any gesture pattern to unlock the screen.

c) Pin lock- This lock provides a digit set of numbers 0 to 9. Users need to enter a specific pin which is a sequence of digits that serves as the key.

d) Password- This lock provides a set of alphabets, numbers and special characters and provides a larger sample space than the pin lock.

e) Pattern lock- This lock is one of the commonly used graphical password scheme in white nine dots are provided and user is required to draw a pattern by easy dragging. Apart from these some other biometric based locks such as face lock, finger print lock, voice lock etc. are also available in smart phones.

1.3.2 Current statistics

With the change in time and awareness among people, especially the youth, the results have improved and a change can be seen in the security habits of people in their smart phones. When some mobile authentication based questions were asked to people about their choices and preferences, the results were as follows:

- 37% people had no password on their device, the reasons for which were given saying it consumes a lot of time each time they need to use their device. Some said they were not good at remembering passwords and some gave some other reasons.

- Out of the remaining 63% people, who had authentication schemes on their devices, 56% people use pattern scheme for authentication saying that it is much faster and easier to remember as compared to other authentication schemes.

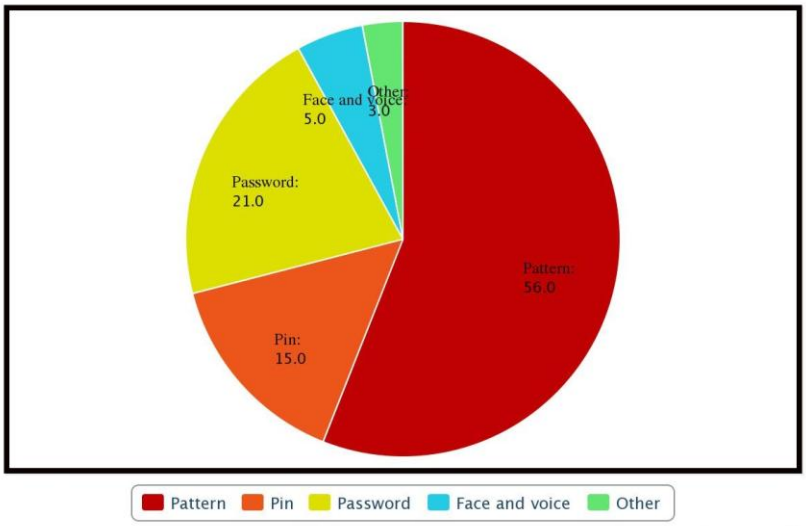

Figure 1.1 Type of authentication method used

- These poor security habits have likely come about because typing passwords on mobile devices is difficult and time consuming and so people prefer convenience over security.

- More than 30% people said that they often mistype their passwords because of small keys and ultimately remove password because of frustration. The inconvenience is greater for people who have put strong and complex passwords ultimately ending with people choosing easy and weak passwords or no passwords at all.

- More than 60% people reported that they need to unlock their devices for more than 15 times on an average daily. And the inconvenience caused for typing passwords is a big issue. 90% people agreed that they wish there was an easier way of authentication for mobile devices.

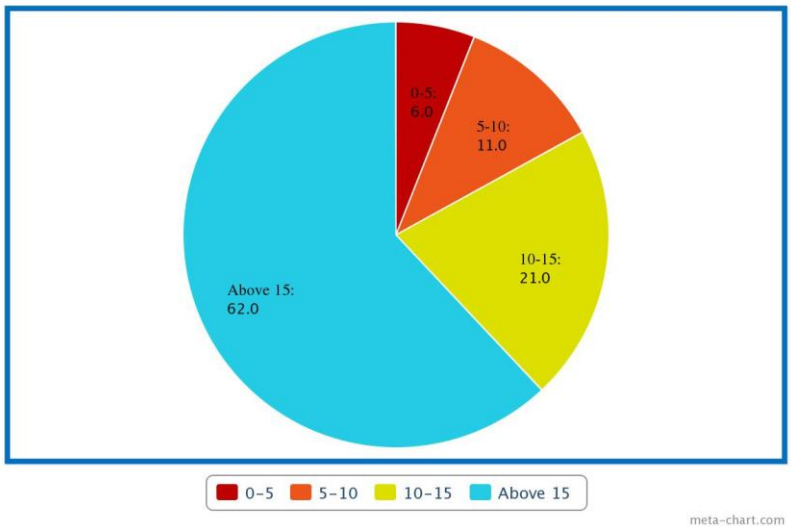

Figure 1.2 Frequency of unlocking smart phone daily

The statistics of what users said when they were asked to tell how many times they need to unlock their smart phones on an average daily have been shown in figure 1.2. Most of them reported that they unlocked their smart phones for more than 15 times on an average daily.

Conclusion: The results in figure 1.1 and figure 1.2, show that easier and faster way of authentication is preferred when it comes to mobile devices that are used very frequently. People prefer pattern lock for authentication which provides one million key spaces. However, if user chooses an easier pattern for the sake of convenience, security becomes weaker and if strong complex patterns are chosen, it becomes uncomfortable. As a result, there is a need of having an easier, faster and smarter way for authentication.

Chapter 2
TERMINOLOGY

S.No	Term	Meaning
1.	Access	The permission or opportunity granted to enter a device
2.	Active biometrics	This refers to the physical traits of human beings to be used as an authentication factor
3.	Algorithm	The detailed process or set of rules for solving a problem by a computer.
4.	Append	To add to a string in the end
5.	Application	A software or program that fulfils a specific purpose in android systems
6.	Authentication	To prove that the user is valid and genuine
7.	Authorization	Giving permission
8.	BB Lock	Behavioral Biometric based authentication method discussed in this report
9.	Behavioral biometrics	Traits of a being that are purely based on habits
10.	Biometric password	A password that is based on physical or behavioral characteristics
11.	Compromised	When the account of a user is being used by some unauthorized person by illegal means
12.	Concatenate	To add to a sting at the end
13.	Database	A set of data recorded in a computer
14.	Digital	Relating to storing or using of data in electrical signals
15.	Feasible	Possible to be done practically

16.	Frequency	Number of times an activity is being performed per unit time
17.	Dynamic generation	Non static, random on the spot generation
18.	Gesture	Moment of thumb of part of body to express something meaningful
19.	Graphical password	A non textual password in visual form
20.	Iteration	Set of instructions to be repeated round wise
21.	Key logger	A software or hardware that keeps a record of the keys pressed in sequence
22.	Online banking	Performing banking transactions over the web
23.	Passive biometrics	This refers to using the behavior or habits of a human as authentication factor
24.	Password	A set of characters that act as key to a device lock
25.	Pattern	A graphical regular path or design
26.	Pixel	A minute area of display on the screen
27.	Physical biometrics	Physical traits of a being that are unique to the being itself
28.	Registering	Enrollment in some application
29.	Resolution	Degree of visibility
30.	Scheme	It here refers to the system or the methodology i.e. the type of authentication method
31.	Security	State of being free from danger or threat
32.	Sensor	Device that measures a physical property and records it
33.	Shoulder surfing	Spying on a user for knowing his password by standing behind and trying to look while user types the password

34.	Smart phone	A computer like mobile phone
35.	Social engineering	To try to know somebody's password by getting hints by verbal communication
36.	Social networking	A network of social interactions and personal relationships
37.	Synaptic weight	A numeric magnifier assigned to a factor depending upon its contribution
38.	Textual password	Non graphical text containing password like a PIN or alphanumeric password
39.	Touch sensitive	Surface or a screen sensitive to touch and being able to record it
40.	Ubiquitous	Frequency of usability
41.	Unauthorized user	An invalid user who does not possess permissions to access a device

Chapter 3
REVIEW OF LITERATURE

Various authentication techniques for mobile system and those based on behavioral biometrics were studied before proposing a new methodology. Some of those have been discussed in this chapter.

3.1 Yet Another Graphical Password Strategy

A brief introduction about DAS, Draw-A-Secret and BDAS, Background Draw-A-Secret has been given in this paper. DAS and BDAS were the very first graphical password strategies with some problems such as Lines above grid lines Endpoints near grid line and strokes near cell corner.

To cure the problems with DAS and BDAS, a new strategy for graphical password has been discussed based on neighboring cell of grid. It works on a 48X48 grid. The basic methodology on which this strategy works is the string S, which is created using the neighbor grid as the pattern, is drawn moving from one cell to another. Also the pen up and pen down activities have been covered with the character '5' being added to the string S. As the user moved up the cell on the grid, '2' is added to the string S. A downward moment appends an '8' in the string. Horizontal left is marked by '6', horizontal right by '4', diagonal movements are also recorded using '1', '3', '7' and '9' for top left, top right, bottom left and bottom right moments respectively. Therefore, this strategy gives much better results as compared to the DAS and BDAS and the similarity computational technique becomes more reliable and easier in comparison to DAS and BDAS that user binary string for storage of pattern path.

3.2 Pressure and Latency-Based Typing Biometric System

This study had been mentioned in the research paper titled "Evaluation of Classifiers in a Pressure and Latency-Based Typing Biometric System. This study has been done for extracting pressure and latency behaviors of users while typing. The accuracy of typing based biometric system has been evaluated in this study using the two factors, pressure and latency where pressure refers to the pressure of key strokes while user types something and latency is the time gap between two key strokes.

It works on the behavioral biometric trait of a user for improved mechanism while typing a password based on individual style and pattern of typing on a keyboard. A pressure sensitive Keyboard was used for this purpose and samples were collected from typing behavior of 18 different users. The result of this study said that latency was more reliable than pressure while it comes on typing habits of an individual.

3.3 Continuous Mobile Authentication

This study "Continuous Mobile Authentication Using A Novel Graphic Touch Gesture Feature" has been done on touch sensitive phones to check the feasibility of behavioral biometrics on the basis of touch gestures on various users. This included the six basic touch gestures namely Slide up, Slide down, Flick left, Flick right, Pinch and Spread. These gestures can be measured while user performs operations like zoom in, zoom out, change pictures in gallery using slide, scroll up, scroll down etc.

This was experimented on 30 users, out of which 28 were left handed. The six basic touch gestures were continuously recorded and system was made to learn, averaging each time a user performed any of these gesture. Later on it was seen that the results of learning process could be used for continuous authentication purpose whether the same user is using the device or someone else is so that it gets locked automatically when unauthorized use has been detected.

3.4 Improved Authentication System for smart phones

This study titled "Design and Implementation of Improved Authentication System for Android Smartphone Users" gives another graphical strategy for authentication purpose. The idea of different launchers for different user purpose has been implemented. A user mode and a guest mode have been discussed. Rarely used personal applications are not available in the launcher of guest mode. And a full access to all the applications is been given in the user mode, that needs an authentication to be done. The other mode is the emergency mode or the guest mode that can be accessed easily without any time consuming authentication requirement.

For authentication for user mode, a methodology has been given that provides six circles placed on the screen in a circular fashion. The order of tapping of the circle is marked with a color change and this is the basis of authentication for user mode. If the

order of the tapping of circles is correct, as saved with the system database, access is granted to the user mode else guest mode is open for the user.

3.5 Graphical Password Based Scheme

This paper discusses the problem in recalling of the textual based passwords and emphasize on the need for graphical password. A very unique graphical password strategy has been discussed in this paper. It has multiple rounds. In each round a set of pictures is provided to the user. In each successive round, shuffling of picture position is done. The user needs to identify his already chosen favorite pictures out of all in each round and mark them by drawing a circle that covers all three of them at the same time.

3.6 Password Input method using authentication Pattern and Puzzle

This scheme talks about the riddle picture and riddle pixels mapping is randomly produced, making the process of authentication unique and joyous. Various schemes are covered under this that has been discussed below.

3.6.1 Convex Hull Click Scheme

Proposed System include Convex Hull Click Scheme secure user from Shoulder Surfing attack or video recording or electronic capture. User chooses many icons as his password. At the time of login, user may go through various icons and recognize his chosen icons. Now user has to form a convex hull that covers three of his chosen icons.

3.6.2 S3PAS scheme

This paper proposed a scheme for client and server environment. Client is shown with local generated image, with character's array. Coordinates of each character are synchronized with server, which is less costly as compared to sending image to server. In this scheme user have to recognize his password letter and create convex hull in mind and enter password as the centre character in convex hull.

3.6.3 Proposed Password Input Method

From Grid of 6X6 user can select 12 cells, with 6x2 approach or 4x3 approach, This is more secure with multiple rounds. User's Password character should not appear in his chosen cell. If it happens, user has to move the cells as the grid is moveable in all

directions. This Mechanism works well and provide security against Shoulder surfing attack, Key logger and Replay attack.

3.7 Authentication Frequency as an Important Design Factor

This scheme mainly focuses on the frequency of handy devices especially the mobile devices. The need for authentication frequency in mobile devices is different from that of in case of laptops and other gadgets. Even for a quick simple work, mobile devices are used and users need to authenticate themselves each time. Thus, trying to provide a solution to this problem, the author talks about a new scheme where the activities of user are recorded like the busiest hours of the user or the times when he is busy. These factors are then used and the user is not asked to authenticate itself always. For example, when the user is alone and there is no noise being sensed by the device, it can be inferred that the user is alone and there is no need to ask for a password. Also there is nobody around to shoulder surf.

All the daily activities of the user are recorded for a period of time and using machine learning concepts, the device is made to learn when to ask for authentication and when not. There are times when user unlocks the device more frequently for small and quick works. Again at such hours, authentication must be skipped as it makes no sense to keep entering your password again and again for quick and short works. The author shows interest in any idea that helps serve the purpose of frequent authentication to be made smarter and learning.

3.8 Input Password Only with Four Keys, Three Times

This scheme focuses on prevention from keylogger attack. While user enters his password, if there is some keylogger being installed in to the system, all the pressed key strokes are been saved and the textual password is easily hacked. This mechanism serves prevention from this problem of keylogger by providing a new mechanism in which only cursor moment keys are used. A keylogger is not able to record the key strokes of cursor movement keys. The benefit of this fact has been used to frame this mechanism to make it safe from keylogger attack.

It is more of a graphical methos in which an 8X8 matrix is provided to the user. This matrix contains characters A-Z, a-Z, 0-9 in a random fashion. Virtually the matrix is

divided into four smaller matrices of 4X4 each with virtual numbers 1 2 3 and 4 assigned to each of it depending upon the position of smaller matrix in bigger matrix. User needs to identify the sub matrix in which the character he chose as his password is present and move to it using the cursor keys. This smaller 4X4 matrix is again subdivided into four equal 2X2 matrices and again the same procedure follows. This happens for three times until 1X1 matrix is left, which is of course the password of the user.

3.9 GOTCHA Password Hackers

Textural passwords are not secure enough as they get cracked very easily. In today's world, the user needs to sign up various websites and in most of cases password is same with average hardness level of password. On other hand if password is different on different website it tends to be under easy category. Offline security password are always prone to Dictionary Attacks, Brute Force use this dictionary attack to break in to password mechanism. In this research paper, the discussed password input mechanism separate human and computer.

GOTCHA is a random puzzle generation protocol, which help can tell if the user trying to get access is human or computer. GOTCHA should satisfy two key properties. First puzzles generated should be easy for human to solve; computer should not be able to solve the puzzle in the time. Second Puzzle must be hard and computer must not be able to solve even if it use random bits generated by computer. GOTCHA make sure that no dictionary attack is possible on puzzle and if any password cracker is used it must receive constant feedback from human while caring on with attack. Puzzle generated by GOTCHA lays on assumption that users can recognise the phrases that they originally used to describe each an inkblot image. Inkbot contains various circle and eclipse of different colour. User is also presented with various names and phrases user needs to identify the image and guess what it could be. User can select number of cycles it has to go through.

Chapter 4
RATIONALE AND SCOPE OF THE STUDY

As it has been discussed in chapter 1, the statistics of user's habits of authentication methods call a need to look into this field more seriously so as to provide a more reliable, easier and smarter method of authentication in devices like smart phones that need to be unlocked many times and may contain confidential data as well. As technology keeps updating itself overnight, the sensitive touch screens of these devices can be used to sense user's habits that can be recorded and later used for authentication purpose. Graphical passwords are more common these days and much more convenient to remember as compared to traditional password schemes. So, graphical passwords in combination with behavioral biometrics have been used for the purpose of identifying the authorization of user so as to achieve the objective of this research.

The scope of technology is quite vast. In the study for smarter way of authentication in mobile systems, the proposed methodology is expected to be implemented on Samsung Android phone that provides glass touch lock screen through which various behavioral biometric factors can be measured. The same can be implemented in any other touch sensitive device that includes Windows based phones, ATM or some other touch sensitive device that can be used for user authentication.

Since using a glass touch is similar to drawing a pattern in a graphical password, this makes the sample space of the input very large. This helps in prevention of various password stealing attacks without compromising with the simplicity of the mechanism. During the study, graphical passwords, behavioral biometrics, and prevention against password stealing attacks have been kept in mind so as to extract the best of all these concepts so as to bring usability, simplicity and security while authentication of smart phones closer to each other.

The number of smart phone users is quite large worldwide and so becomes the scope for it. The proposed idea can be implemented in and Touch sensitive device that needs to be unlocked very frequently daily. The statistics of users having and not having any authentication method, the proposed system can serve as a helpful solution to the same. As the technology is developing each day, devices with more sensitive touch

screens might be available in future that may be able to record more gestures of a user. These habits can then be recorded and used for the purpose of identifying the correct user. Even if some unauthorized user gets to know the pattern or the pin, he may not be able to get access. An authorized user may not be able to redraw the same pattern with same behavior, but it would not be so different as compared to that of an unauthorized one.

With the emerging technology and handy devices being launched every now and then, people are becoming more dependent on mobile devices and are shifting their activities more on these devices instead of using desktops and laptops. Tablets and smart phones have taken their place when it comes to doing temporary quick works. This makes people more and more dependent on these devices. This dependency has extended to keeping our banking and other accounts logged in with these devices. Thus, the discussed methodology can be implemented and used in almost all the future mobile devices that are used very frequently throughout the day.

Chapter 5
OBJECTIVES OF THE STUDY

5.1 Objectives

The objective of this research is to provide a method for authentication in smart phones such that it is easier, cheaper, faster and secure at the same time. This includes improvisation of the statistics mentioned in figure 1.1 and figure 1.2 of chapter 1 of this report, in the terms that users do not find it difficult to type or remember their passwords and at the same time they achieve security.

The main objective that was kept in mind during the process was to find a better solution to the problem of users not using any authentication method in their smart phones. The following points were kept in mind as the objective of the study of this research so that it is useful to the smart phone and tablet users worldwide. A solution that possesses the same can be summarized as having following qualities:

a) **Easy to remember:** Easy to remember so that the problem of forgetting passwords is solved and users do not remove their passwords in frustration. Since the proposed method does not contain any textual password to be remembered, this quality is maintained. Though physical biometric passwords do not need to be remembered, but they compromise ease with delay and unease while use like we experience in face lock if it is dark.

b) **Fast and Quick:** The system must be fast and quick so that the problem of users complaining about the time taken while authentication is solved. The proposed system is graphical based, so is expected to be quick. Unlike textual passwords, there is lesser scope of typing mistake because of small keys and large thumb size. Also since it does not include any physical traits to be scanned, it is much faster than active biometric locks.

c) **Difficult to hack:** The system must be difficult to hack as biometrics cannot be copied, an unauthorized user cannot possess same gesture habits as authentic user and illegal access can be reduced. Also since biometrics cannot be observed or seen while drawing a pattern, it becomes difficult to hack. It is so unique to a

person that it is very difficult for two different people possessing similar biometric traits.

d) **Cheaper in terms of cost:** The system is expected to be cheaper as compared to physical biometric based systems that require special hardware like fingerprint scanner, a high quality camera for face scan and other physical trait scanners that costs high and may not function properly in unsuitable environment like face recognition in dark is difficult or voice recognition in noisy environment again is very difficult.

e) **Adaptive of user's habits:** The system is expected to learn and adapt user's changing habits with time by implementing a self learning algorithm which can be designed on clustering basis, in future. This algorithm can be made by making use of concepts of artificial neural networks and clustering of data. With the changing habits of user over time, the system may be able to adapt accordingly and update itself automatically.

The discussed system fulfils the objective of the research by possessing all the above mentioned objectives so that this can be useful for smart phone users worldwide and the research turns to be fruitful.

Chapter 6
RESEARCH METHODOLOGY

Keeping in mind the objective of this study, a methodology has been discussed that would work on touch sensitive devices that are more likely to be used in future. For providing a smarter way of authentication, in the terms of simplicity and security at the same time, a behavioral biometric based user authentication scheme has been discussed. The behavioral factors would be measured simultaneously while pattern is being drawn. This includes five main factors:

- Velocity ‘V’ while drawing the pattern.
- Pressure ‘P’ exerted on the touch screen while drawing the pattern.
- Portion ‘G’ of the screen where pattern is being drawn.
- Area ‘A’ covered by the thumb or finger of the user while unlocking the device.
- Time ‘T’ taken by the user to draw the pattern in milliseconds.

If any of these parameters does not match with that of user’s habit, access cannot be granted. Also if the pattern path itself is not similar, access cannot be granted. Varying of any of these parameters to a huge extent would result in blocking the user from accessing the device. A relatively small difference with the stored values of these parameters would be negligible as it is very difficult to redraw the pattern with exactly gesture each time user wishes to unlock the device. Figure 6.1, figure 6.2, figure 6.3, and figure 6.4 and figure 6.5 shows the same.

The procedure includes a process of registration first that includes making the device record the habit of user by making him perform the action of drawing a pattern repeatedly in the same manner. While the user draws the pattern, all the factors namely path, time, pressure, area, position and velocity are been sensed and saved to the database. The repeated gesture of drawing the pattern should not vary much while same user is drawing it. An average of the repeated inputs, depending upon their reliability factor are been saved into the device database for authentication during login attempt.

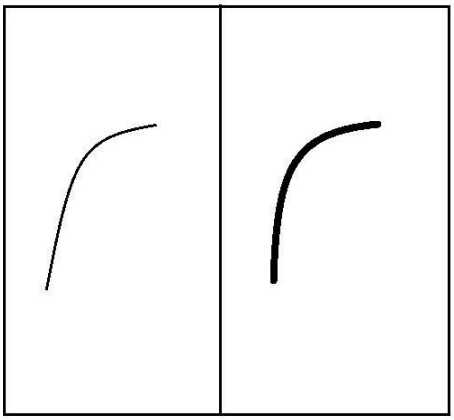

Figure 6.1 Varying Area of touch

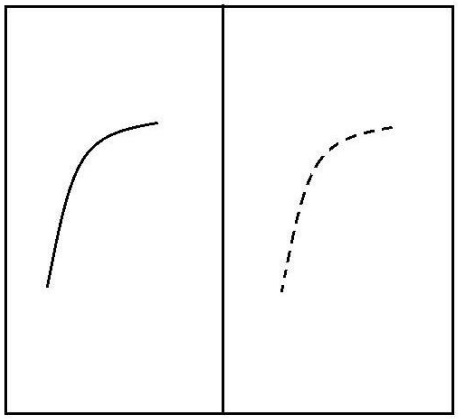

Figure 6.2 Varying Velocity

Figure 6.1 shows huge variation in area of contact of screen and touching finger while pattern is being drawn. A valid user when tries to draw a pattern for multiple times, not too much of variation in the area of touch of finger or thumb with the screen in expected. Figure 6.2 show huge variation in the speed of drawing the pattern. A registered user when tries to draw a pattern for multiple times, not too much of variation in the velocity of drawing the same pattern in expected.

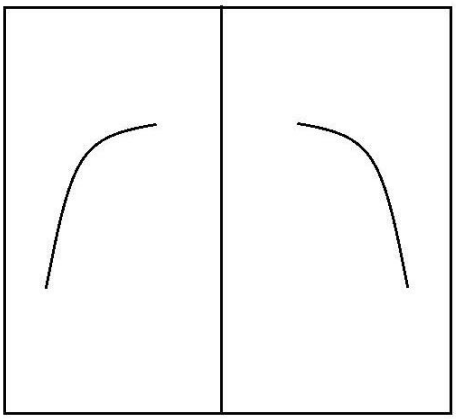

Figure 6.3 Varying Pattern paths

Figure 6.3 shows huge variation in the pattern and thus the string formed as discussed in section 6.1. This is highly not acceptable when it comes to user authentication as it is expected from the valid user to draw same path each time they wish to login as it acts as key to the lock of device. Thus, pattern act as an important factor.

Figure 6.4 shows variation in pressure while drawing the gesture pattern. Since this is also one of the important factors depending upon the orientation and way of holding the device by the user and the physical trait which is the size of finer or thumb, pressure values vary from person to person while they try to draw the same pattern. This factor can also be used as a factor for authentication purpose as it is included in the passive biometrics of an individual.

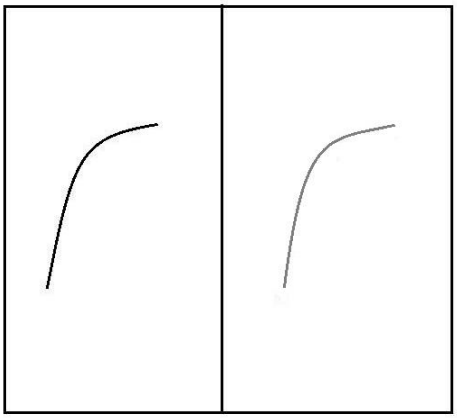

Figure 6.4 Varying Pressure

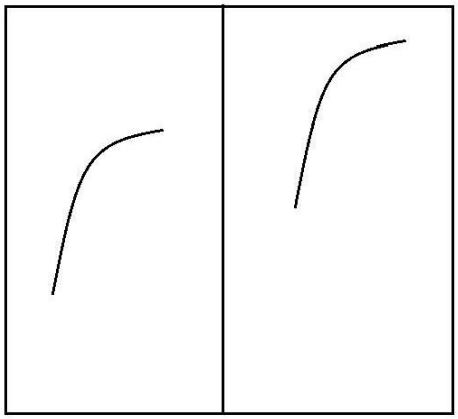

Figure 6.5 Varying Positions

Figure 6.5 shows variation in the position where the pattern is been drawn. This trait depends upon the size of the hand and thumb or finger. Also it depends more on the habit of a person of holding his own device. It is very likely that a single person would hold a device similar way each time and make use of same portion of the screen more conveniently. Thus, this can be used as a factor for authentication.

For recording of position of gesture pattern, the screen of device is been divided into a grid of six equal halves with each being identified using an alphabets A, B, C, D, E and F as shown in figure 6.6. Depending upon the starting pixel position of the pattern, it is being classified into one of the group and stored in the database. User is expected to redraw the pattern into same cell each time according to behavioral biometrics.

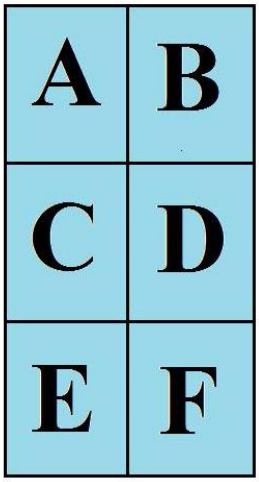

Figure 6.6 Position detecting grid

6.1 Pattern input mechanism

As the user tries to unlock screen, and makes pattern on the glass lock screen of the device, the recording of the pattern begins based on the pixel values of the touched area. No concept of grid is used in this methodology. Instead, a string S is generated dynamically according to the traced path the user draws. A similar concept as in YAGP is used for string generation. A character is concatenated to the string depending upon the pixel value of the position in the path relative to the last pixel position traced. Since high

resolution screens provide large number of pixels, some fixed number of pixels would be skipped for each concatenation in the string.

A sample pattern drawn by the user is shown in figure 6.1.1. The corresponding string S can be generated using direction of pixel in comparison to last major pixel depending upon number of falling of next major pixel. In the pattern drawn in figure 6.1.1, the first letter of string S would be 8. Now the invisible box would move to next major pixel and the same process continues and numbers start appending in the S.

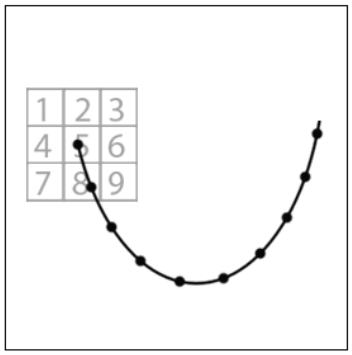

Figure 6.1.1 Pattern to string mechanism

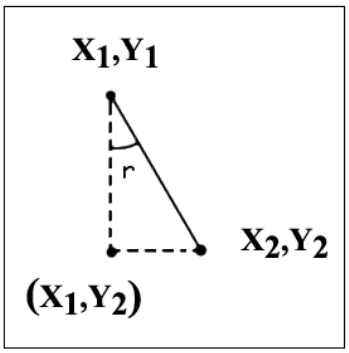

Figure 6.1.2 Identifying the angle

The methodology for identifying which number is to be chosen from the string generating list to be concatenated in string S, can be seen in figure 6.1.2. This generates three possible cases as follows:

- If (x_2-x_1>y_2-y_1), then r>45 and S=S.6
- If (x_2-x_1<y_2-y_1), then r<45 and S=S.8
- If (x_2-x_1=y_2-y_1), then r=45 and S=S.9

Similarly, for all other cases, depending upon the path of the pattern, the direction in which it moves relative to the previous point, a concatenation is been done in the string S representing the traversed path. Depending upon the speed of drawing the pattern, the pixel positions that are been detected are termed to as major points and each major point is relative to its previous major point in some direction. This direction is been detected and string is been generated accordingly.

6.2 Comparing mechanism

Each user would have an already saved pattern of unlock while registering with the system. A string S is present with the database of the system with which the new string S' is to be compared for authentication. Along with this, other factors i.e. velocity, area, position and pressure would be saved with the device.

Since it is not feasible to say that the user must redraw the same pattern exactly with exactly same position, pressure, area and velocity as it is saved with the device, the concept of margin has been introduced i.e. a fixed error value that can be tolerated for each parameter. Access can only be given if redrawn pattern is drawn with almost same velocity, almost same pressure, at almost same portion covering almost same area i.e. all the following five conditions are satisfied:

- $S=|S'-S_m|$, where S_m is the fixed value of tolerated margin of pattern
- $G=|G'-G_m|$, where G_m is the fixed value of tolerated margin of position
- $P=|P'-P_m|$, where P_m is the fixed value of tolerated margin of pressure
- $A=|A'-A_m|$, where A_m is the fixed value of tolerated margin of area
- $V=|V'-V_m|$, where V_m is the fixed value of tolerated margin of velocity
- $T=|T'-T_m|$, where T_m is the fixed value of tolerated margin of time

These fixed values are some percent of recorded values depending upon the strictness of the comparison. If the user wishes to have strong and tight comparison, these values are relatively small and user itself needs to draw the pattern more precisely and the inverse also holds true.

If incase, the authentic user is unable to redraw the same pattern, another authentication procedure AP2 would run that has been discussed in section 6.3. The flowchart for comparing mechanism can be seen in figure 6.3.1. The string S' is generated depending upon the pattern drawn. It is then compared with the stored string S. If the pattern matches, rest of the factors is compared in the same manner keeping a tolerant margin value.

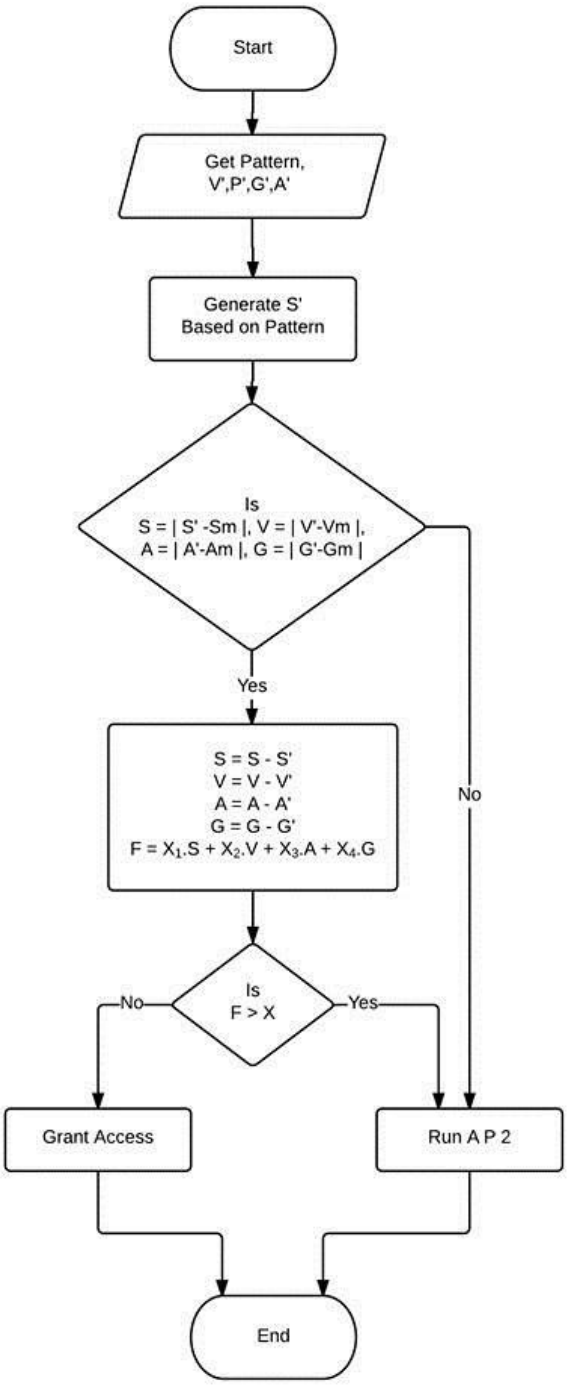

Figure 6.2.1 Flowchart for comparing mechanism

Once all the parameters match individually, F' is calculated based on the synaptic weights of each parameter x_1, x_2,…x_n. Since each factor plays a specific role and depending upon its reliability by analyzing the data, they can be given some weights. If this matches with the stored F, access is granted else AP2 runs. AP2 i.e. Authentication Process two has been explained in section 6.3.

6.3 Authentication Process 2

If incase authorized user is unable to draw the pattern in the same manner by mistake, a set of questions based on the user's own activity in the device can be asked. These questions may be related to the applications used in the smart phone in last fortnight period.

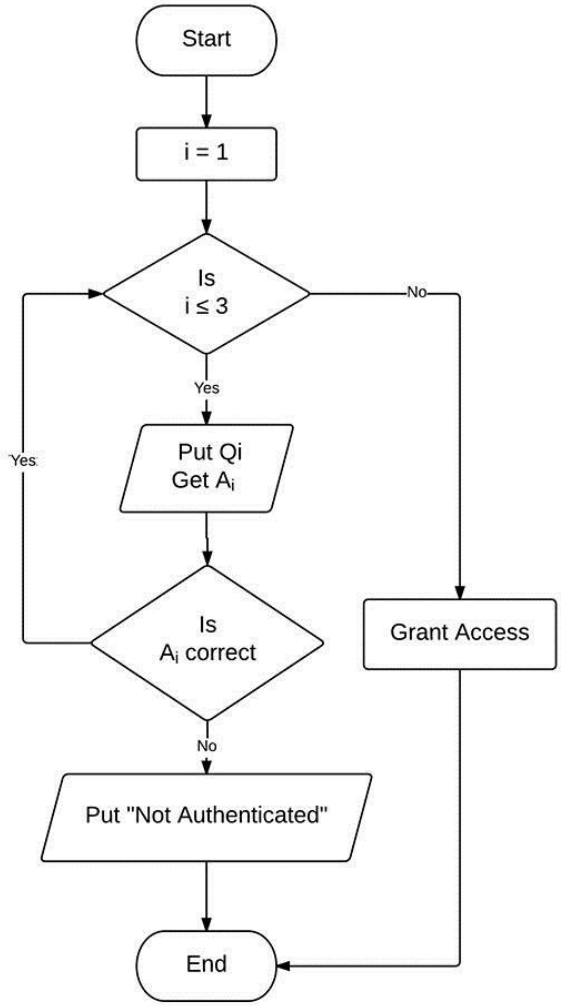

Figure 6.3.1 Flowchart for Authentication Process 2

These memory based questions can only be answered correctly by the authorized user itself who has been using the smart phone. A set of questions Q_i, atleast three in number can be randomly asked to the user with a list of correct answers A_i associated to each. These questions may be like, "Did you call abc in last one week?" The flowchart in figure 6.3.1 explains the same process.

Chapter 7
RESULTS AND DISCUSSION

7.1 Experimental Work

To check the correctness and feasibility of the idea, various users were made to draw patterns of their choice and the data was recorded that includes the string S, starting position of the pattern G, velocity of drawing pattern V, time taken in milliseconds T, pressure P and area A. Each user entered a pattern 10 times and data was stored for further analysis. A step wise procedure of pattern recording for one user can be seen in figure 7.1.1, figure 7.1.2, figure 7.1.3 and figure 7.1.4. The very first step is to opt for recording gesture pattern. As soon as user clicks on it, a new window asking to draw your pattern opens. Here, user has to draw a pattern of his own choice iteratively for ten times. String of the path, as well as other factors begins recording with the very first step. If the user is using a stick, pressure values are obtained and if finger or thumb is been used to draw the pattern, area values are obtained. Both the factors might be able to be measured in future devices. This experiment was conducted on many users of which data of twelve have been discussed in this report in section 7.2.

The string generation and matching is highly dependent on the type of pattern drawn. If more curves are included in the path, string may not be equal each time but it increases the sample space of the system i.e. almost unlimited patterns can be drawn in the discussed system as per the convenience of user. Once all the ten rounds are complete, the values of all the factors and string can be saved to the database for further use. The system keeps updating its database with the applications used along with the date and time of each so that the authentication process 2 can be carried out smoothly. Two users may draw similar patterns but they cannot draw it the same way i.e. other factors cannot be same for two different users.

As figure 7.1 shows the procedure of recording of gesture pattern by a user repeated ten times. As the pattern is being drawn, the sting S, indicating the path of the pattern is generated. Along with that, highest pressure, velocity, area, time and position are been recorded with each iteration of entering the gesture pattern. The number of

iterations can even be reduced to three but more the number of iterations, more precisely is the system able to record the movements.

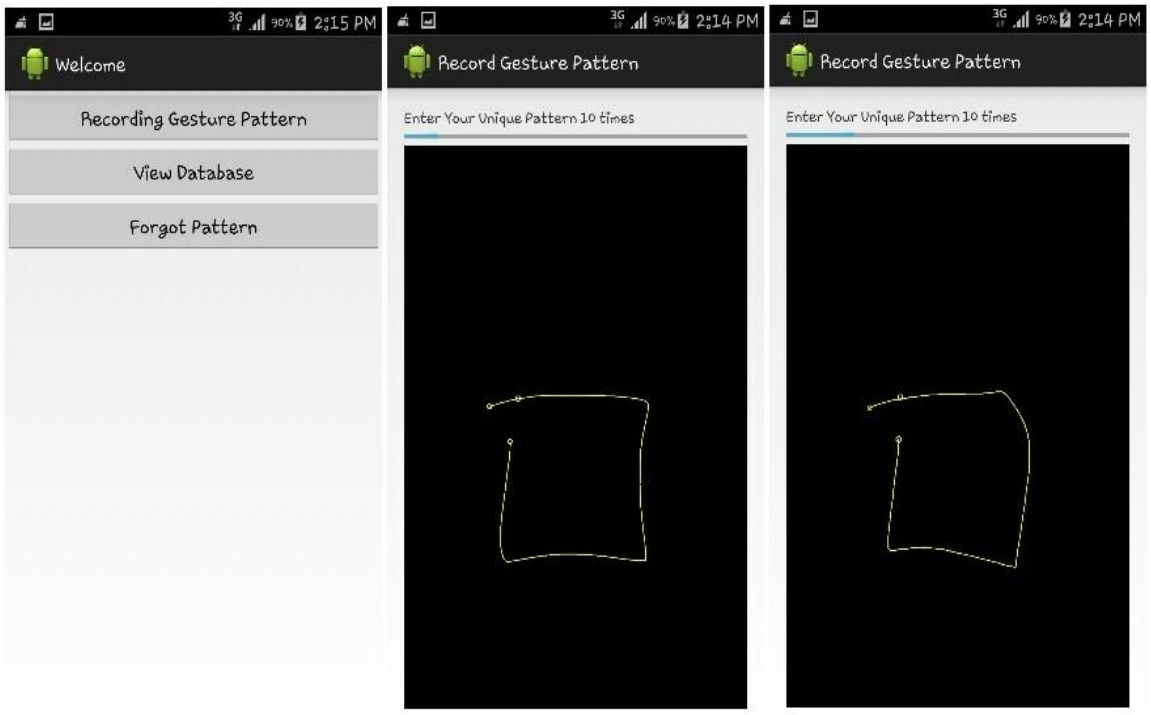

Figure 7.1.1 Stepwise recording of gesture pattern (A)

Figure 7.1.2 Stepwise recording of gesture pattern (B)

Figure 7.1.3 Stepwise recording of gesture pattern (C)

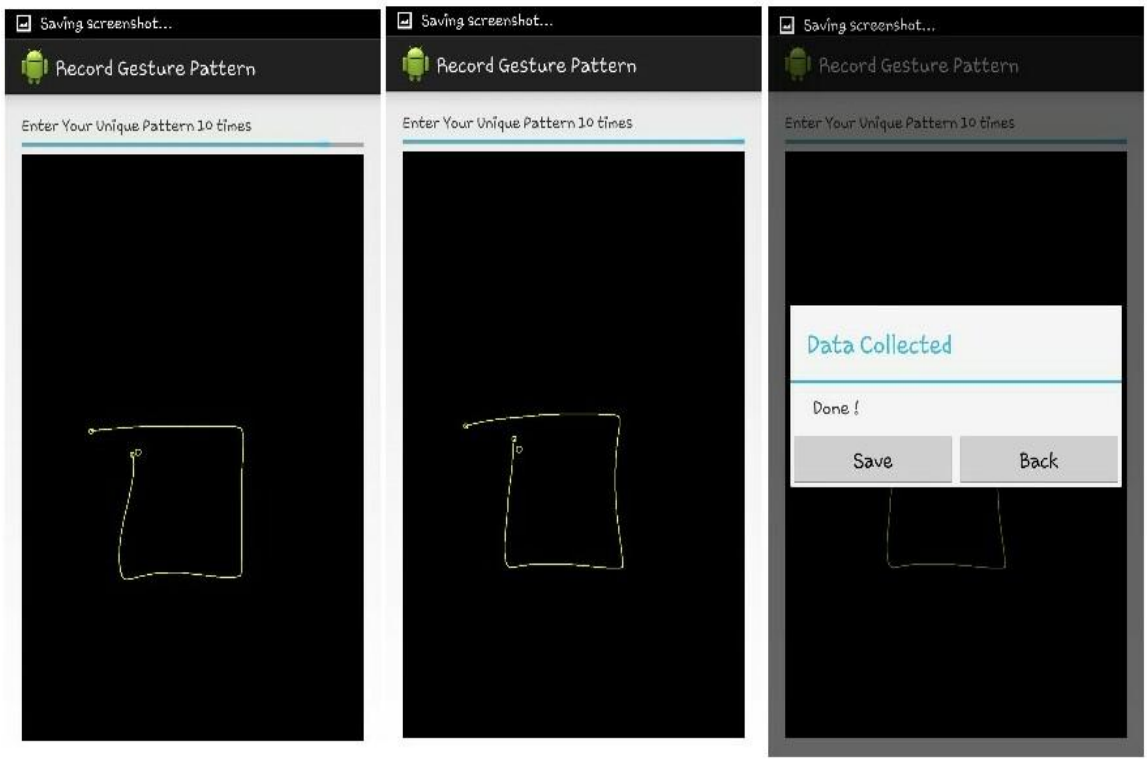

Figure 7.1.4 Stepwise recording of gesture pattern (D)

As soon as the user begins to draw the gesture pattern, the recording of all the behavioral gesture begins. Various users were made to enter these patterns ten times each. Each user

then entered the same pattern ten times with results as shown in section 7.2. This process was carried out on various users with android devices where each user tried to redraw its favorite pattern in almost same way as did for first time and the results of each were recorded and analyzed to find and frame some synaptic weight to each parameter to be used for recognizing an authorized user depending upon the reliability of each parameter that can be concluded by analyzing of the collected data. These fixed synaptic weights can then be assigned to the equation discussed in flowchart in figure 6.2.1 under the section 6.2 for calculating the value F and comparing it with F' calculated at the time someone tries to unlock the device.

7.2 Data Analysis and Interpretation

The data as shown in section 7.2 was collected from different users and results can were recorded that included the generated string S, time taken to draw the pattern T, in milliseconds, Area covered by the finger or the thumb while touching the screen at the time of drawing the pattern, pressure P exerted on the screen while drawing the pattern, velocity V at which pattern was drawn and the position of the screen where the pattern is drawn.

In each figure Time had been recorded in milliseconds, String has been generated as discussed in section 6.1, area has three values (a, b, c) with 'a' representing length of major axis of eclipse formed by area touching the screen with finger or thumb at starting point, 'b' representing length of major axis of eclipse formed by area touching the screen with finger or thumb at highest point of contact throughout the pattern making, 'c' is the length of major axis of eclipse formed by area touching the screen with finger or thumb at final point of pattern drawing. Pressure has three values (x, y, z) with 'x' representing pressure recorded while drawing with pen at starting point of pattern making, 'y' representing the highest pressure throughout the pattern drawing and 'z' representing the pressure at final pixel of pattern. Velocity is the speed at which the pattern is been drawn in pixels per second and location is the portion of the screen where the first pixel of pattern lies and may have values A, B, C, D, E or F as discussed in chapter 6 Research Methodology. Figure 7.2.1 to figure 7.2.6 are data for pattern been drawn using stick and figure 7.2.7 to figure 7.2.12 are data for pattern been drawn using finger or thumb. Area values for pattern drawn with stick has no values as no eclipse is been formed. Similarly pressure values for patterns drawn using thumb are been rounded off to maximum i.e.1.0.

Time	String	Area	Presure	Velocity	Location
782	23687474	0 , 0 , 0	0.148 , 0.28 , 0.23	61.0 p/s	E
700	23687474	0 , 0 , 0	0.176 , 0.28 , 0.12	61.0 p/s	E
700	236874	0 , 0 , 0	0.21 , 0.31 , 0.12	61.0 p/s	E
601	26874	0 , 0 , 0	0.178 , 0.31 , 0.01	63.0 p/s	E
618	236874	0 , 0 , 0	0.157 , 0.31 , 0.21	63.0 p/s	E
647	2369874	0 , 0 , 0	0.204 , 0.33 , 0.21	61.0 p/s	E
641	236874	0 , 0 , 0	0.204 , 0.33 , 0.17	60.0 p/s	E
626	232369874	0 , 0 , 0	0.204 , 0.33 , 0.22	62.0 p/s	E
679	232369874	0 , 0 , 0	0.166 , 0.33 , 0.11	60.0 p/s	E
602	236874	0 , 0 , 0	0.173 , 0.33 , 0.21	63.0 p/s	E

Figure 7.2.1 Gesture pattern data of user 1

Time	String	Area	Presure	Velocity	Location
686	64747476	0 , 0 , 0	0.146 , 0.27 , 0.22	62.0 p/s	A
579	64786	0 , 0 , 0	0.105 , 0.27 , 0.05	62.0 p/s	C
526	6474746	0 , 0 , 0	0.105 , 0.27 , 0.09	62.0 p/s	C
551	64747476	0 , 0 , 0	0.121 , 0.27 , 0.08	61.0 p/s	C
536	64746	0 , 0 , 0	0.137 , 0.27 , 0.13	63.0 p/s	C
528	6747476	0 , 0 , 0	0.14 , 0.27 , 0.16	62.0 p/s	C
580	647476	0 , 0 , 0	0.105 , 0.27 , 0.06	62.0 p/s	C
504	3647476	0 , 0 , 0	0.11 , 0.27 , 0.12	63.0 p/s	C
429	6476	0 , 0 , 0	0.136 , 0.27 , 0.18	65.0 p/s	C
493	676	0 , 0 , 0	0.112 , 0.27 , 0.15	62.0 p/s	C

Figure 7.2.2 Gesture pattern data of user 2

Figure 7.2.1 and figure 7.2.2 contains data recorded by user 1 and user 2 respectively while they try to draw pattern of their choice using stick. Time, Pattern path, pressure, velocity and location have been recorded for same. Values for area are absent since stick covers no significant area while making the pattern. Location refers to the portion of the screen where the starting pixel of the pattern lies as discussed in figure 6.6 and time has been recorded with each attempt in milliseconds. Also velocity has been recorded in pixels per second for each iterative attempt.

Time	String	Area	Presure	Velocity	Location
701	323214789	0 , 0 , 0	0.107 , 0.27 , 0.04	61.0 p/s	E
684	3247896	0 , 0 , 0	0.142 , 0.29 , 0.07	61.0 p/s	E
625	3247896	0 , 0 , 0	0.173 , 0.29 , 0.2	62.0 p/s	E
557	324789	0 , 0 , 0	0.172 , 0.29 , 0.23	62.0 p/s	E
550	324789	0 , 0 , 0	0.213 , 0.29 , 0.03	63.0 p/s	E
505	324789	0 , 0 , 0	0.155 , 0.29 , 0.12	61.0 p/s	E
536	324789	0 , 0 , 0	0.191 , 0.31 , 0.18	63.0 p/s	E
581	3247898	0 , 0 , 0	0.133 , 0.31 , 0.22	61.0 p/s	E
596	3247896	0 , 0 , 0	0.208 , 0.31 , 0.17	63.0 p/s	E
513	324789	0 , 0 , 0	0.171 , 0.32 , 0.04	64.0 p/s	E

Figure 7.2.3 Gesture pattern data of user 3

Time	String	Area	Presure	Velocity	Location
664	23238	0 , 0 , 0	0.165 , 0.26 , 0.04	61.0 p/s	E
556	23238	0 , 0 , 0	0.156 , 0.26 , 0.17	62.0 p/s	C
437	238	0 , 0 , 0	0.194 , 0.26 , 0.08	64.0 p/s	C
437	23686	0 , 0 , 0	0.141 , 0.26 , 0.18	61.0 p/s	C
437	23289	0 , 0 , 0	0.184 , 0.29 , 0.24	64.0 p/s	C
461	23268	0 , 0 , 0	0.19 , 0.29 , 0.06	62.0 p/s	C
436	23232898	0 , 0 , 0	0.218 , 0.4 , 0.19	64.0 p/s	C
469	2989	0 , 0 , 0	0.185 , 0.4 , 0.18	63.0 p/s	C
434	289	0 , 0 , 0	0.201 , 0.4 , 0.2	64.0 p/s	C
467	2898	0 , 0 , 0	0.168 , 0.4 , 0.17	64.0 p/s	C

Figure 7.2.4 Gesture pattern data of user 4

Figure 7.2.3 and figure 7.2.4 contains data recorded by user 3 and user 4 respectively while they try to draw pattern of their choice using stick. Time, Pattern path, pressure, velocity and location have been recorded for same. Values for area are absent since stick covers no significant area while making the pattern. Location refers to the portion of the screen where the starting pixel of the pattern lies as discussed in figure 6.6 and time has been recorded with each attempt in milliseconds. Also velocity has been recorded in pixels per second for each iterative attempt.

Time	String	Area	Presure	Velocity	Location
982	4232324789869	0 , 0 , 0	0.127 , 0.38 , 0.24	61.0 p/s	D
828	423247896	0 , 0 , 0	0.095 , 0.38 , 0.19	61.0 p/s	D
793	42324789	0 , 0 , 0	0.103 , 0.39 , 0.03	61.0 p/s	D
783	432147898	0 , 0 , 0	0.088 , 0.39 , 0.09	61.0 p/s	D
775	43247898	0 , 0 , 0	0.145 , 0.41 , 0.25	60.0 p/s	D
738	42324789	0 , 0 , 0	0.154 , 0.44 , 0.17	60.0 p/s	D
730	42324747898	0 , 0 , 0	0.129 , 0.44 , 0.15	61.0 p/s	D
799	42324789898	0 , 0 , 0	0.108 , 0.44 , 0.07	61.0 p/s	D
700	4232489	0 , 0 , 0	0.211 , 0.44 , 0.27	61.0 p/s	D
724	4324747898	0 , 0 , 0	0.196 , 0.44 , 0.01	62.0 p/s	D

Figure 7.2.5 Gesture pattern data of user 5

Time	String	Area	Presure	Velocity	Location
867	47869874	0 , 0 , 0	0.155 , 0.35 , 0.08	59.0 p/s	B
872	4869841	0 , 0 , 0	0.17 , 0.35 , 0.12	60.0 p/s	B
813	489698742	0 , 0 , 0	0.189 , 0.35 , 0.22	61.0 p/s	B
828	4786984	0 , 0 , 0	0.184 , 0.35 , 0.26	61.0 p/s	B
730	48696841	0 , 0 , 0	0.214 , 0.35 , 0.24	60.0 p/s	B
669	4789698414	0 , 0 , 0	0.206 , 0.36 , 0.01	62.0 p/s	B
754	478969841	0 , 0 , 0	0.226 , 0.36 , 0.21	61.0 p/s	B
738	47869684	0 , 0 , 0	0.206 , 0.37 , 0.06	60.0 p/s	B
634	4789696984	0 , 0 , 0	0.238 , 0.37 , 0.2	61.0 p/s	B
662	4789696984	0 , 0 , 0	0.175 , 0.4 , 0.19	61.0 p/s	B

Figure 7.2.6 Gesture pattern data of user 6

Figure 7.2.5 and figure 7.2.6 contains data recorded by user 5 and user 6 respectively while they try to draw pattern of their choice using stick. Time, Pattern path, pressure, velocity and location have been recorded for same. Values for area are absent since stick covers no significant area while making the pattern. Location refers to the portion of the screen where the starting pixel of the pattern lies as discussed in figure 6.6 and time has been recorded with each attempt in milliseconds. Also velocity has been recorded in pixels per second for each iterative attempt.

Time	String	Area	Presure	Velocity	Location
841	47647896	7 , 12 , 9	1.0 , 1.0 , 1.0	60.0 p/s	B
872	489647896	9 , 13 , 6	1.0 , 1.0 , 1.0	60.0 p/s	B
843	489647896	9 , 13 , 7	1.0 , 1.0 , 1.0	58.0 p/s	B
812	4789647896	8 , 13 , 6	1.0 , 1.0 , 1.0	59.0 p/s	B
801	4764786	10 , 15 , 6	1.0 , 1.0 , 1.0	58.0 p/s	B
783	4786364786	11 , 15 , 6	1.0 , 1.0 , 1.0	60.0 p/s	B
793	478963647896	8 , 15 , 9	1.0 , 1.0 , 1.0	60.0 p/s	B
789	4786367896	9 , 15 , 6	1.0 , 1.0 , 1.0	60.0 p/s	B
730	47636786	8 , 15 , 5	1.0 , 1.0 , 1.0	60.0 p/s	B
769	4786786	9 , 15 , 6	1.0 , 1.0 , 1.0	59.0 p/s	B

Figure 7.2.7 Gesture pattern data of user 7

Time	String	Area	Presure	Velocity	Location
2645	8	5 , 9 , 8	1.0 , 1.0 , 1.0	51.0 p/s	A
2125	868	7 , 9 , 5	1.0 , 1.0 , 1.0	53.0 p/s	A
2170	868	8 , 9 , 7	1.0 , 1.0 , 1.0	52.0 p/s	A
1934	868	6 , 10 , 6	1.0 , 1.0 , 1.0	54.0 p/s	B
1560	868	6 , 10 , 5	1.0 , 1.0 , 1.0	57.0 p/s	B
1474	868	6 , 10 , 5	1.0 , 1.0 , 1.0	56.0 p/s	B
1432	868	6 , 10 , 5	1.0 , 1.0 , 1.0	56.0 p/s	B
1275	878628	5 , 10 , 6	1.0 , 1.0 , 1.0	57.0 p/s	B
826	7868	8 , 10 , 4	1.0 , 1.0 , 1.0	59.0 p/s	B
1218	8628	9 , 10 , 5	1.0 , 1.0 , 1.0	56.0 p/s	B

Figure 7.2.8 Gesture pattern data of user 8

Figure 7.2.7 and figure 7.2.8 contains data recorded by user 7 and user 8 respectively while they try to draw pattern of their choice using their finger. Time, Pattern path, area, velocity and location have been recorded for same. Values for pressure are full since finger covers large area while making the pattern and pressure cannot be sensed. Location refers to the portion of the screen where the starting pixel of the pattern lies as discussed in figure 6.6 and time has been recorded with each attempt in milliseconds. Also velocity has been recorded in pixels per second for each iterative attempt.

Time	String	Area	Presure	Velocity	Location
893	47636878	7 , 11 , 8	1.0 , 1.0 , 1.0	59.0 p/s	B
559	47863678	9 , 14 , 5	1.0 , 1.0 , 1.0	60.0 p/s	B
501	478378	10 , 14 , 6	1.0 , 1.0 , 1.0	61.0 p/s	B
525	786378	9 , 17 , 13	1.0 , 1.0 , 1.0	60.0 p/s	B
544	478378	9 , 17 , 9	1.0 , 1.0 , 1.0	62.0 p/s	B
515	4783678	9 , 17 , 9	1.0 , 1.0 , 1.0	60.0 p/s	B
549	78378	10 , 17 , 11	1.0 , 1.0 , 1.0	61.0 p/s	B
492	7837	10 , 17 , 12	1.0 , 1.0 , 1.0	60.0 p/s	B
531	783678	9 , 17 , 10	1.0 , 1.0 , 1.0	54.0 p/s	B
605	7832789	9 , 18 , 15	1.0 , 1.0 , 1.0	61.0 p/s	B

Figure 7.2.9 Gesture pattern data of user 9

Time	String	Area	Presure	Velocity	Location
423	232323	26 , 40 , 21	1.0 , 1.0 , 1.0	59.0 p/s	E
333	23	13 , 40 , 5	1.0 , 1.0 , 1.0	63.0 p/s	E
348	23	17 , 40 , 8	1.0 , 1.0 , 1.0	63.0 p/s	E
355	23	17 , 40 , 8	1.0 , 1.0 , 1.0	61.0 p/s	E
348	23	13 , 40 , 12	1.0 , 1.0 , 1.0	63.0 p/s	E
394	23	16 , 40 , 7	1.0 , 1.0 , 1.0	58.0 p/s	E
414	23	20 , 40 , 10	1.0 , 1.0 , 1.0	57.0 p/s	E
414	23	15 , 40 , 7	1.0 , 1.0 , 1.0	62.0 p/s	E
459	2323	15 , 40 , 11	1.0 , 1.0 , 1.0	58.0 p/s	E
371	23	17 , 40 , 9	1.0 , 1.0 , 1.0	61.0 p/s	E

Figure 7.2.10 Gesture pattern data of user 10

Figure 7.2.9 and figure 7.2.10 contains data recorded by user 9 and user 10 respectively while they try to draw pattern of their choice using their finger. Time, Pattern path, area, velocity and location have been recorded for same. Values for pressure are full since finger covers large area while making the pattern and pressure cannot be sensed. Values for pressure are full since finger covers large area while making the pattern and pressure cannot be sensed. Location refers to the portion of the screen where the starting pixel of the pattern lies as discussed in figure 6.6 and time has been recorded with each attempt in milliseconds. Also velocity has been recorded in pixels per second for each iterative attempt.

Time	String	Area	Presure	Velocity	Location
1713	2687968	8 , 12 , 6	1.0 , 1.0 , 1.0	58.0 p/s	A
1646	826878	7 , 12 , 8	1.0 , 1.0 , 1.0	56.0 p/s	A
1866	8232687878	8 , 13 , 8	1.0 , 1.0 , 1.0	58.0 p/s	A
1491	8232874898	9 , 13 , 6	1.0 , 1.0 , 1.0	54.0 p/s	A
1353	87823236368748	9 , 13 , 5	1.0 , 1.0 , 1.0	53.0 p/s	A
1442	826878	8 , 14 , 8	1.0 , 1.0 , 1.0	58.0 p/s	A
1300	823687898	8 , 14 , 6	1.0 , 1.0 , 1.0	57.0 p/s	A
1272	8267898	8 , 14 , 8	1.0 , 1.0 , 1.0	58.0 p/s	A
1207	82368748	9 , 14 , 5	1.0 , 1.0 , 1.0	56.0 p/s	A
1094	8238789898	9 , 14 , 8	1.0 , 1.0 , 1.0	59.0 p/s	A

Figure 7.2.11 Gesture pattern data of user 11

Time	String	Area	Presure	Velocity	Location
529	83	5 , 9 , 5	1.0 , 1.0 , 1.0	60.0 p/s	A
582	8232	7 , 9 , 6	1.0 , 1.0 , 1.0	61.0 p/s	A
548	83	5 , 10 , 7	1.0 , 1.0 , 1.0	62.0 p/s	A
587	83	6 , 10 , 9	1.0 , 1.0 , 1.0	61.0 p/s	A
528	863	6 , 10 , 9	1.0 , 1.0 , 1.0	62.0 p/s	A
476	832	10 , 11 , 5	1.0 , 1.0 , 1.0	63.0 p/s	A
499	8632	8 , 12 , 5	1.0 , 1.0 , 1.0	60.0 p/s	A
439	83	9 , 12 , 9	1.0 , 1.0 , 1.0	63.0 p/s	A
429	83	9 , 12 , 10	1.0 , 1.0 , 1.0	62.0 p/s	A
434	83	9 , 12 , 8	1.0 , 1.0 , 1.0	62.0 p/s	A

Figure 7.2.12 Gesture pattern data of user 12

Figure 7.2.11 and figure 7.2.12 contains data recorded by user 11 and user 12 respectively while they try to draw pattern of their choice using their finger. Time, Pattern path, area, velocity and location have been recorded for same. Values for pressure are full since finger covers large area while making the pattern and pressure cannot be sensed. Values for pressure are full since finger covers large area while making the pattern and pressure cannot be sensed. Location refers to the portion of the screen where the starting pixel of the pattern lies as discussed in figure 6.6 and time has been recorded with each attempt in milliseconds. Also velocity has been recorded in pixels per second for each iterative attempt.

Along with gesture pattern recording, authentication process 2, as discussed in chapter 6 Research Methodology, was also tested with a round of three questions being asked from each user if he is unable to redraw the pattern with same gesture as recorded. The basic applications of any android device have been used for this purpose namely call, message and used applications. The question being asked in round 1 is always from contacts and call log. The question being asked in round 2 is always from messaging application. And the question being asked in round 3 is about the applications being used. These activities of user are being recorded while he uses the device. Since the fundamental applications are being used, these can easily be used in any device. Other fundamental applications can also be used for this purpose depending upon the device brand.

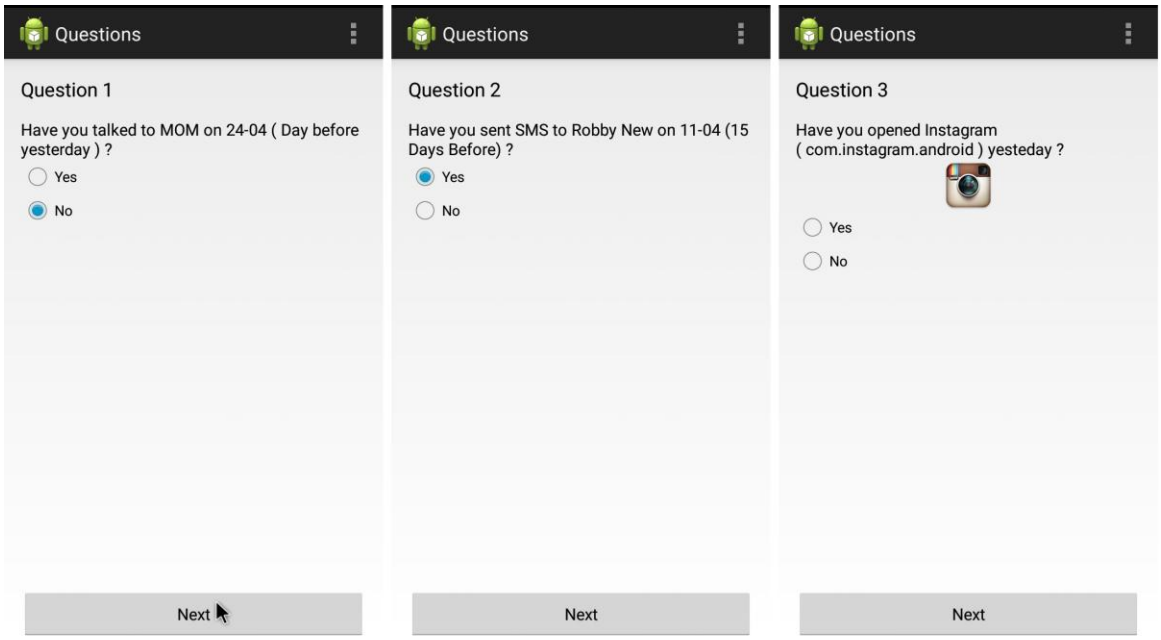

Figure 7.2.13 Authentication Process 2 example

If user successfully answers all the rounds correctly, it is considered that the user is authorized since only an authorized user can remember its activities. It was taken into consideration that questions are being formed only about the activities of last fifteen days since it becomes difficult to remember activities past fortnight. If any of the answer goes wrong, the user is considered unauthorized and the application moves back to the pattern drawing mechanism. This procedure happens for three times. If the user is unable to pass through any of this correctly, the process pauses for some time.

7.3 Performance Evaluation

It is clear from the data in section 7.2 that the system is reliable and serves to be easier and secure than the previously existing authentication methods. A quick review of comparison with existing methods can be seen in table 7.1

Lock Type / Performance	Time Consumed	Ease of Remembering	Security	Reliable	Cost
Pin Lock	Average	Low	Low	High	Low
Password	Average	Low	Average	High	Low
Patern Lock	Low	High	Low	High	Low
Face Lock	High	High	High	Low	High
Finger Print	High	High	High	Average	High
Voice Lock	High	High	High	Low	High
Graphical Lock	Average	Average	Average	Low	Average
BB Lock	Low	Average	High	Average	Low

Table 7.1 Comparison with existing lock types

In table 7.1, time consumed is the time taken while entering the key that may be a password or a pattern or any input key. This is an important factor as the system should not be time consuming and frustrating as discussed through statistics in chapter 1 Introduction of this report. Ease of Remembering is another important factor when it comes to use a user authentication system in devices such as smart phones which is very frequent as discussed in chapter 1 of this report. Security is the main factor as discussed in this report since smart phones contain sensitive data and thus authentication is required. Reliability is the factor discussing the number of times an authentic user is granted access i.e the factor telling the correctness of the system. Cost is also another factor that needs to be kept in mind so that no specific special hardware is required for providing high security.

Chapter 8
CONCLUSION AND FUTURE SCOPE

8.1 Conclusion

According to studies, more than half of smart phone users do not use any authentication method for their devices complaining that the existing methods are difficult to remember and time consuming. Moreover, it can be seen that a weak password is easy to hack and complex ones are difficult to remember. Security is compromised with usability when the frequency of using the device is high as in smart phones. The concept of biometrics claims to be more reliable and secure as it is almost impossible for two different users to have same physical or behavioral traits. Since implementing user authentication based on physical biometrics is costly in terms that it requires special hardware, behavioral biometric based scheme has been proposed in this report. There is a strong need of a mechanism that is quick, secure and easy at the same time i.e. a smarter way of authentication is required. In this report, a behavioral biometric based password scheme has been discussed that can be implemented on graphical pattern drawing just like a swipe performed on glass lock. The objective of this study is to provide a secure, cheap, easy and quick user authentication scheme. It is expected that the proposed solution would serve smart phone users worldwide.

As the experiment and results have shown, parameters such as time, velocity, position and area are quite reliable when it comes to the habits or behavior of a user while other factors can be given less weights while comparison. It is clear from the recorded data that biggest area of touch, highest point of pressure, time and velocity can be given high consideration while comparing whether the user is authentic or not. Behavioral biometrics play a big role in identification of user as it is very difficult to copy the gesture habits of some other person. Also, the recovery process of the discussed scheme is much simple and easy as per user's point of view but since it is time taking, it cannot be used in the first place. So, keeping in mind the ease for users at first priority, authentication process 2 has been used as process for recovery and BBlock as the default authentication scheme. Thus, it proves to be a better factor for identification especially when it comes to smart phones as it is easier, faster, cheap and reliable.

8.2 Future Scope

The implemented system in this research makes use of graphical password scheme along with behavioral biometrics. This serves to be a better system in terms of ease and reliability. This system can be made more user-friendly if concepts of neural network are added to it for making it more adaptive with the changing habits of user with time. Neural networks is a branch of intelligent systems that helps make the system work more like a human brain and makes it more adaptive. This can be added to the system and identification of authorization of user can be done using clustering. Scope of this scheme can be extended to all the future touch sensitive devices. Also, Machine learning and neural network concepts, together if applied to this system may help in big improvement in this system by making it much more reliable and secure. Fuzzy membership functions can also be assigned to each of the parameters depending upon their reliability varying from person to person thus improving the system to a great extent.

Chapter 9
LIST OF REFERENCES

I. Books

- Reto Meier, *Professional Android 4 Application Development*, Wrox
- Neil Smyth, Techotopia, *Android 4.2 App Development Essentials – First Edition*
- Stan Z. Li, *Encyclopedia of Biometrics*, Springer Science & Business Media

II. Research Papers

- Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, and Xiyang Liu, (2008), "*YAGP: Yet Another Graphical Password Strategy*", Annual Computer Security Applications Conference
- Xi Zhao, Tao Feng And Weidong Shi (2013), "*Continuous Mobile Authentication Using A Novel Graphic Touch Gesture Feature*", Applications and Systems (BTAS),IEEE Sixth International Conference
- Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang (2011), "*A Graphical Password Based System for Small Mobile Devices*",IJCSI International Journal of Computer Science Issues
- Ziming Zhao, Gail-Joon Ahn, Jeong-Jin Seo and Hongxin Hu (2013) , "*On the Security of Picture Gesture Authentication*", 22ND USENIX Security Symposium
- Kwang Il Shin, Ji Soo Park, Jae Yong Lee and Jong Hyuk Park (2012), "*Design and Implementation of Improved Authentication System for Android Smartphone Users*", 26th International Conference on Advanced Information Networking and Applications Workshops
- Imran M. Khan, Imama, K.M. Ushama, M. Abiniu , Lai Weng Kin and C. P. Lim (2011), "*Evaluation of Classifiers in a Pressure and Latency-Based Typing Biometric System"*, 4th International Conference on Mechatronics (ICOM)
- Mike Just (2014), "*Authentication Frequency as an Important Design Factor*" Symposium on Usable Privacy and Security (SOUPS)

- Akane Ito, Yui Ohtaka, Yoshie Yamada, Manabu Okamoto (2014), "*Input Password Only with Four Keys, Three Times*" Symposium on Usable Privacy and Security (SOUPS)
- Grover Aman, Narang Winnie (2012), *"4-D Password: Strengthening the Authentication Scene*", International Journal of Scientific & Engineering Research
- E. Shi, Y. Niu, M. Jakobsson, and R. Chow (2010), *"Implicit authentication through learning user behavior*". In M. Burmester, G. Tsudik, S. S. Magliveras, and I. Ilic, editors, ISC, volume 6531 of Lecture Notes in Computer Science,
- Beum Su Park (2011), "*Password Input method using authentication Pattern and Puzzle*" Computer Sciences and Convergence Information Technology (ICCIT), 6th International Conference
- Jeremiah Blocki (2013), GOTCHA Password Hackers, Proceedings of the 2013 ACM workshop on Artificial intelligence and security

III. Websites

- http://passwordresearch.com/stats/statindex.html
- http://www.ieee-security.org/TC/SPW2013/papers/data/5017a173
- http://www.ieee-security.org/TC/SP2011/PAPERS/2011/paper007
- http://www.go-gulf.com/blog/cyber-crime/
- https://developer.android.com/training/index.html
- http://www.adtechglobal.com/Data/Sites/1/marketing/juniperwhitepapermobiledevicesecurity