



# **SECURING ONLINE TRANSACTION BIOMETRICS IN MOBILE PHONE**

## **A PROJECT REPORT**

*Submitted by*

<b>ANANDAPADMANABHAN.G</b>	<b>950816104004</b>
<b>MICHAEL AMALAN.J</b>	<b>950816104031</b>
<b>SANTHOSH KUMAR.A</b>	<b>950816104045</b>
<b>SATHYAGIRI.V</b>	<b>950816105046</b>

*in partial fulfilment for the award of the degree*

*of*

**BACHELOR OF ENGINEERING**

**in**

**COMPUTER SCIENCE AND ENGINEERING**

**GOVERNMENT COLLEGE OF ENGINEERING, TIRUNELVELI**

**ANNA UNIVERSITY: CHENNAI 600 025**

**APRIL 2020**

## **BONAFIDE CERTIFICATE**

Certified that this project report “**SECURING ONLINE TRANSACTION BIOMETRICS IN MOBILE PHONE**” is the bonafide work of  
“**G.ANANDAPADMANABHAN , J.MICHAEL AMALAN, A.SANTHOSH KUMAR, V.SATHYAGIRI**” who carried out the project work  
under my supervision.

**SIGNATURE,**  
**Dr.G.TAMILPAVAL,M.E.,Ph.D.,**  
**HEAD OF THE DEPARTMENT,**  
Dept. of Computer Science and Engg.  
Government College of Engineering,  
Tirunelveli-627007.

**SIGNATURE,**  
**Prof.N.JEENATH LAILA,M.E.,**  
**ASSISTANT PROFESSOR,**  
Dept. of Computer Science and Engg.  
Government College of Engineering,  
Tirunelveli-627007.

Submitted for project **Viva- Voce** held at Government College of Engineering  
Tirunelveli on \_\_\_\_\_.

**Internal Examiner**

**External Examiner**

## **ACKNOWLEDGEMENT**

First And foremost we thank GOD the glorious almighty for enabling us to complete the project successfully.

We render special thanks to Dr.M.NATARAJ M.E,Ph.D Principal of Government College of Engineering, Tirunelveli for permitting us to do this project successfully.

We are grateful to Dr. G.TAMIL PAVAI M.E., Ph.D., MISTE , Head of the Department, Computer Science and Engineering Department, whose moral support has been inspiring.

I take this opportunity to express my thanks to my guide

Mrs. N.JEENATH LAILA M.E., Assistant Professor, for her encouragement and valuable support in completing this project work in time. I would also like to thank faculty adviser of our department

Mrs. M.MAHIL M.E., Assistant Professor, Department of Computer Science & Engineering for their valuable suggestions in bringing out this project successfully.

We sincerely thank all the teaching and non-teaching staff members of this department for their assistance in completing our project.

Finally, we thank our family members and friends for their co-operation and selfless help and support.

## **ABSTRACT**

Owing to a lot of hacks and other security concerns with respect to the card payment system, biometrics is next in line as the authentication module for payment systems. The hassle the user has to put up with in a card payment system by having to carry different cards and having to remember passwords is appalling and losing the card is another issue altogether. Usually fingerprints are used to authenticate the card and pin number that have been entered. The system has been designed to let customers pay the bills using only in registered mobile number and fingerprint. In this paper, it is developed as a simulation of an android application that is used on the sales side to emulate the process of authenticating a user using the fingerprint to let the access on prepaid balance and make the payment to the retail store.

## TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	Acknowledgement	ii
	Abstract	iii
	List of figures	vi
<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
<b>2</b>	<b>LITERATURE SURVEY</b>	<b>9</b>
<b>3</b>	<b>PROBLEM ANALYSIS</b>	<b>10</b>
	EXISTING SYSTEM	10
	PROPOSED SYSTEM	10
	BLOCK DIAGRAM	11
<b>4</b>	<b>REQUIREMENTS SPECIFICATION</b>	<b>13</b>
	INTRODUCTION	13
	HARDWARE REQUIREMENTS	13
	SOFTWARE REQUIREMENTS	13
<b>5</b>	<b>METHODOLOGY</b>	
	<b>LIST OF MODULES</b>	
	FINGERPRINT MATCHING	
	ALGORITHMS	17
	MINUTIAE EXTRACTION AND	
	MATCHING ALGORITHMS	20
	THRESHOLD CRYPTOGRAPHY	
	TECHNIQUE	23
	AUTOMATED IDENTIFICATION	25

	PERFORMANCE ANALYSIS	31
6	RESULTS	32
7	CONCLUSION	45
8	REFERENCES	46

## **LIST OF FIGURES**

<b>FIG NO.</b>	<b>FIGURE NAME</b>	<b>PAGENO</b>
3.1	Proposed blockdiagram	11
3.2	Application	12
4.1	Fingerprint Scanner	15
4.2	End to end Authentication Security	16
5.1	Fingerprint Recognition Process	19
5.2	Minutiae found on the fingerprint image	28
5.3	Determination Of Color	29
5.4	Color of minutae	30
6.1	Add money Screen	31
6.2	Home screen after adding money	32
6.3	Account identification by fingerprint	33
6.4	Matched account page	34
6.5	Transfer success page	35
6.6	Post Transaction success page	36
6.7	Service registration page	37
6.8	Service screen	38

6.9	Login screen	39
6.10	Initial balance screen page	40
6.11	Money transfer page	41
6.11	Balance after money transfer	42
6.12	Money transfer success	43



# **CHAPTER 1**

## **INTRODUCTION**

With the advancement of science and technology our daily activities have become faster and easier at the cost of having complex tools and technologies. The online banking transactions are part of daily routine for an individual. The existing online banking system has several drawbacks. Firstly hacking, from the internet any one can hack the username and password and the result is third person gets access to owner account. As anyone is not with twenty four hours on the Internet, i.e. access bank website, it takes some time to know that your account get hacked and third one can get transfer the money to his own account. Secondly, every time one has to carry laptop or PC with you. So for this issue secured payment applications on mobile device i.e. M-commerce is proposed.

Today is the era of mobile, everyone having the mobile in his hands, instead of using the laptop or PC, mobile is the best option to use for the banking purpose. The next generation of banking applications won't be on desktops or mainframes but on the small mobile devices we carry every day. Secured e-banking on the mobile is the latest issue for all mobile users. M-commerce, in the context, provides a lot of services like Mobile ticketing, Mobile banking, Mobile location based services, Mobile auctions, Mobile purchasing and so on.

Mobile devices are rapidly becoming a key computing platform, transforming how people access business and personal information. Access to business data from mobile devices requires secure authentication. Authentication is the act of verifying that an individual is who he claims to be. Today we're using usernames and passwords, but passwords are weak in that many people write them down, or forget them. Passwords may be captured by spyware or Trojan horses on an infected computer and they are easy to guess.

The ease of guessing depends on the password strength, which is up to the user to define. Traditional authentication systems require the user perform the cumbersome task of memorizing numerous passwords, personal identification numbers, pass-phrases, and answers to secret questions etc. in order to access various databases and systems. More often, it becomes almost impossible to the different formats due to case sensitivity, requirement of alphanumeric text, and the necessity to change passwords or pass-phrases periodically to prevent from accidental compromise or theft. Many users choose passwords to be part of their names, phone numbers, or something which can be guessed. Moreover, to handle the hard task of remembering so many passwords, people tend to write them in files, and conspicuous places such as desk calendars, which expose chances of security violation.

Another authentication approach is biometrics, which is a way of authentication through something your body is or can do, rather than something as password. Biometric authentication is the process of verifying if a user or identity is who they claim to be using digitized biological pieces of the user. It comes in all sorts of flavors fingerprint, iris scan, hand geometry, face recognition, voice recognition, handwriting and typing dynamics -most of these have different variants. Generally speaking, there are four factors of physical attributes that are used or can be used in user authentication:

- Finger print scans, which have been in use for many years by law enforcement and other government agencies and is regarded as a reliable, unique identifier.
- Retina or iris scans, which have been used to confirm a person identity by analyzing the arrangement of blood vessels in the retina or patterns of color in the iris.
- Voice recognition, which uses a voice print that analyses how a person says a particular word or sequence of words unique to that individual.
- Facial recognition, which use unique facial features to identify an individual.

#### Finger print based on Transaction:

Biometrics is the measure and activity to analyze the people's physical and behavioral characteristics. It helps in identifying a particular person and to provide access or control to a particular activity of an individual. Every human being is unique and can be recognized by his traits. Biometric payments will become the buzz word in the near future. Biometric payments is highly secured, user friendly and it eradicates the fraudulent payment transactions. It as well frees the individual by carrying payment cards during biometric payments. In the recent days, almost all the individuals use many credit and debit cards for transactions. The major setback in using this card is the individual should remember the secret codes or passwords of all the cards that they use. Alternatively, in the case of our proposed design since the biometric system is used the verification is done on one to one basis. The trained data which is in encrypted form will be stored in the database. After verification of the database with the captured biometric data then the person will be going for an easy payments.

## **CHAPTER 2**

### **LITERATURE SURVEY**

**[1] MangalaBelkhede\*, VeenaGulhane\*\*, Dr. Preeti Bajaj\*\*\* “Biometric Mechanism for enhanced Security of Online Transaction on Android system: A Design Approach” ISBN 978-89-5519-163-9, Feb. 19~22, 2012 ICACT2012**

The next generation of banking applications won't be on desktop or mainframes but on the small devices we carry every day. Secured e banking on the mobile is the latest issue for all mobile users. In this paper authors have focused on, how biometric mechanism provides the highest security to the mobile payment. The present security issues surround the loss of personal information through the theft of the cell phone.

**[2] Fahad Al-harby, Rami Qahwaji, and Mumtaz Kamala “Secure Biometrics Authentication: A brief review of the Literature”**

This project presents a brief overview of the literature in the field of Biometrics authentication, The advent of the Internet saw technological innovations such as Biometrics device, in particular fingerprint reader, as an electronic equivalent to manuscript authentication in the online environment. However, the use of this technology is still insignificant. The aim of this project is to review the various studies that have explored the technical and legal issues associated with Biometrics authentication with an objective to provide insights on their lack of acceptance.

**[3] UdayRajanna Ali Erol George Bebis” A comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion” Springer-Verlag London Limited 2009.**

Fingerprint classification represents an important preprocessing step in fingerprint identification, which can be very helpful in reducing the cost of searching large fingerprint databases. Over the past years, several different approaches have been proposed for extracting distinguishable features and improving classification performance. In this paper, we present a comparative study involving four different feature extraction methods for fingerprint classification and propose a rank-based fusion scheme for improving classification performance. Specifically, we have compared two well-known feature extraction methods based on orientation maps (OMs) and Gabor filters with two new methods based on "minutiae maps" and "orientation collinearity". Each feature extraction method was compared with each other using the NIST-4 database in terms of accuracy and time. Moreover, we have investigated the issue of improving classification performance using rank-level fusion. When evaluating each feature extraction method individually, OMs performed the best. Gabor features fell behind OMs mainly because their computation is sensitive to errors in localizing the registration point. When fusing the rankings of different classifiers, we found that combinations involving OMs improve performance, demonstrating the importance of orientation information for classification purposes. Overall, the best classification results were obtained by fusing orientation map with orientation collinearity classifiers.

**[4] Yager N, Amin A (2004) Fingerprint classification: a review. Pattern Anal Appl 7:77–93**

Biometrics is the automatic identification of an individual that is based on physiological or behavioural characteristics. Due to its security-related

applications and the current world political climate, biometrics is currently the subject of intense research by both private and academic institutions. Fingerprints are emerging as the most common and trusted biometric for personal identification. The main objective of this paper is to review the extensive research that has been done on fingerprint classification over the last four decades. In particular, it discusses the fingerprint features that are useful for distinguishing fingerprint classes and reviews the methods of classification that have been applied to the problem. Finally, it presents empirical results from the state of the art fingerprint classification systems that have been tested using the NIST Special Database 4.

**[5] Yager N, Amin A (2004) Fingerprint verification based on minutiae features: a review. Pattern Anal Appl 7:94–113.**

Fingerprints have been an invaluable tool for law enforcement and forensics for over a century, motivating research into automated fingerprint-based identification in the early 1960s. More recently, fingerprints have found an application in biometric systems. Biometrics is the automatic identification of an individual based on physiological or behavioral characteristics. Due to its security-related applications and the current world political climate, biometrics is presently the subject of intense research by private and academic institutions. Fingerprints are emerging as the most common and trusted biometric for personal identification. The main objective of this paper is to review the extensive research that has been done on automated fingerprint matching over the last four decades. In particular, the focus is on minutiae-based algorithms. Minutiae features contain most of a fingerprint's individuality, and are consequently the most important fingerprint feature for verification systems. Minutiae extraction, matching algorithms, and verification performance are discussed in detail, with open problems and future directions identified.

**[6] T. Ahonen, A. Hadid and M. Pietikainen, “Face recognition with local binary patterns”, European Conference on Computer Vision, Prague, 469–481, 2004.**

In this work, we present a novel approach to face recognition which considers both shape and texture information to represent face images. The face area is first divided into small regions from which Local Binary Pattern (LBP) histograms are extracted and concatenated into a single, spatially enhanced feature histogram efficiently representing the face image. The recognition is performed using a nearest neighbour classifier in the computed feature space with Chi square as a dissimilarity measure. Extensive experiments clearly show the superiority of the proposed scheme over all considered methods (PCA, Bayesian Intra/extra personal Classifier and Elastic Bunch Graph Matching) on FERET tests which include testing the robustness of the method against different facial expressions, lighting and aging of the subjects. In addition to its efficiency, the simplicity of the proposed method allows for very fast feature extraction.

**[7] John Daugman “New Methods in Iris Recognition” VOL. 37, NO. 5, OCTOBER 2007.**

This project presents the following four advances in iris recognition:

- 1) more disciplined methods for detecting and faithfully modeling the iris inner and outer boundaries with active contours, leading to more flexible embedded coordinate systems;
- 2) Fourier-based methods for solving problems in iris trigonometry and projective geometry, allowing off-axis gaze to be handled by detecting it and “rotating” the eye into orthographic perspective;

- 3) statistical inference methods for detecting and excluding eyelashes; and
- 4) exploration of score normalizations, depending on the amount of iris data that is available in images and the required scale of database search.

Statistical results are presented based on 200 billion iris cross-comparisons that were generated from 632 500 irises in the United Arab Emirates database to analyze the normalization issues raised in different regions of receiver operating characteristic curves.

**[8] Kawagoe M, Tojo A (1984) “Fingerprint pattern classification”. *Pattern Recognit* 17(3):295–303.**

This project presents a new method for fingerprint classification. In this method, fingerprint images are divided into  $32 \times 32$  sub regions to obtain direction pattern. Next, the relaxation smoothing process with singularity detection and convergence checking is performed. Starting from the singular regions found, feature parameters of the fingerprint are obtained by extracting major flow-line\* traces. The result of the experiments shows that this approach is capable of classifying fingerprint patterns into more than ten categories.

**[9] Dr. Manish Manoria,Ajit Kumar Shrivastava,Satyendra Singh Thakur,,DebuSinha.(2011)” Exploring the Prospect of Secure Biometric Cryptosystem using RSA for Blind Authentication.**

Information security is the primary goal for any information based system. In this work, we have combined RSA cryptography for securely deliver biometric information to destination and it can recover the original message, without destroying the data pattern. We have explored one of the most-efficient RSA encryption algorithm and its performance with biometric information (fingerprint) using MATLAB 7.5 and jdk1.6. Our research includes the



determination of appropriate key sizes and the evaluation of different matching schemes for the application of blind authentication. In our work the finger print matching performance is more than 90% with good security assurance.

**[10] System I. Iancu, N. Constantinescu, M. Colhon “Fingerprints Identification using a Fuzzy Logic” ISSN 1841-9836, E-ISSN 1841-9844 Vol. V (2010), No. 4, pp. 525-531.**

This project presents an optimized method to reduce the points number to be used in order to identify a person using fuzzy fingerprints. Two fingerprints are similar if  $n$  out of  $N$  points from the skin are identical. We discuss the criteria used for choosing these points. We also describe the properties of fuzzy logic and the classical methods applied on fingerprints. Our method compares two matching sets and selects the optimal set from these, using a fuzzy reasoning system. The advantage of our method with respect to the classical existing methods consists in a smaller number of calculations.

## **CHAPTER 3**

### **PROBLEM ANALYSIS**

#### **EXISTING SYSTEM:**

The Augmented Biometrics System is used with secure online transaction checks for different levels of security but it takes longer time for authentication. It has given an elaborative study on the review of biometric recognition techniques. The methodologies adopted cannot be utilized for any application oriented transactions. The implemented biometric system for authentication purpose and predominantly it has been deployed in various utility computing. But the main drawback in this method is the system has been incorporated with password based design. The review of transition to cashless economy deals with electronic payment system with minor level of security. It is designed as a mobile app which is widely used for online banking transactions and merchant payment system. As OTP alone used for authentication, the level of security provided for transaction is vulnerable to Denial of Service attacks. They analyzed all the biometric systems and concluded that finger print based system is user friendly and very less time consuming authentication.

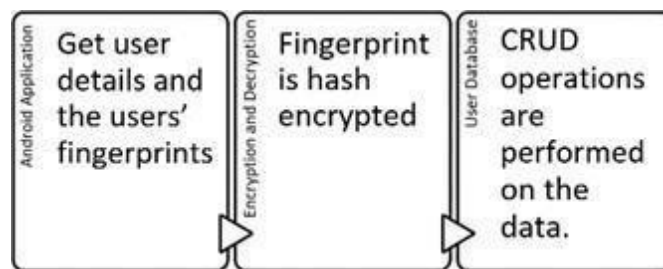
#### **PROPOSED SYSTEM:**

The proposed system lot of hacks and other security concerns with respect to the card payment system, biometrics is next in line as the authentication module for payment systems. The hassle the user has to put up with in a card payment system by having to carry different cards and having to remember passwords is appalling and losing the card is another issue altogether. Usually fingerprints are used to authenticate the card and pin number that have been entered. Our system has been designed to let customers pay the bills using only their registered mobile number and fingerprint. In this project, we have

developed a module of an android application that is used on the sales side to emulate the process of authenticating a user using his fingerprint to let him access his prepaid balance and make his payment to the retail store.

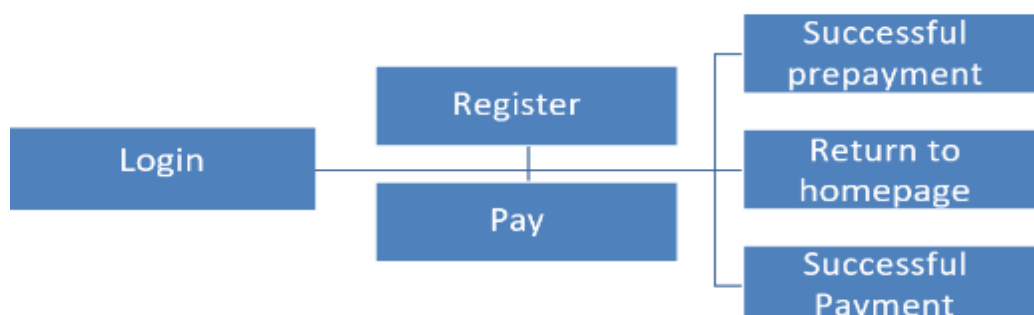
## BLOCK DIAGRAM:

The overall design of the system can be broken down into three components as shown in Fig.1. First, Android application, Encryption and Decryption modules and the user database.



**Fig: 3.1 the proposed blockdiagram**

Fig.2. describes the detailed architecture of the proposed system. The application opens up to the login page and demands the user to enter his/her details as username and phone number and it also leads to the register page for first time users to register with their information



**Fig 3.2 application diagram**

**Working principle:**

If the username already exists, the user is authenticated to the payment page. The system flow can be clearly understood from the diagram above. Asks for the name and the mobile number from the user to login. The registration page helps register a new user on to the application and lets the user make his prepayment which will be stored as the user's balance on the database.

The details this page demands from the user are Age, Email, balance and all the details are added to the database. The billing staff enters the amount payable, and the user is prompted to place his/her registered fingerprint to complete the payment. Upon successfully logging in, the payment page displays the balance in the user's account along with the amount to be paid for the products/services now. The sales person enters the amount to be paid just like as in a card payment system, except here, the swiping of the card is substituted by reading of the user's fingerprint using an individual fingerprint scanner. Here, the fingerprint data that was stored when the user was registered is retrieved to check for the authenticating the user for the payment. The fingerprint data is retrieved from the database in an encrypted format, and then decrypted at the time of verification. To add balance to the existing account, fingerprint is used. This ensures that no tampering can occur. All access to the database, or rather, a particular person's record in the database, is made only through that person's fingerprint. This ensures that no tampering can take place at the seller side. Encryption of the record is carried out using the fingerprint data and a 256 bit key. The record once updated, is encrypted again, before being written onto the database. The entire payment process is secured through the use of encryption and fingerprint authentication. The final page on the application to indicate the successful prepayment upon registering on the registration page and successful payment upon payment after authentication on the payment.

## **CHAPTER 4**

### **REQUIREMENT SPECIFICATION**

#### **Introduction:**

The requirement for this experiment requires both hardware and software requirements that are illustrated below

#### **HARDWARE REQUIREMENTS**

Processor	:	core i3 processor
Hard Disk	:	500 GB.
Ram	:	2 GB
Monitor	:	17VGA Color
Android smartphone:		ver 7,8,9
USB finger print	:	Mantra MFS100 Scanner

#### **SOFTWARE REQUIREMENTS**

Operating System	:	Windows 7,8,10
IDE	:	Andriod studio
Language	:	JAVA/J2EE
Back End	:	SQL

## **HARDWARE REQUIREMENT**

Finger print scanner:

Fingerprint Scanner is a biometric device for authentication and identification through fingerprint recognition. It is a very safe and easy to use device for security compared to passwords and other things. Fingerprint cannot be removed or changed and every fingerprint is different from any other, fingerprints are much used for identification.

Mantra MFS 100 Finger print scanner:



Fig 4.1 : Finger print Scanner

Features:

Lowest FAR and FRR

Support AadhaarAuth API Specification V2.0

Device Securely Signs the Biometric Data

UIDAI Certified RD Service & PID block Encrypted with in RD Service

Plug and play USB 2.0 high speed interface

500 dpi optical fingerprint sensor

Supports Windows 7,8,10, Windows Vista, Windows 2000, Windows Server 2003/2007/2008, Linux, Windows ME, Windows 98 SE SDK, Libraries and Drivers support across all above Platforms. (32 Bit and 64Bit) Easy Integration on to production servers and application support.

#### **APPLICATION:**

PC/Network security

E-commerce

Groupware

Time and Attendance System

Smart Card Application

Public Application

AFIS

Health & Medical

UIDAI Auth Application

## SENSOR SPECIFICATION:

Sensor Characteristics	
Parameters	Specification
Fingerprint Sensor	: Optical (Scratch Free Sensor Surface)
Image Resolution	: 500 DPI / 256 Gray
Platen Area	: 14 x 16 mm
Operating Temperature	: 0~50°C
Standards	: ANSI-378, ISO19794-2
Supports Encryption Algorithms	: AES256, RSA2048
Supports Hashing Algorithms	: MD5, SHA256
Traceability	: Every Device Has a Unique Physical Device ID
Interface	: USB 2.0 High Speed/Full Speed, Plug & Play
Certification	: PIV, CE, FCC, RoHS, IEC60950 Certified
Platen	: Hard Glass
Sensor Certification	: STQC/UIDAI
Operating System	: Android, Windows, Linux

Fig 4.2 End to end Authentication System security



## **CHAPTER 5**

### **METHODOLOGY**

#### **LIST OF MODULES:**

1. Fingerprint Matching Algorithms
- 2 Minutiae Extraction And Matching Algorithm
- 3 Threshold Cryptography technique
- 4 Automated Fingerprint Identification

#### **Module 1:**

##### **FINGERPRINT MATCHING ALGORITHMS**

The existing fingerprint recognition systems uses the approaches based on the local and global feature representations of the fingerprint images such as minutiae, ridge shape, texture information etc.

##### **Ratio of Relational Distance Matching**

This algorithm works in two phases 1. Finding common unique points, 2. Matching phase.

In first phase , two images with  $N1$  and  $N2$  identified minutiae points respectively, this phase output is  $M$  which is a common minutiae points from  $N1$  and  $N2$  ,  $M$  is  $N1$  intersection  $N2$  i.e  $M = (N1 \cap N2)$  where  $N1$  is minutiae points of image1 and  $N2$  is minutiae point of image2. After this new term called  $M$  (i)-tuples is introduced which represents information about a minutiae that can be identified uniquely among the set of all minutiae. There are 2 images are

consider as a base image (BM) and input image (IM). Either of them can be BM or IM and vice versa. Step 1 to find M (i)-tuples is for each  $i = 1$  to  $N1$ , 5 nearest minutiae points are found. This is calculated by finding Euclidean distance from 'i'th minutiae point to all the other minutiae points in set  $N1$  (BM) and noting down 5 euclidean distance with respect to euclidean distance. Step 2 if there are 5 points then calculate euclidean distance by subtracting the  $iN$  from  $i$ . then calculate ratio between them according to the formula  $(a - b) : (a - c) = \text{Max} \{(a-b), (a-c)\} / \text{Min} \{(a-b), (a-c)\}$ . same way calculate M(i)-tuples for input image (IM). All this ratios are compared to get an candidate common list which is done in phase 2 matching phase confirmed common points are identified by drawing tree like structure and listed them , this algorithm results a tree whose vertices features are in Confirmed Common Points List which contains common minutiae points in image 1 and image 2 . Now final results is given if  $C(N)$  is the number of points in Confirmed Common Points List and  $N$  is maximum Number of points in base and input images , then  $C(N) \geq (N/2)$  if this is true then positive score of both images are same is given else negative score is displayed.

## **K-Nearest Neighbor Minutiae Clustering**

Mainly two considerations are lie in this algorithm which are as follows:

1. It uses graph as fingerprint data structure.
2. Fingerprint search is optimized by clustering fingerprint graph feature. As graph is set of edges and vertices here vertices represents feature of fingerprint and edges represents minutiae so clustering of graph data is done by K-NN clustering algorithm based on Euclidean distance between the vertices of the graph .It is the simplest clustering algorithm. The nodes are classified by votes of its neighbors , each node is assigned to the class that is closest among its K nearest neighbor's , where K is integer value. If K=1 then node is assigned to the class of its nearest neighbor.

Following steps are involved for K-NN clustering : 1. Each node of the graph which is in the feature set has a class label , Class =  $c_1, c_2, \dots, c_n$ .

2. Calculating the Euclidean distance matrix for finding Knearest neighbor's where K is the number of neighbors.
3. Most common class labels within the set are determine by analyzing K-closest nodes.

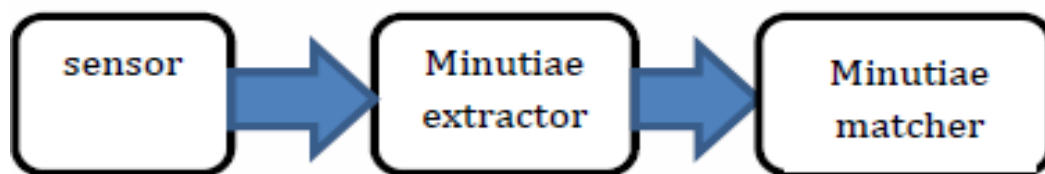
4. The most common class label is assigned to the node being analyzed.

After this clustering of graph nodes the fingerprint matching is performed. To identify the fingerprint it reads each fingerprint clustered graph templates from database and compares it with clustered input fingerprint graph templates. If graph templates are matched then the total graph isomorphism is applied. This continues till the input fingerprint is matched with fingerprint stored in database otherwise no match found returns.

## **Module 2:**

### **Minutiae Extraction and Matching Algorithm**

The basic method of minutiae extraction is divided in to three part Pre-processing, Minutiae Extraction, Post processing .Fig. 1. shows the Fingerprint recognition process using minutiae based algorithm



**Fig.1.Fingerprint recognition process**

This method divides three basic steps in to 7 modules which are given below.

#### **Step 1: Input-**

In this step we take five fingerprints of personas input and process them.

#### **Step 2: Binarization:**

This transform the 8-bit Gray fingerprint image to a 1-bit image with 0- value for ridges and 1-value for furrows.

### **Step 3: Thinning:**

Ridge thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide.

**Uses an iterative, parallel thinning algorithm.**

- 1) To get a thinned image we find the location of middle black pixel at each stage of continuation of the curve.
- 2) In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3).
- 3) And finally removes all those marked pixels after several scans.

### **Step 4: Minutiae Connect:**

This operation takes thinned image as input and produces refined skeleton image by converting small straight lines to curve to maximum possible extent.

### **Step 5: Minutiae Margin:**

This increases the margin of endpoints by one pixel of curves of length at least three pixels.

### **Step 6: Minutiae point Extraction:**

For extracting minutiae point we compute the number of one- value of every 3x3 window:

1. If the centroid is 1 and has only 1 one valued neighbor, then the central pixel is a termination.

2. If the central is 1 and has 3 one-value neighbours, then the central pixel is a bifurcation.
3. If the central is 1 and has 2 one-value neighbours, then the central pixel is a usual pixel.

### **Step 7: False Minutiae Removal**

Procedure for removing false minutiae is given below:

- If the distance between one bifurcation and one termination is less than  $D$  and the two minutiae are in the same ridge. Remove both of them. Where  $D$  is the average inter-ridge width representing the average distance between two parallel neighboring ridges.
- If the distance between two bifurcations is less than  $D$  and they are in the same ridge, remove the two bifurcations.
- If two terminations are within a distance  $D$  and their directions are coincident with a small angle variation. And they suffice the condition that now any other termination is located between the two terminations. Then the two terminations are regarded as false minutia derived from a broken ridge and are removed.
- If two terminations are located in a short ridge with length less than  $D$ , remove the two terminations.
- If a branch point has at least two neighboring branch points, which are each no further away than maximum distance threshold value and these branch points are closely connected on common line segment than remove the branch points. And last we do the minutiae matching. Two fingerprint images to be matched, any one minutia is chosen from each image, and then the similarity of the two ridges associated with the two referenced minutia points is calculated. If the similarity is larger than a threshold, each set of minutiae to a new coordination system is

transformed, whose origin is at the referenced point and whose x-axis is coincident with the direction of the referenced point. After we get two sets of transformed minutia points, we use the elastic match algorithm to count the matched minutia pairs by assuming two minutiae having nearly the same position and direction are identical.

### **Module 3:**

#### **Threshold Cryptography Technique**

#### **Fingerprint Matching using Gabor Filter**

The different processing steps from pre-processing to matching as the final step of the fingerprint authentication are

- Quantized co-sinusoidal triplets
- Discrete Fourier transform
- Gabor filters

The first step is the normalization, which results in a better contrast of the fingerprint image. After that, the fingerprint is segmented, which crops areas of the recorded image, which do not contain any relevant information. This is the end of the pre-processing. The last pre-processing step usually consists of a fingerprint enhancement. However, tests have shown that the subsequent reference point detection works on non-enhanced fingerprint images as well as on enhanced. Therefore, any further enhancement is not required for the subsequent processing steps. After that, the fingerprint image is filtered using a Gabor filter. Now, it is possible to create the feature map, which is used as the template. This template is matched in the subsequent matching step with templates of other fingerprints. The result of the matching is the matching score, which represents how good two fingerprints resemble each other. Most method

f

identification use minutiae as the fingerprint features. For small scale fingerprint recognition system, it would not be efficient to undergo all the pre-processing steps (edge detection, smoothing, thinning ), instead Gabor filters will be used to extract features directly from the gray level fingerprint. No pre-processing stage is needed before extracting the features [7].

## **1) Image Acquisition**

A number of methods are used to acquire fingerprints. Among them, the inked impression method remains the most popular one. Inkless fingerprint scanners are also present eliminating the intermediate digitization process [11]. Fingerprint quality is very important since it affects directly the minutiae extraction algorithm. Two types of degradation usually affect fingerprint images:

- 1) The ridge lines are not strictly continuous since they sometimes include small breaks (gaps);
- 2) Parallel ridgelines are not always well separated due to the presence of cluttering noise. The resolution of the scanned fingerprints must be 500 dpi while the size is 300 x 300.

## **2) Feature Extractor**

Gabor filter based features have been successfully and widely applied to face recognition, pattern recognition and fingerprint enhancement. The family of 2-D Gabor filters was originally presented by Daugman (1980) as a framework for understanding the orientation and spatial frequency selectivity properties of the filter. The fingerprint print image will be scanned by a 8x8 window; for each block the magnitude of the Gabor filter is extracted with different values of  $m$  ( $m = 4$  and  $m = 8$ ). The features extracted (new reduced size image) will be used as the input to the classifier.



### 3) Classifier

The classifier is based on the k-nearest neighborhood algorithm KNN. “Training” of the KNN consists simply of collecting k images per individual as the training set. The remaining images consists the testing set. The classifier finds the k points in the training set that are the closest to x (relative to the Euclidean distance) and assigns x the label shared by the majority of these k nearest neighbors. Note that k is a parameter of the classifier; it is typically set to an odd value in order to prevent ties.

The last phase is the verification phase where the testing fingerprint image [10]:

- 1) Is inputted to the system
- 2) Magnitude features are extracted
- 3) Perform the KNN algorithm
- 4) Identify the person

### Module 4:

#### **AUTOMATED FINGERPRINT IDENTIFICATION**

**Automated fingerprint identification** is the process of using a computer to match fingerprints against a database of known and unknown prints. Automated fingerprint identification systems (AFIS) are primarily used by law enforcement agencies for criminal identification purposes, the most important of which is the identification of a person suspected of committing a crime or linking a suspect to other unsolved crimes.

**Automated fingerprint verification** is a closely related technique used in applications such as attendance and access control systems. On a technical level, verification systems verify a claimed identity (a user might claim to be John by

presenting his PIN or ID card and verify his identity using his fingerprint), whereas identification systems determine identity based solely on fingerprints.

AFISs have been used in large-scale civil identifications, the chief purpose of which is to prevent multiple enrollments in an electoral, welfare, driver licensing, or similar system. Another benefit of a civil AFISs is to check the background of job applicants for sensitive posts and educational personnel who have close contact with children.

### **Fingerprint-matching algorithms**

Fingerprint-matching algorithms vary greatly in terms of Type I (false positive) and Type II (false negative) error rates. They also vary in terms of features such as image rotation invariance and independence from a reference point (usually, the "core", or center of the fingerprint pattern). The accuracy of the algorithm, print matching speed, robustness to poor image quality, and the characteristics noted above are critical elements of system performance.

Fingerprint matching has an enormous computational burden.[clarification needed] Some larger AFIS vendors deploy custom hardware while others use software to attain matching speed and throughput. In

general, it is desirable to have, at the least, a two-stage search. The first stage will generally make use of global fingerprint characteristics while the second stage is the minutia matcher.

In any case, the search systems return results with some numerical measure of the probability of a match (a "score"). In ten-print searching, using a "search threshold" parameter to increase accuracy, there should seldom be more than a single candidate unless there are multiple records from the same candidate in the database. Many systems use a broader search in order to reduce the number of missed identifications, and these searches can return from one to ten possible matches. Latent to tenprint searching will frequently return many (often fifty or more) candidates because of limited and poor quality input data.

The confirmation of system-suggested candidates is usually performed by a technician in forensic systems. In recent years,[when?] though, "lights-out" or "auto-confirm" algorithms produce "identified" or "non-identified" responses without a human operator looking at the prints, provided the matching score is high enough. "Lights-out" or "auto-confirm" is often used in civil identification systems, and is increasingly used in criminal identification systems as well.

## **USER AUTHENTICATION MODE:**

In the user authentication mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, (usually via a PIN Personal Identification Number), a user name, a smart card, etc., and the system conducts a one to-one comparison to determine whether the claim is true or not. Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

## AFIS algorithm

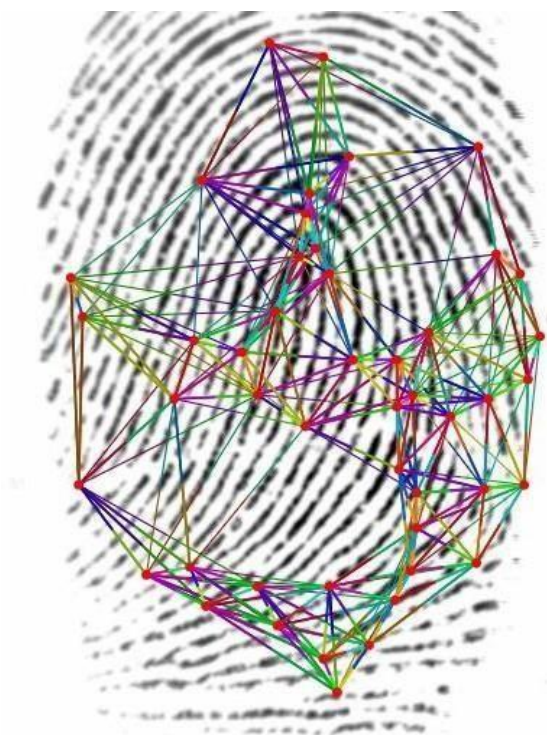
SourceAFIS algorithm is mostly about *understanding* fingerprints. Of course, SourceAFIS is not a human, so how could it understand anything? For algorithms, understanding data means describing it with high-level abstractions. In case of SourceAFIS, these high-level abstractions are *minutiae*, or ridge endings and bifurcations. Minutiae are simply points on the image with associated direction angle.



**Fig 5.2 : Minutiae found on the fingerprint image.**

This is essentially what gets saved in the template. Many small abstractions happen along the way from fingerprint image to the list of minutiae (the template), but we will talk about that some other time.

After minutiae, there is one more abstraction step, which produces *edges*. Edge is a line connecting two minutiae. Edge has length and two angles inherited from its minutiae. Edge angles are expressed as relative to the edge. These three properties of the edge (length and two relative angles) do not change when the edge is moved or rotated and that's exactly what we need for matching.



**Fig 5.3 : Color is determined by edge length and angles. Similar edges have similar colors.**

SourceAFIS then tries to find at least one edge shared by the two fingerprints being matched. This is done very quickly using a nearest neighbor algorithm that has performance comparable to a hash table. That will give us the *root pair*, which is the initial pair of matched minutiae, one from each fingerprint.

Starting from the root pair, SourceAFIS crawls edges outwards and builds a *pairing* consisting of a number of paired minutiae and paired edges.



**Fig 5.4 : Root minutiae are blue. Pairing tree is green. Graph of supporting edges is yellow.**

SourceAFIS now looks carefully at the pairing and decides whether such pairing means a match or whether it's just a coincidence. Of course, everything could be a coincidence, but the difference between weak and strong match is that strong match is very unlikely to be a coincidence.

This is where SourceAFIS runs *scoring*, the last part of the algorithm. The basic idea is that every paired minutia or edge is an event that is unlikely to happen randomly. The more of such unlikely events there are, the less likely the pairing is to be just a coincidence. So the algorithm essentially counts various matched features and also scores them on how closely they match. Final sum of the partial scores is shaped to align to some reasonable scale and returned from the algorithm. Application takes the score and compares it to some *threshold* to decide whether it's a match or not.

If you are still hungry for information, take a look at template format and algorithm transparency. Reading the source code is the definitive way to answer all your remaining questions.

## PERFORMANCE ANALYSIS

The following table shows the performance analysis of the various matching techniques.

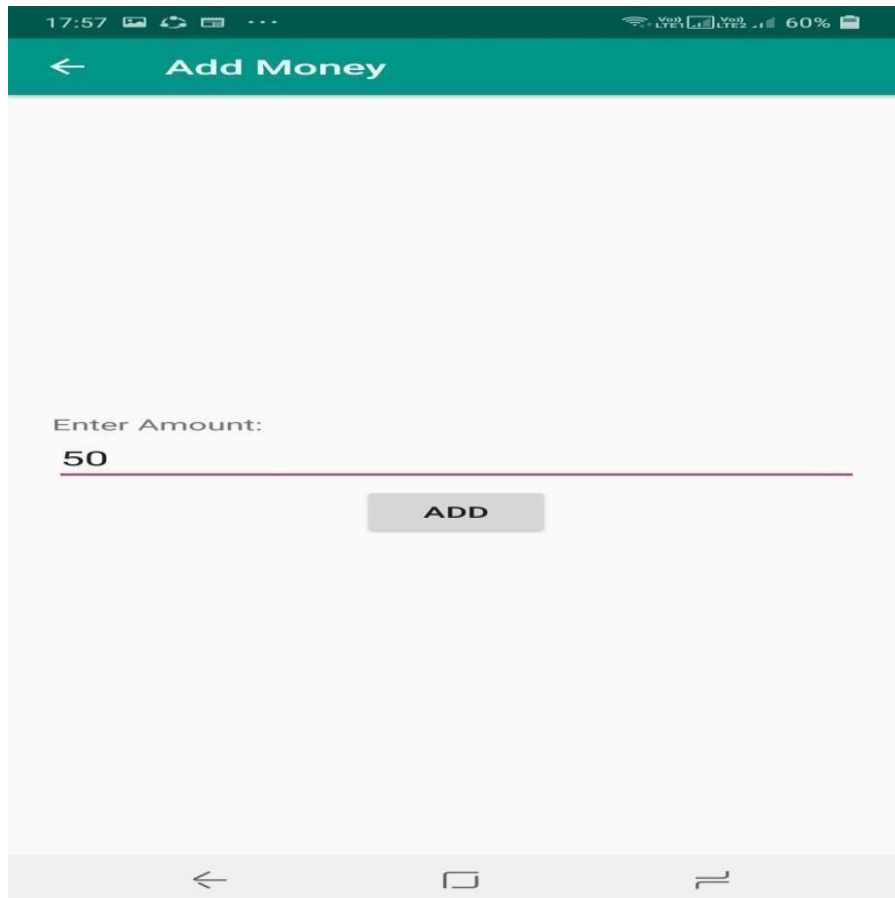
### PERFORMANCE ANALYSIS OF THE TECHNIQUES

TECHNIQUES	OBJECTIVE	LIMITATIONS
Minutiae based algorithms	To design an algorithm with privacy and security purpose	Not suitable for low quality templates
Threshold cryptographic techniques	To develop a technique by dividing into small shares	Compression is required for reconstruction of fingerprint image
Fingerprint matching using gabor filter	To develop technique to increase genuine acceptance rate	More number gabor filters are used
K-nearest neighbour clustering	To identify the fingerprint it reads from the fingerprint clustered templates from databases	This technique is to increase the processing time

## CHAPTER 6

### RESULTS

#### ADD MONEY



17:57

← Add Money

Enter Amount:

50

ADD

Fig 6.1 Add money screen



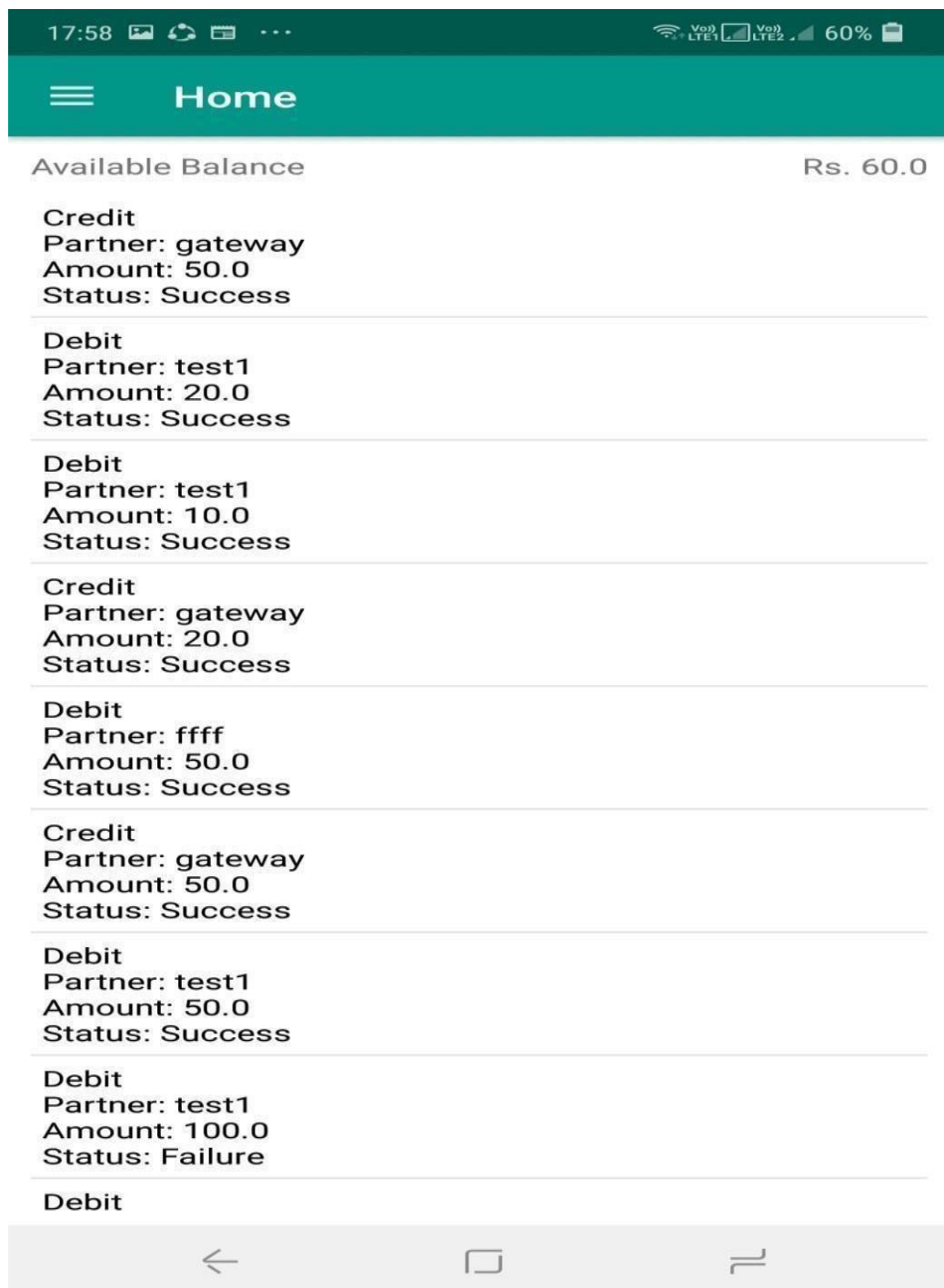


Fig 6.2 : Home screen after adding money

# FINGERPRINT BASED MONEY TRANSFER SERVICE

## Account Identification by Finger Print



Fig 6.3 Account Identification by Fingerprint

## MATCHED ACCOUNT PAGE

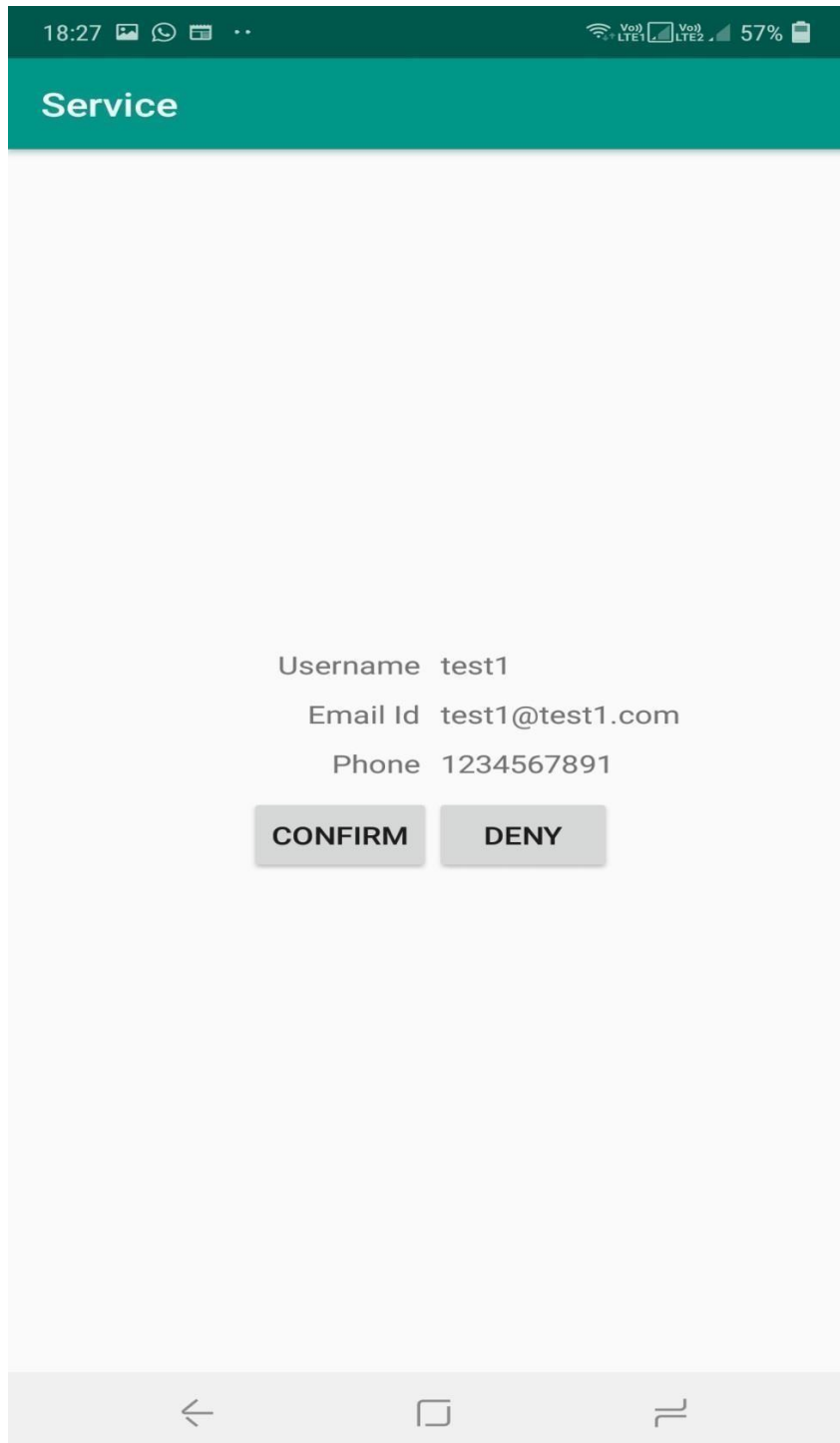


Fig 6.4: Matched account page

## MONEY TRANSFER SUCCESS PAGE



Fig 6.5 Transaction Successful Page

POST TRANSACTION BALANCE PAGE



Fig 6.6 Post Transaction Balance page

## SERVICE REGISTRATION

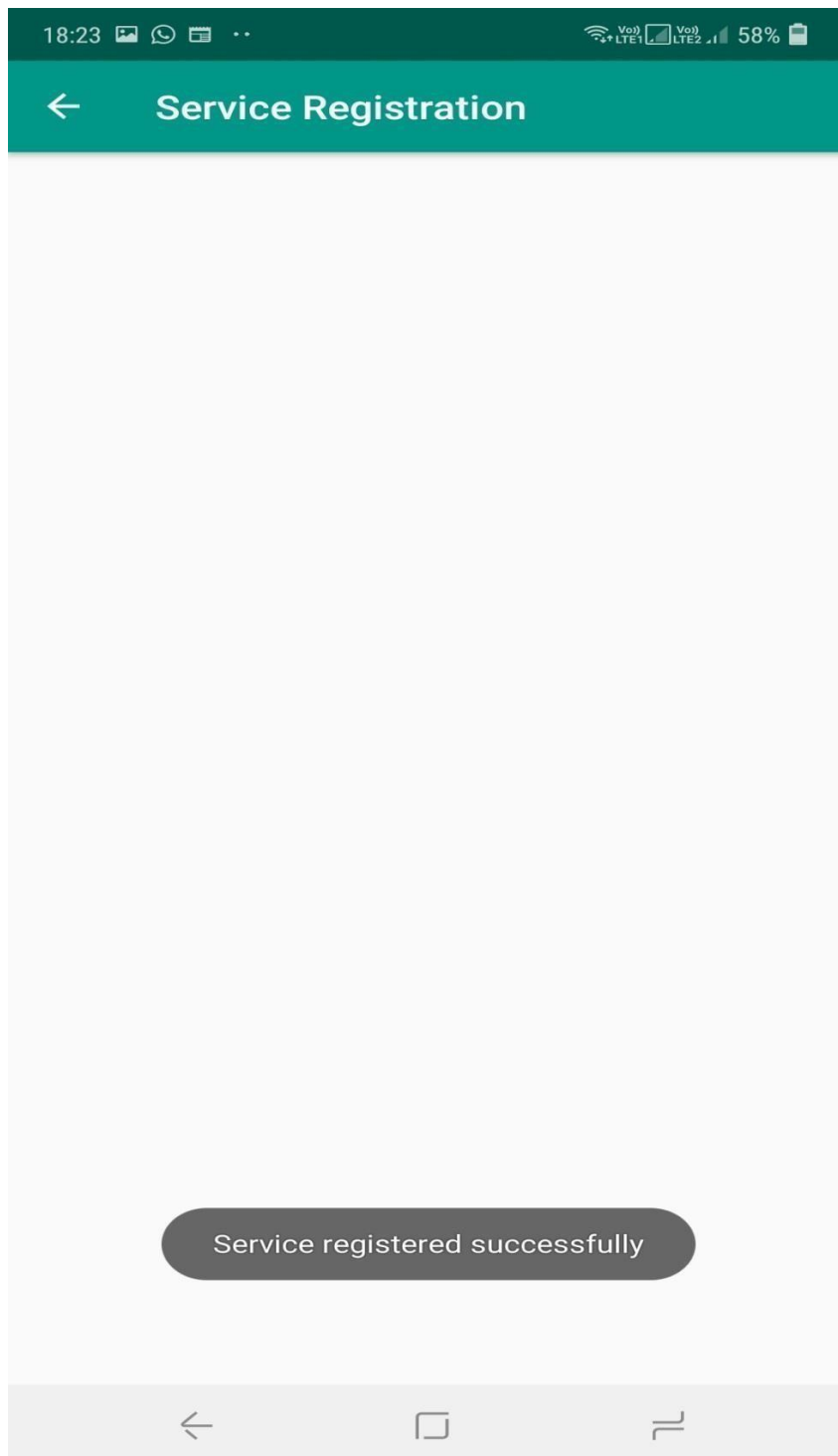


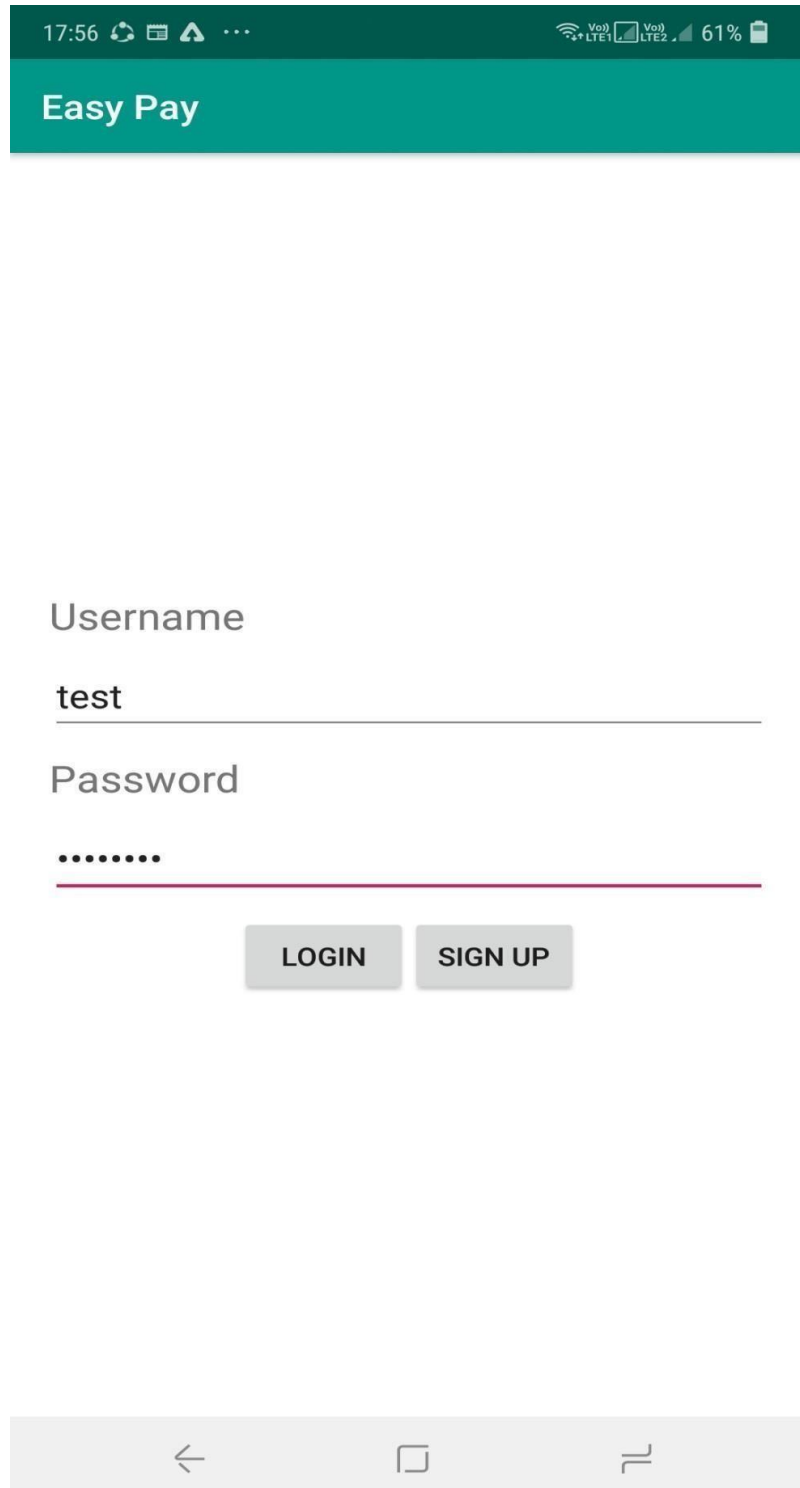
Fig 6.7 Service registration Page

## SERVICE SCREEN



Fig 6.8 Service Screen

## LOGIN LOGIN SCREEN



The image shows a mobile application login screen for 'Easy Pay'. At the top, there is a dark green header bar with the text 'Easy Pay' in white. Below the header, the screen is white. There are two input fields: 'Username' and 'Password'. The 'Username' field contains the text 'test'. The 'Password' field is masked with dots. Below the input fields, there are two buttons: 'LOGIN' and 'SIGN UP'. At the bottom of the screen, there is a grey bar with three icons: a back arrow, a square, and a double line.

17:56 17:56 VoLTE1 VoLTE2 61%

Easy Pay

Username

test

Password

.....

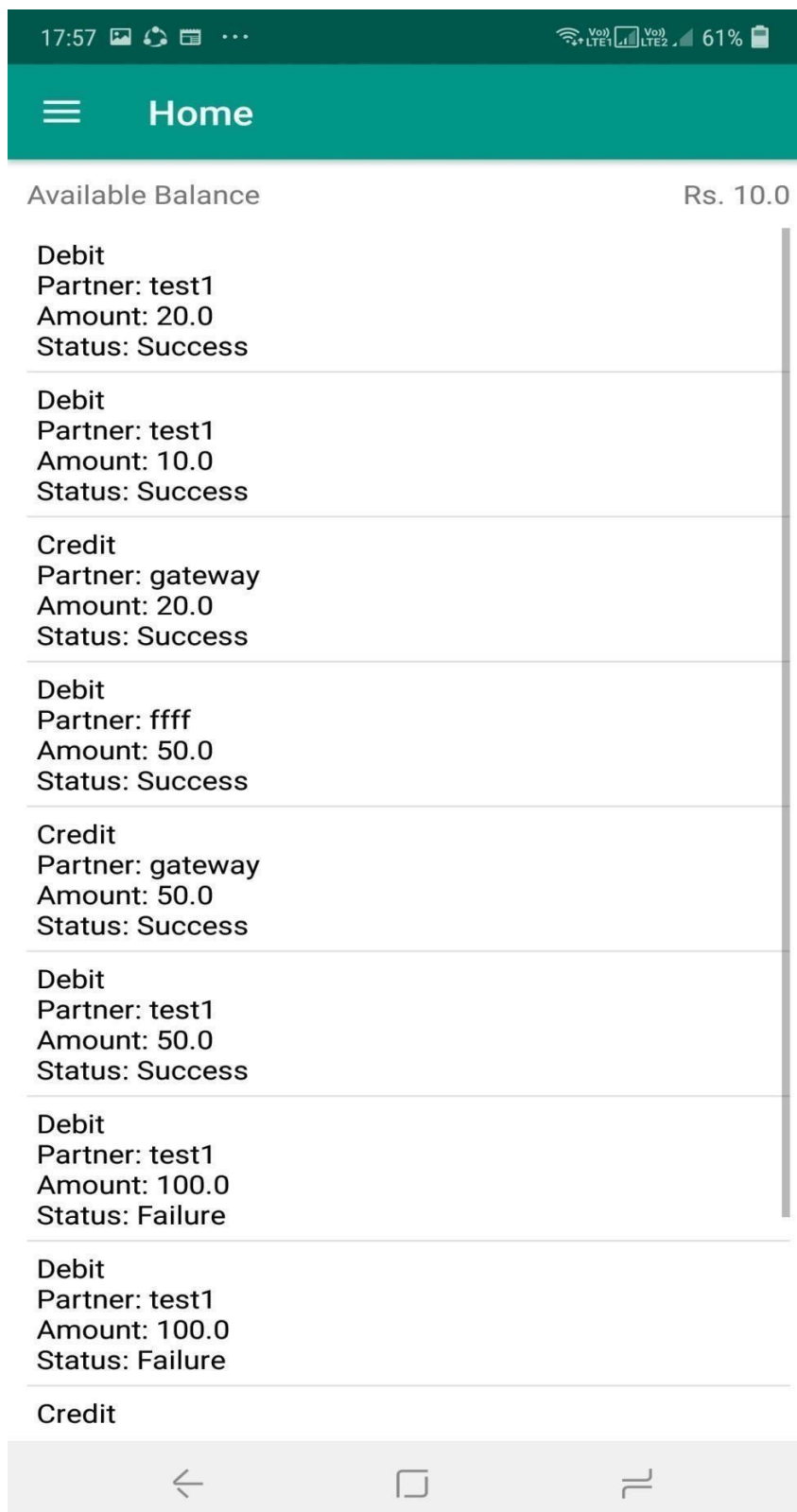
LOGIN SIGN UP

< □ ≡

Fig 6.9 Login Screen



## INITIAL BALANCE



Available Balance				Rs. 10.0
Debit	Partner: test1	Amount: 20.0	Status: Success	
Debit	Partner: test1	Amount: 10.0	Status: Success	
Credit	Partner: gateway	Amount: 20.0	Status: Success	
Debit	Partner: ffff	Amount: 50.0	Status: Success	
Credit	Partner: gateway	Amount: 50.0	Status: Success	
Debit	Partner: test1	Amount: 50.0	Status: Success	
Debit	Partner: test1	Amount: 100.0	Status: Failure	
Debit	Partner: test1	Amount: 100.0	Status: Failure	
Credit				

Fig 6.10 Initial Balance screen

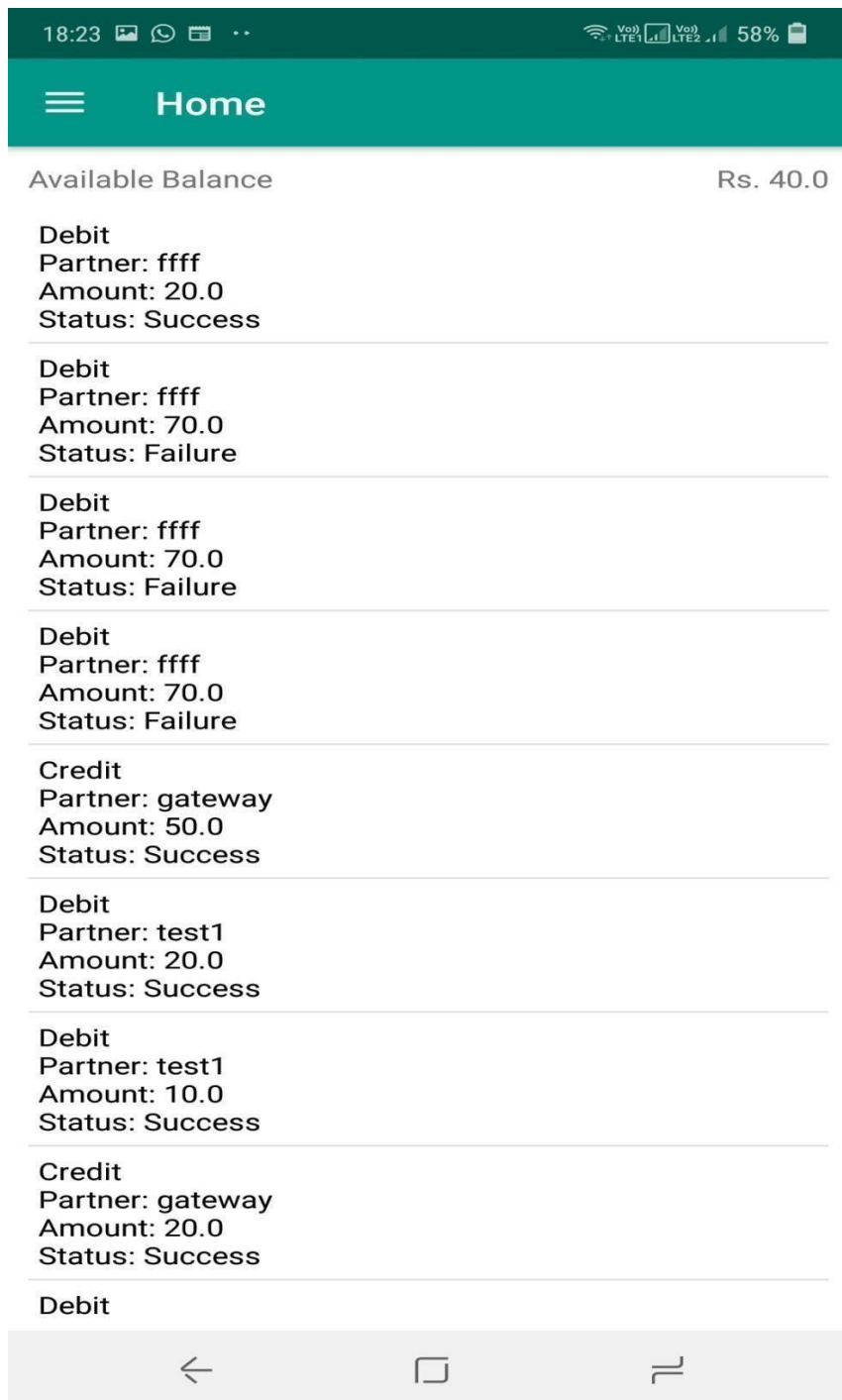
## MONEY TRANSFER

### AMOUNT GREATER THAN BALANCE

The screenshot shows a mobile application interface for transferring money. At the top, a teal header bar contains a back arrow and the text "Transfer Money". Below this, the status bar shows the time 17:58, various connectivity icons, and a 60% battery level. The main content area has a light gray background. It features two input fields: the first is labeled "Email / Mobile Number / Username" and contains the text "ffff"; the second is labeled "Amount" and contains the text "70". Below the "Amount" field is a gray button labeled "TRANSFER". At the bottom of the form area is a dark gray rounded rectangle containing the text "Unable to Transfer Money". The bottom of the screen shows a standard Android navigation bar with back, home, and recent apps icons.

Fig 6.11 Money transfer page

## BALANCE AFTER MONEY TRANSFER



The image is a screenshot of a mobile application interface. At the top, there is a status bar with the time 18:23, signal strength indicators, and a battery level of 58%. Below the status bar is a teal header with a hamburger menu icon and the word "Home". The main content area has a light gray background. At the top of this area, it says "Available Balance" followed by "Rs. 40.0" on the right. Below this, there is a list of transactions, each separated by a horizontal line. The transactions are as follows:

Type	Partner	Amount	Status
Debit	ffff	20.0	Success
Debit	ffff	70.0	Failure
Debit	ffff	70.0	Failure
Debit	ffff	70.0	Failure
Credit	gateway	50.0	Success
Debit	test1	20.0	Success
Debit	test1	10.0	Success
Credit	gateway	20.0	Success
Debit			

At the bottom of the screen, there is a light gray navigation bar with three icons: a back arrow, a square, and a double line.

Fig 6.12: Balance after money transfer

# MONEY TRANSFER SUCCESS

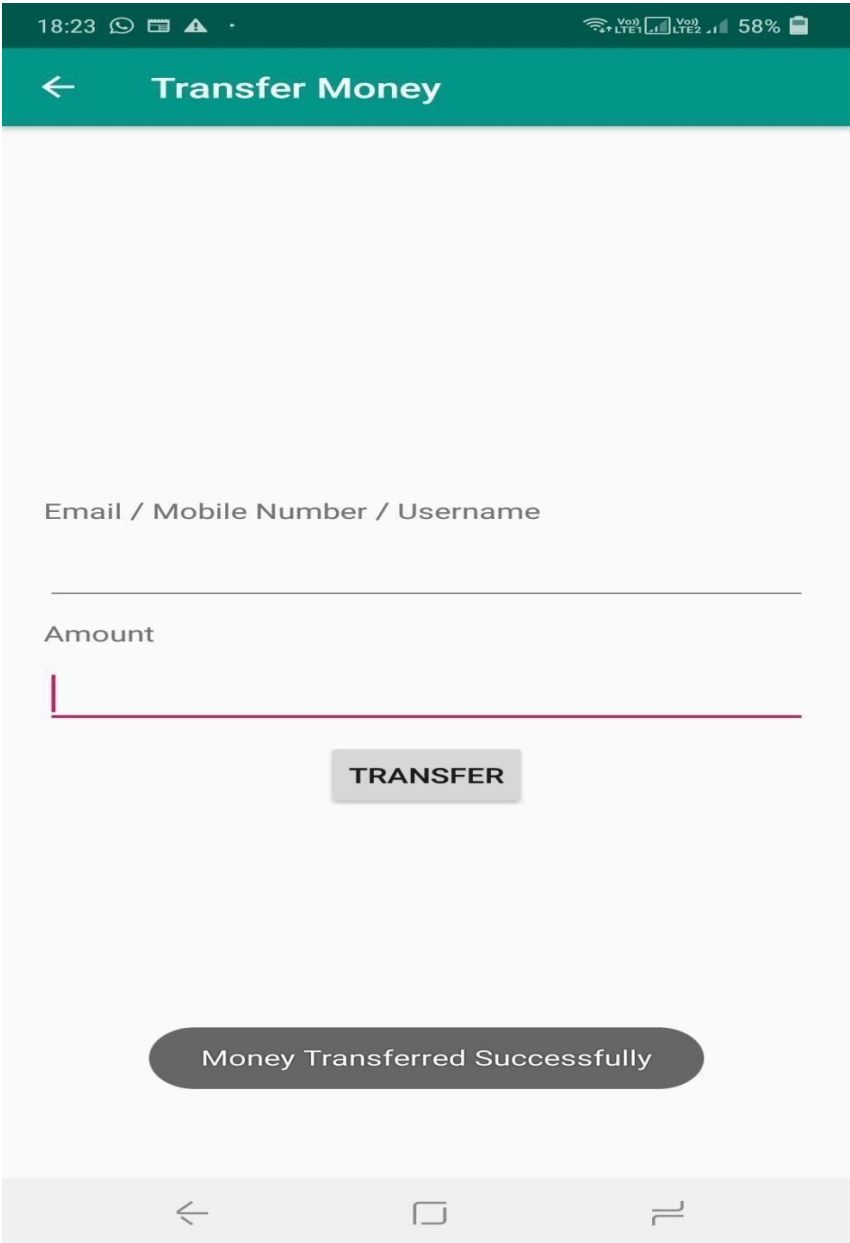


Fig 6.13 Money transfer success

## **CHAPTER 7**

### **CONCLUSION**

We performed three different feature extraction methods for fingerprint authentication and reported the results on their security compromise. Our results indicate that Minutiae"s have the best performance to provides secured m-commerce. In this work, the design approach for a Biometric Mechanism for enhanced Security of Online Transaction on Android system has been proposed. Here run time fingerprint would be captured for mobile transaction; it is not stored already in the mobile device so it provides more security and not stolen by third party. This gives the better level of security mechanism for m-commerce system.

## CHAPTER 8

### REFERENCES

1. MangalaBelkhede\*, VeenaGulhane\*\*, Dr. Preeti Bajaj\*\*\* “Biometric Mechanism for enhanced Security of Online Transaction on Android system: A Design Approach” ,Feb. 19~22, 2012
2. Dr. Manish Manoria,Ajit Kumar Shrivastava,Satyendra Singh Thakur,,DebuSinha.(2011)” Exploring the Prospect of Secure Biometric Cryptosystem using RSA for Blind Authentication”.
3. System I. Iancu, N. Constantinescu, M. Colhon “Fingerprints Identification using a Fuzzy Logic” ,2010.
4. Dr Suresh Sankaranarayanan, “Biometric Security Mechanism in mobile Payment”, Published by the IEEE Computer Society, 2010.
5. UdayRajanna Ali Erol George Bebis” A comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion” Springer-Verlag London Limited 2009.
6. ChetanaHegde, Manu S, P DeepaShenoy, Venugopal K R, L M Patnaik (2008) “Secure Authentication using Image Processing and Visual Cryptography for Banking Applications”.
7. John Daugman “New Methods in Iris Recognition”,october 2007.
8. T. Ahonen, A. Hadid and M. Pietik ” ainen, “Face recognition with local binary patterns”, European Conference on Computer Vision,Prague, 469, 2004.
9. Fahad Al-harby, Rami Qahwaji, and Mumtaz Kamala “Secure Biometrics Authentication: A brief review of the Literature”2004.
10. YagerN,Amin A(2004) “Fingerprint verification based on minutiae features”.
- 11..Kawagoe M, Tojo A (1984) “Fingerprint pattern classification”. Pattern recognition”

