UID based Mobile Money Implementation in Rural Areas of India

A

Dissertation

submitted

in partial fulfillment

for the award of the Degree of

Master of Technology

in Department of Computer Science Engineering

(with specialization in Software Engineering)

Supervisor Name
Dinesh Goyal
Associate Professor
SGVU, Jaipur

Submitted By:
Dolly Varshney
SGVU081090959

Department of Computer Science & Engineering

Suresh Gyan Vihar University
Mahal, Jagatpura, Jaipur

December - 2013

SURESH GYAN VIHAR UNIVERSITY

The first research oriented University of state

Certificate

This certifies that the dissertation entitled

"UID Based Mobile Money Implementation in Rural Areas of India"

is submitted by

Dolly Varshney

SGVU081090959

Xth Semester, M.Tech (SE) in the year **2013** in partial fulfillment of

Degree of Master of Technology in *Software Engineering*

SURESH GYAN VIHAR UNIVERSITY, JAIPUR.

_____

Mr. Dinesh Goyal

Associate Professor

SGVU, Jaipur

Date:

Place: Jaipur

Candidate's Declaration

I hereby that the work, which is being presented in the Dissertation, entitled "**UID based Mobile Money Implementation in Rural Areas of India**" in partial fulfillment for the award of Degree of "**Master of Technology**" in Dept. Of Computer Science & Engineering with specialization in **Software Engineering** and submitted to the **Department** of **Computer Science & Engineering, Suresh Gyan Vihar University** is a record of my own investigations carried under the Guidance of **Mr. Dinesh Goyal**, Department of Computer Science & Engineering.

I have not submitted the matter presented in this Dissertation anywhere for the award of any other Degree.

(Dolly Varshney)

……..

Software Engineering

Enrolment No.: SGVU081090959

Counter Singed by

Mr. Dinesh Goyal
Associate Professor
Suresh Gyan Vihar University, Jaipur

DETAILS OF CANDIDATE, SUPERVISOR (S) AND EXAMINER

Name of Candidate: Dolly Varshney

Dept. of Study: Engineering Department of Computer Science

Enrolment No.: SGVU081090959

Thesis Title: UID based Mobile Money Implementation in Rural Areas of India

Supervisor (s) and Examiners Recommended **(with Office Address including Contact Numbers, email ID)**		
Supervisor Mr. Dinesh Goyal Associate Professor (CS) Suresh Gyan Vihar University, Jaipur dgoyal@gyanvihar.org		
Examiner		
1	**2**	**3**

Signature with Date

Program Coordinator Dean / Principal

ACKNOWLEDGEMENT

I would like to express my gratitude to all those who gave me the possibility to complete this dissertation. I want to thank the Department of Computer Science Engineering of Suresh Gyan Vihar University, Jaipur for giving me permission to commence this dissertation in the first instance, to do the necessary research work.

I am deeply indebted to my supervisor Prof. Dinesh Goyal from the Department of Computer Science Engineering of Suresh Gyan Vihar University, Jaipur whose help, stimulating suggestions and encouragement helped me in all the time of research for and writing of this dissertation.

Last, I would like to give my special thanks to my family members and friends for their faith and giving me the first place by supporting me throughout my life and their patient love enabled me to complete this work.

Dolly Varshney

CONTENTS

List of Figures

List of Tables

ABSTRACT

Mobile Money is a technology that allows people to make financial transactions using mobile phone technology. This is a new and fast adopting, an alternative payment method. Mobile money services are being deployed in many markets around the world. There is strong evidence that these services can improve access to formal financial services in developing countries.

In many developing territories, mobile operators have been more successfully reach unbanked consumers than banks . In this case, where customers have a cell phone, but no bank account, mobile wallet provides a unique opportunity to serve the amendment, bringing customers from the cash economy access to the orthodox financial system, and to provide them with access to financial services. Delivery speed and benefits are also important, such as perception of safety trading losses and secure funding . There are number of services in many countries related to m-money which has also increased the take up of mobiles. These services are typically used to perform low-value transactions and located in rural and urban environments

Objective of the propsed work is to analyse and develop a secure and cheap model of Mobile Money transfer which involves multi level security, without additional cost. Our proposed framework would enable the sender to transfer money without much overhead of bank processing, also it would release the sender from the transportation and processing cost, which will make our proposed model more suitable and flexible.

Here, we are using Aadhaar for individual’s identity authentication. This 3-level security model is for especially rural dwellers and unbanked consumers.

CHAPTER 1

INTRODUCTION

1.1 MOBILE MONEY

Mobile Money (M-money) can be understood as a series of financial services provided to consumers via Mobile Phone. The services comprise credits, prudence, lodgings and payments. It could be people who transfer funds domestic or international balance of payments, or to pay for goods and services or business mobile banking.[18]

41% of the population in India does not have access to banks and banking resources[31]. Mobile Money services are currently deployed in many markets around the world and in India too, and there is proof that they can better access to formal commercial services in growing countries. In many developing territories, mobile operators have been more successfully reach unbanked consumers than banks [31]. In this case, where customers have a cell phone, but no bank account, mobile wallet provides a unique opportunity to serve the amendment, bringing customers from the cash economy access to the orthodox financial system, and to provide them with access to financial services. Delivery speed and benefits are also important, such as perception of safety trading losses and secure funding [31]. There are number of services in many countries related to m-money which has also increased the take up of mobiles. These services are typically used to perform low-value transactions and located in rural and urban environments [31].

1.2 UNIQUE IDENTIFICATION CARD (UID)

In India, Aadhaar is a 12-digit personal identification number provided to each individual card which is issued by the Unique Identification Authority of India. This number serves as a certification of identity and address, anywhere in India. Aadhaar is biometric-based identity card.

For the online authentication UIDAI proposes use of demographic and biometric data of citizens. The UID (Aadhaar) Number, is a matchless identity for the entire citizen, this is allocated to all of them it means that every citizen have a matchless separate identity that is issued by public agencies or private agencies at the behalf of the government.

The purposes of Authentication are following:

- To allow Aadhaar-holders to prove identity and
- For service providers to confirm the resident's identity claim for services delivery and give access to detriments. Aadhaar Authentication shall make life simpler to the resident as it is meant to be a convenient system to prove one's identity without having to provide identity proof documents whenever a resident seeks a service.

We are using UID for first level authentication of the recipient.

1.3 ONE TIME PASSWORD

"One-time Password" as the name depicts it is only used once and that too for a short span of time. The algorithm that is used to generate OTP is psuedorandomness.
There is a time synchronisation between the client and the authentication server and also it works for short period of time as it is already being mentioned .OTP works on token system. Each time user uses a new password (or token) which is dead after a particular time.

There are various time passwords on the server and sends its way through to the other users of the system - of - band channels, such as: SMS. Ultimately, in some systems, the paper printed with OTP token, the user must carry [27]. We have used one time password for second level authentication of recipient. Some systems use particular electronic security tokens, and bring the user to generate a one-time password, and using a small display out.[27]

1.4 FINGERPRINTS

Fingerprint scan is also renowned as finger scan. It is oldest and widely used biometric technique of authentication. Fingerprints are considered ideal means of identification. Every individual has his own unique fingerprints. No two individuals can have same pattern of fingerprints.
Fingerprints remain unchanged for lifetime
Fingerprint scanning is the process of taking human fingerprints and then storing them in database. It saves image in digital form. It just takes few seconds to compare two fingerprints. Only specific characteristics that are unique to every fingerprint are used to being filtered and saved in encrypted form as biometric key or mathematical representation. Fingerprints are not saved in form of image, they are saved in digital form i.e. in a series of numbers(a binary code). Algorithm cannot reconvert the digital image to original image

1.5 MOTIVATION FOR RESEARCH WORK

In most developing nations of the world, the greatest majority of the population is living in rural areas, generally not well educated and disadvantaged of access to financial services. Around 480 million people, mostly living in the country's 630,000 villages, have no banking access. They generally trust on payments from economic migrants for poverty easement.

Most of the rural denizens somehow depend on remittance from their family members or friends because these rural areas have lack or limited access to financial services. People have to travel a mile away for collect their money to the nearest pay out point which is often costly and time consuming.

In rural areas there is no facility of banks or other option to borrow or send money so the rural people are forced to borrow money from the local money lenders at very high interests. Moreover, these local lenders tend to suppress these borrowers by charging high interest which often results in selling of the property or other valuables by the borrower to pay the amount back to the lender. Also, if the rural people want to borrow money from the bank then it is a big deal for them; as first they have to travel miles to reach the nearest branch of bank and the bank formalities seem to be a sort of headache for them.

Therefore, it is required that such a system should be developed especially for rural people that would enable them to access all the facilities provided by the banks in urban areas.

1.6 PROBLEM DOMAIN OF THE RESEARCH

In rural areas, mostly people do not possess bank accounts and even in most rural areas there are no banks or other financial systems for these people. Thus, these people remain deprived from the services provided by the bank and cannot take benefit from these services. Moreover, these people are not perfect to carry out bank procedures since mostly people are illiterate or old or young that they do not understand the formalities of the procedure. Most people are depends on the earning member of their family how might be living far in cities to earn money. So, a system is needed that would enable the dependents living in the rural areas to receive money from the earning member living in the city in an easy way.

These are following issues; rural denizens have to face to while accessing formal financial institutions:

- Significant distances to the closest service point;
- High cost of transportation in reaching to the service point;

- Problem in filling out application forms and completing the necessary documentations required by banks as they are not well educated;
- Limited options, such as only account-to-account transfers with access hurdles(e.g., minimum balance requirements);
- Unfamiliarity with other options offered by financial service providers

1.7 OBJECTIVE OF THE RESEARCH

Objective of the research work is to analyse and develop a secure and cheap model of Mobile Money transfer which involves multi level security, without additional cost. Our proposed framework would enable the sender to transfer money without much overhead of bank processing, also it would release the sender from the transportation and processing cost, which will make our proposed model more suitable and flexible.

Here, we are using Aadhaar for individual's identity authentication. A 3-level security is employed using the phone, fingerprints and the Aadhaar. Our purpose is to design a mobile money model for especially rural dwellers and unbanked consumers that shows following features:

- reliable
- easy to access
- affordable
- efficient
- timeliness

1.8 ORGANISATION OF THE THESIS

Chapter 2 covers about overview of Mobile phone, Mobile phone users in India, Mobile Money, Authentication and it's types, One time password and unique identification card (UID) .

Chapter 3 covers review of literature on projects based on Mobile Money.

Chapter 4 deals with the final proposed framework of UID based Mobile Money implementation in rural areas in India.

Chapter 5 covers research findings of the proposed work and it also explain comparision with existing technologies

Chapter 6 covers conclusion and future scope of the research work.

Chapter 7 covers references used in the work.

CHAPTER 2

OVERVIEW OF TECHNOLOGY USED

2.1 MOBILE PHONE

2.1.1 INTRODUCTION

Mobile phone is also known as a cell phone and a handset. It is an electronic equipment that can make and receive phone calls over a wireless communication link while moving anywhere in the world. This is done by connecting to a mobile network provided by our mobile provider. It provides access to the public telephone network. On the other hand, a cordless phone is used only within a little range of a private base station. Along with telephony, modern wireless mobile phones support an extensive variety of other services: such as SMS, video mail, electronic-mail, web access, infrared, Bluetooth, applications related to business, entertaining games and photography. These mobile phones that offer computing capabilities referred to as smart phones.

2.1.2 MOBILE PHONE USERS IN INDIA

The mobile phone market has witnessed tremendous growth in the last decade in India. Having all the major cellular companies in India providing its services there way was an exponential increase in the subscriber base of mobile phone.

"India has 55.48 lakh mobile users according to our Mobile Landscape of India (IML) 2013 Study. 54 percent of these owners of the devices in rural areas compared to 25.6 crore in cities and towns, " said co-founder Mrutyunjay Juxt PTI. There is a total of Rs 77.39 SIM- functional action, but only 64.34 55.48 crore sims using mobile devices owners, the report says the study.[3]

The following table shows the increment in number of Mobile Money Subscribers(in millions) in India since January 2002[24]:

Year	January	February	March	April	May	June	July	August	September	October	November	December
2002	0.28	0.35	0.41	0.28	0.29	0.35	0.36	0.49	0.37	0.53	0.72	0.8
2003	0.64	0.6	0.96	0.64	2.26	1.42	2.31	1.79	1.61	1.67	1.9	1.69
2004	1.58	1.6	1.91	1.37	1.33	1.43	1.74	1.67	1.84	1.51	1.56	1.95
2005	1.76	1.67	0.73	1.46	1.72	1.98	2.45	2.74	2.48	2.9	3.51	4.46
2006	4.69	4.28	5.03	3.88	4.25	4.78	5.28	5.9	6.07	6.71	6.79	6.48
2007	6.81	6.21	3.53	6.11	6.57	7.34	8.06	8.31	7.79	8.05	8.32	8.17
2008	8.77	8.53	10.16	8.21	8.62	8.94	9.22	9.16	10.07	10.42	10.35	10.81
2010	9.88	7.44	8.00	1.85	8.35	4.73	-20.61	-5.13	-1.74	-2.39	-13.63	-25.88
2009	15.41	13.82	15.64	11.90	11.58	12.04	14.38	15.08	14.98	16.67	17.65	19.10
2011	18.99	20.20	20.21	15.34	13.35	11.41	6.67	7.34	7.90	7.79	2.97	9.47
2012	19.90	18.76	20.59	16.9	16.31	17.98	16.92	18.18	17.1	18.98	22.88	22.62

Table 2.1: mobile subscriber (in millions) in India[24]

2.1.3 MOBILE PHONE IN RURAL INDIA

The rural economy has recorded impressive development since past decade[35]. Almost each and every villages is expected to be connected by all-weather road, every rural Panchayat have an Internet connection , and almost every house in the village of five hundred plus population have electricity and the proud owner of a mobile phone.[35]

Number of rural subscriber exploded over the past five years. A lot of conveniences are offered by mobile phone at an affordable cost to rural consumers in all segments. Today India is the super fastest developing telecom market and the second largest country in the world with over 755 million mobile subscribers. A huge clot of this growth Entrance rural markets have witnessed exponential growth.[4]

Rural Indians have collected about 3 million mobile phone SIM cards in June 2013 to benefit telecom operator companies such as Airtel, Idea Cellular , Reliance Communications, Aircel , Vodafone, Uninor , Videocon , etc.

Latest data from the mobile subscriber base of TRAI shows significant increase in rural mobile users. Mobile phone subscription in rural areas step up from 348.19 million in May from 2013 to 351.10 million in June 2013. Rural tele density has stepped up from 40.83 to 41.14. Mobile phone subscription in urban areas stepped up from 522.01 million in May 2013 to 522,270,000 in June 2013 . Urban wireless tele density has stepped down from 139.32 to 139.16. TRAI said

the total wireless subscriber base stepped up from 870.20 million in May 2013 to 873,360,000 in June 2013, recording a monthly increment of 0.36 percent.[37]

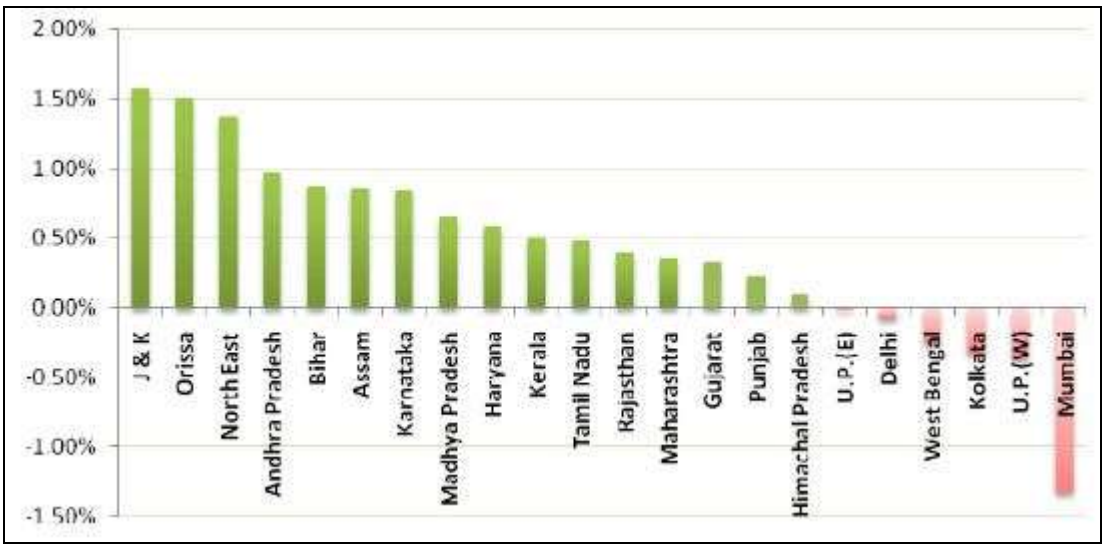


Fig. 2.1: Service Area wise growth in total mobile subscribers (May-June 2013)[25]

The share of urban wireless subscribers has declined from 59.99 percent to 59.80 percent where as share of rural wireless subscribers has step up from 40.01 percent to 40.20 percent[37]. The gross wireless tele-density in India reached 71.08 from 70.90 the previous month.

2.2 MOBILE MONEY

2.2.1 INTRODUCTION

Mobile Money is a technology that allows people to make financial transactions using mobile phone technology. This is a new and fast adopting, an alternative payment method. Mobile money services are being deployed in many markets around the world. There is strong evidence that these services can improve access to formal financial services in developing countries.

The support of both banking and non-banking companies, developers to create mobile applications for money, mobile phone manufacturers of mobile money to support Near Field Communications (NFC) chips and antennas , and finally the other mobile operators are the crucial elements for mobile money to be successful.

The traditional " bricks and mortar " banking infrastructure is struggling to make the business model work is to serve clients with low incomes , especially in remote areas. However, mobile operators already have a large terrestrial distribution networks that can be used for providing customers, mobile network funds where they can perform transaction like cash in or cash. Major

mobile operators in developing countries typically have 100 to 500 times extra airtime reseller outlets than all the bank branches combined. Also, some mobile operators strong brands recognized that even in remote areas. Mobile operators can use their existing brand strength to gibe base to a trusting relationship with clients which is important for driving the adoption of financial services.

2.2.2 MOBILE MONEY ECOSYSTEM

Stakeholder	Expectations
Consumer	• Reduced risk of carrying cash • Minimal learning curve • New service is available everywhere • Low or zero additional cost of usage • Security of transactions • Person-to-person transactions • Able to send and receive money (both domestic and international remittances)
Friends/family members	• Able to send and receive money (both domestic and international remittances) • Able to send/receive money in emergency situations
Employers	• Reduce time • Reduce cash risks
Mobile network operator (MNO)	• Potential to add value to existing services • Increase customer loyalty • New revenue channels • Increase average revenue per user • Reduce airtime distribution cost
Banks/microfinance institutions (MFI)	• Branding and customer loyalty • New customers • Ownership or co-ownership of the new payment application • Secure and trusted payment service • Anti-money laundering requirements • Integration/use of existing infrastructure and payment methods
Agents	• Earns commission on transactions • New revenue streams • Increase traffic and sales
Merchants	• Offer convenience to customers
Regulator	• Promote financial inclusion • Promote interoperability among payment services • Reduce risks of money laundering

Source: Adapted from S. Karnouskos, Mobile payment: a journey through existing procedures and standardization activities, Communications Surveys & Tutorials, IEEE , vol.6, no.4, pp.44,66, Fourth Quarter 2004. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5342298

Table 2.2: Expectations of parties in mobile money transfer ecosystem

A number of parties involved in the business of mobile money. For mobile operators, mobile money means more customers and higher average gross money per customer. Most of the offerings therefore are based on fulfill customer loyalty to enhance the total revenue from telephone services[6]. Table 2.2 shows the main expectations of different parties in the ecosystem of mobile money in emerging economies. [6]

2.2.3 MOBILE MONEY IN INDIA

In India , a billion of people are " not covered by banking services " and to rely on funds or informal financial services that are usually dangerous, inconvenient and expensive. However, more than a billion of these people have mobile phone. It provides a framework for mobile money bringing mobile technologies are used to provide convenient and affordable financial services to insufficient degree.

For years in India , mobile phones are to be used for banking , such as account balances and transaction details in real time purposes.

In India , a variety of companies such as Airtel , Loop Mobile, Obopay and Vodafone have introduced Mobile Money. While there are a large number of methods of mobile payments, SMS or text message seems to be first choice because it is easier and easier to use.

The latest mobile payment services India, money - on - Mobile (MoM) argued that recently clocked 67.5 million unique visitors as of August 31, 2013, which was 4.9 million unique visitors last month[26]. CALPIAN (OTCMKTS: PPITS), which states the service is now supported by 157.860 persons, an increase services industry has increased in size by five times , with more than 100 mobile money deployments alive in the world today - 80% of which are in emerging markets[26] .

MoM currently has 8.8 million active users 30 days of July 2013, marginally higher than the previous quarter and the previous month.

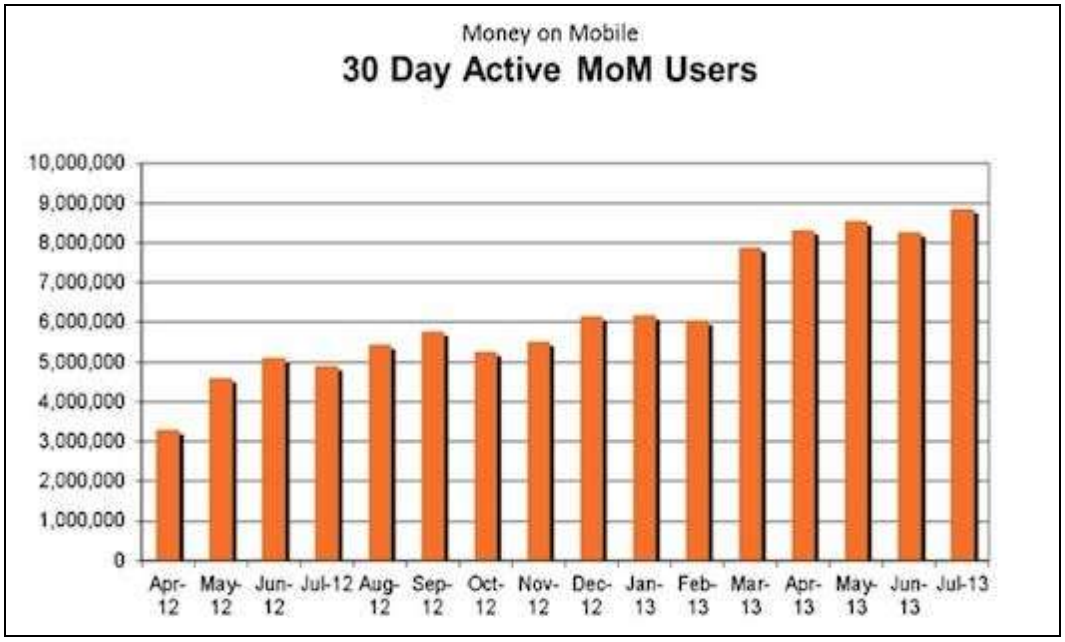


Fig.2.2: Active MoM users in India[26]

In India, Airtel Money is the most popular, especially due to its classifieds mobile payment, network coverage and network of customer service centres across India. With Airtel Money, we can register and create an account on our mobile, and is then topped Mobile balance in the account by visiting a customer service centre or online Airtel through the banking network.

2.2.4 MOBILE MONEY IN RURAL INDIA

The use of mobile phones in rural India is growing because the advantages of using mobile phones for mobile money transfer are now being understood and realized by rural dwellers.

Both mobile operators and manufacturers are indulged in increasing the awareness of people living in rural areas of India , and this has resulted in strong devepolment for both, since the mobile phone users and subscribers has increased.[9]

Poor, rural women are the least likely to use mobile money

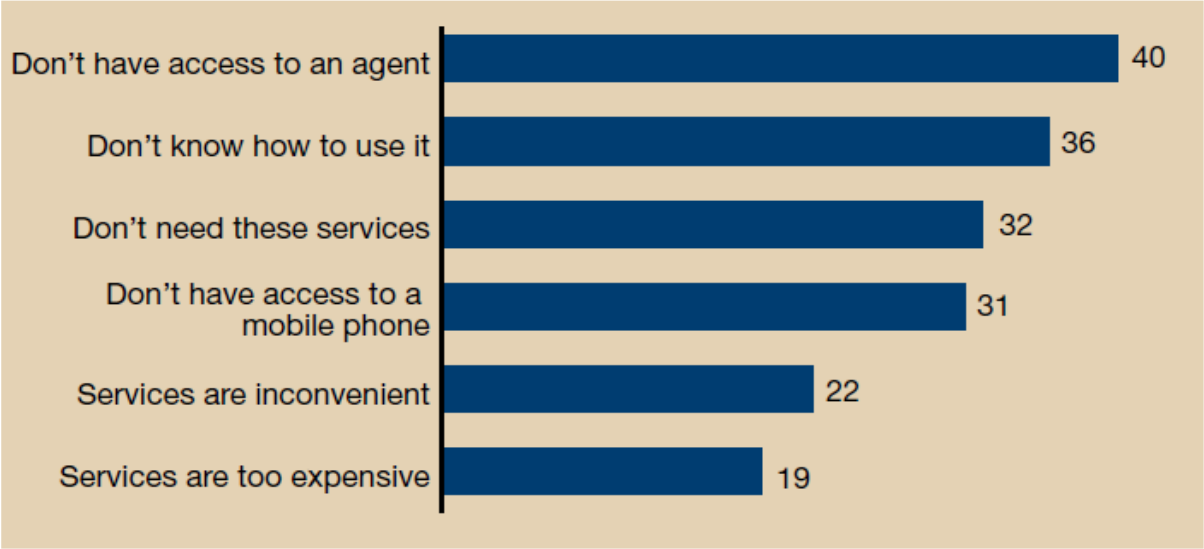
Using mobile money differs significantly by demographics, with rural women below the line of the least likely to use poverty and urban men above more likely to use the poverty line. Across every demographic breakdown, urban residents are more likely to use mobile than rural residents money. [6]

Awareness of mobile money is high, but the lack of understanding continues to limit the growth of mobile money

Despite high levels of awareness, many people are still unclear about the variety of ways you can use mobile money and how to operate the services. Agents said providers should change their advertising approach of simply creating awareness for developing understanding of services and benefits.[6]

Top barrier to mobile money use

In focus group discussions, nonusers describe the factors that prevent them from using mobile money. Many non-users cited cost of mobile money as the main reason for not using the service, however, seemed to have a poor understanding of the actual charges. For example, many do not understand the transaction costs, and some believed that there are charges for savings.
Many users have gained negative perceptions on mobile money through word-of-mouth stories of users in relation to untrusted networks, lack of security and high costs.[6]



Source: InterMedia tracking survey of Tanzanian adults; wave 4, N=2,000; Base n=1028 nonusers; September 2012-October 2012. Multiple answers were allowed.

Fig.2.3: Top six reasons nonusers report for not using mobile money (percentage)[6]

Many active users report insufficient understanding of how to operate mobile money, and many have difficulties performing basic transactions

When asked to rate their level of understanding on a scale of zero to 10 (zero represents no understanding), many active users reported their understanding below five. In the four-wave,

more than a quarter of the active users reported "always" needing help to complete transactions, and another 12 percent reported needing help "sometimes."

Despite continuing problems with understanding how mobile money works, the percentage of users who said they can complete transactions without assistance improved from 50 to 60 percent over the course of the study. Based on the discussion groups, active users seemed to have a better understanding of the security features of mobile money in four wave you in previous waves. Agents and marketing materials that describe the security features are two main contributing factors.[6]

2.3 AUTHENTICATION

2.3.1 INTRODUCTION

Authentication is the act of verifying the truth of an attribute of givens or entity. This may include confirming the identity of a person or a program, tracing the origin of an artifact or ensure that the product is what it claims to be packaging and labeling. Often Authentication includes least one form of identification.

2.3.2 TYPES OF AUTHENTICATION

Among all the above mentioned security parameters authentication of the user is the area of major concern. Users can be authenticated using a number of techniques such as passwords, PINs, smart cards, or tokens. Authentication can further be classified as follows, depending on the technique used for authentication purpose [48]:-

- **Knowledge-based authentication (K):** In this method the user possesses passwords, PINs or something similar like this and uses it to pass the authentication gateway. In this method, the password or the PIN has to be memorised by the user.
- **Object-based authentication (P):** In this method the user possesses the smart cards or the tokens which are thus used for the authentication.
- **Biometric-based authentication (B):** In this method the user uses the unique personal characteristics that he possesses. The authentication process is carried by using the biometric characteristics possessed by the users. Some of the characteristics are fingerprints, voice, iris, face, signature, etc.

Currently, PINs are the most widespread form of authentication used [42]. Since no other method of authentication is available in the market so the users have become addicted to the habit of using passwords or PINs for the purpose of security, or more precisely speaking, authentication. Authentication process in many mobile money transfer applications available in the market uses the password or PIN protection. As compared to the debit cards which require only the signature of the user to complete the payment process, the uses of PIN in the mobile devices to access the mobile money transfer applications provides a far better and secure method. As in case of using a money transfer application from a mobile device the user first has to enter a PIN to access the SIM card, therefore this itself provides a clear identity of the user of the SIM card. Moreover, PINs are harder to guess or crack as compared to the signature copying [49].

If for authentication lengthy and complex PINs are used then it will be difficult for the hacker to crack or guess the PINs; but along with the lengthy and complex PINs comes the problem of memorising it. It becomes very difficult for the user to remember such a long and complex PIN, thus, the user might write it down somewhere to memorise it when needed but this again gives rise to a situation of threat as the PIN written could be copied or stolen or even lost. Thus, it raises the question on the security of the system again [43].

From the above study we can conclude that so far the best method for authentication is the use of biometric with PIN. The biometric authentication is the method of identifying and verifying the identity of the user through the biometric traits. These biometric traits are believed to be unique for each individual around the world. A list of advantages has been mentioned in the above sections which proofs that the biometric authentication is far better than the authentication using PINs or passwords. The most important advantage of biometric is that it cannot be either stolen or forgotten or could be transferred to other person [43][50]. These advantages of the biometrics make it more reliable and secure method when compared to the token-based and object-based authentication techniques. Furthermore, its non-transferable property makes it a strong tool against repudiation [43].

As authentication being the essence of any Mobile Money system, thus the selection of the method of authentication must be made with a great care and analysing each and every minute details of the Money transfer system.

2.3.2.1 OBJECT BASED AUTHENTICATION

These systems typically use tokens for authentication , that is object that can authenticate a user. Common examples are modern ATM cards physical keys, proximity cards, or credit cards. Tokens are good because they are simple. Physical keys, for example, are widely supported and cheap to produce and use[7].

Idea used for this authentication have their own weaknesses, however. Because they are simple and cheap to produce. This makes them vulnerable to fake. As they are typically a physical object or device that can be easily stolen . For this reason, the tokens are typically used with some other method, such as a PIN code to reduce its utility in case of theft.[7]

We have used UID as object based authentication device in this thesis.

2.3.2.1.1 UNIQUE IDENTIFICATION CARD (UID)

2.3.2.1.1.1 INTRODUCTION

In India, 27 January 2009 it is great day in Indian history, on this day Unique Identification Authority of India (UIDAI) was established. At the beginning of this project it is imagine covering nine different states and four union territories. So the resultant the Unique Identification number (UID) is issued firstly in Tamil Nadu, West Bengal, Andhra Pradesh, Maharashtra, Orissa, Gujarat, Karnataka, Goa and Kerala and the also issued in the union territories of Lakshadweep, Andaman & Nicobar Islands, Dadar & Nagar Haveli an Puducherry. At all these placed the Unique Identification card (UID) shell be issued firstly and the target to completely in 2010 early. UIDAI is expected to provide UID to around 60 crores people in 4 to 5 years.[8]

2.3.2.1.1.2 WHAT IS UID (UNIQUE IDENTIFICATION)?

The ways in which such a system is applied is dependent on the country, but in the majority cases, a citizen is allocate a number at birth or when they get in touch legal age (normally the age of 18). Noncitizens are allocating such numbers when they come into the country.

Algorithms used in UID is (modulus 10).

Aadhaar is meant for people of all ages (including children) in order to establish identity . Because Aadhaar is only for individuals , it is different for all members of a family. Uniqueness of each individual to decide , the demographic details (residential address information) of the person and his / her biometric data (photograph , iris -scan , fingerprints) collected is stored in a centralized database.[34].

Fig. 2.4: AADHAAR card

2.3.2.2 KNOWLEDGE BASED AUTHENTICATION

Usually computers use passwords, the "something you know" factor, for basic authentication. Passwords are most widely used and the simplest model to implement authentication. Unfortunately, models of passwords are also the weakest model authentication because passwords are guessed or stolen with relative ease. Users tend to choose weak passwords. They want to charge with the creation and maintenance of a relatively secure password. This type of weakness, being so common, makes any model password vulnerable.

We have used one time password for implement knowledge based authentication.

2.3.2.2.1 ONE TIME PASSWORD

2.3.2.2.1.1 INTRODUCTION

Authentication is a basic trouble in the field of Information security. Getting a user password and gain access to critical system is not a tedious task for any hacker and if they hack a account once, they can continue to access data unless the password is changed by account owner. As the authentication techniques are improving system, attackers are also improving their system to steal important information. So it is advised to use 2 factor authentications in very important and confidential data [39].

2.3.2.2.1.2 WHAT IS ONE TIME PASSWORD?

"One-time" as the name depicts it is only used once and that too for a short span of time. The algorithm that is used to generate OTP is psuedorandomness.
There is a time synchronisation between the client and the authentication server and also it works for short period of time as it is already being mentioned .OTP works on token system. Each time user uses a new password (or token) which is dead after a particular time.

2.3.2.2.1.3 TECHNIQUE BEHIND OTP

One time password should not be confused with “One –Time Pad”[37]. One time password is easy to heard and use but practically it implements a strong technique for encryption. One Time Password refers to a secret Password that is shared between prover and verifier and used only for one. if it is used once, then it can’t be reused again or we can say it will not remain valid.[37]
Systems that use One-Time password schemes; use concept and rules and mechanisms for the two parties (prover and verifier) to share One-Time Password. Weakness and efficiency of a given scheme vary depending on the used scheme but concept is unharmed.[37]
There is basically two types of methods which are used for providing “One time password”

- RSA SecureID
- HOTP

2.3.2.2.1.4 Limitation of OTP

OTP systems limit themselves to authenticate a user. It is not used for authenticate a transaction. But OTP systems have a bright future as they can also be used to authenticate a transaction by implementing some more security controls [37].

2.3.2.2.1.5 METHOD OF GENERATING OTP

There are basically two methods by which all One Time Password are generated:

1. TIME SYNCHRONISATION:-A security token or we can say a clock pulse is comes into work on which OTP works. For that particular clock pulse OTP works.

2. MATHEMATICAL ALGO's:-A mathematical algorithm has been used to generate the one time password. Next one time password depends upon the previous password generated. The algorithm that is related with the OTP generation works on inverse function (i.e. f inverse).

2.3.2.2.1.6 ONE TIME PASSWORD IN BANKING SYSTEM IN INDIA

Today, each and every bank uses One time password to increase security level. Abhishek Rajan, head of Mobile Commerce Business at One97 Communication explains the way needed by customer to snd an SMS to his bank's designated shortcode/number[40]:

Basically format of SMS containing One Time Password in bank system made up of a keyword with last 4 digits of his credit/ debit card number. For e.g. Customer of Citibank needs to send SMS 'OTP XXXX' to 52484 to get his OTP . Here XXXX are last 4 digits of card number. Then user receives a SMS containing One Time Password which is valid only for a single transaction and tends to be expires after a short period of time[40].

In situation where user forgets to apply for generating OTP before the transaction, associated bank automatically sends him one time password immediately when user insert card in the IVR. The OTP requires after one use even if the transaction is not successfull.

The validity period of the OTP, varies from bank to bank, according to rajan[40],

- Axis Bank: OTP will be sent by SMS automatically after you have entered Card details on IVR
- Citibank: SMS 'OTP XXXX' to 52484 or 9880752484 (OTP valid for 30 minutes)
- HDFC Bank: SMS 'PWD XXXX' to 9717465555 (OTP valid for 2 hours)
- ICICI Bank: SMS 'IOTP 16-digit card number' to 5676766 (OTP valid for 24 hours)
- State Bank of India: SMS 'OTP XXXX' to 5676791 (OTP valid for 12 hours)
- Standard Chartered Bank: Online registration process (OTP valid for 24 hours)

Fig. 2.5: Validity period of OTP in various bank of India

2.3.2.3 BIOMETRIC AUTHENTICATION

2.3.2.3.1 INTRODUCTION

As defined by Nanavati [42] biometrics is the "automated use of physiological or behavioral characteristics to determine or verify identity."

While a more detailed definition is provided by Bolle [44] who has defined biometrics as:

> *"Biometrics refers to identifying an individual based on his or her distinguishing characteristics. More precisely, biometrics is the science of identifying or verifying the identity of a person based on physiological or behavioral characteristics".*

Biometric analysis a person by measuring certain aspects of the individual anatomical or physiological (such as your hand or fingerprint), some of the deep-rooted skills, or other behavioral characteristics (such as your handwritten signature), or something that is a combination of two characteristics (such as voice).

2.3.2.3.2 DIFFERENT TYPES OF BIOMETRICS

Biometric methods are largely classified into two categories – namely behavioral biometrics and physiological biometrics. There is also a third category of biometrics which is a combination of the above two categories, hence the name of the third category is combination biometrics.

All the three categories are discussed in details below.

Behavioral biometrics: Behavioral biometric is the method of authenticating a person or a user on the basis of the behavioral aspects of the person or the user. Behavioral aspects of a person include the features like signature, voice, keystroke, etc. In this method the user is verified using the active traits of his behaviour (Wolf et al., 2003). These active traits are measured with respect to a particular time period and analysed and hence recorded (Nanavati et al., 2002, p. 42). This record is then used to validate the user/person against the live sample of the active behavioral trait.

An example of this process is the signature verification technique. In this technique the factors like the writing speed, pressure and time taken is measured and calculated. Thus, anything measured in a time frame is known as behavioral biometric. Since, behavioral biometric are dynamic in nature; so it is believed that they tend to change with time.

Physiological biometrics : When the people are analyzed on the basis of the physical characteristics of the eye , fingers or skin and evaluated as unique characteristics , these characteristics are known as physiological biometric identification methods. The physical characteristics of a person is unlikely to change during his lifetime, thus, these characteristics are permanent in nature. They do not tend to change with time unless, barring any accidents or other incidents of wear and tear. These traits are acquired by a person at the time of his birth and continue to be with him all his lifetime. Various types of physiological biometric technologies involve facial recognition, retina scanning, iris scanning, fingerprint recognition and hand geometry.

Combined biometrics : there are a few methods that are the combination of both the physiological and the behavioral biometrics method. Hence the name of the technique is the combined biometrics technique. The combined biometric technique makes use of the both traits of a person; it analyse the physical traits of the person based on his behavioral aspects of his nature. Example of such a technique is the speech recognition technique. The speech recognition technique analyses the physical aspects of the voice such as the vocal tract, modulation and nasal cavity of that person along with the behavioral aspects like accent and pronunciation [42].

2.3.2.3.3 REASONS FOR USING BIOMETRICS

The current verification process used for the purpose of authentication is working quite nicely and people are used to this method and also, most of the applications in the market offer these authentication methods. But there is a need to change this conventional method of authenticating the user. There are number of reasons that suggest the change of the current authentication system with the biometric-based authentication system. The reasons behind this scenario are listed and explained in the following section:-

i. **Security:** As explained previously, the biometric-based authentication is far better approach than the token-based and knowledge-based authentication [42]. The one reason behind this is that the biometric authentication uses the human traits for the authentication purpose while the other two techniques uses PINs, password, smart cards or tokens [43][42]. Moreover, the traits cannot be forgotten, stolen or cracked or transferred to anyone else. The use of biometrics in m-payments will make it more acceptable in the market both by the customers and by the merchants as well.

ii. **Convenience:** With the use of the biometric-based authentication technique there is no need to memorise that passwords or PINs or to carry along with the smart cards or the tokens. Biometric authentication methodology makes use of the biometric traits which are in-built features of a person's physical or behavioral aspects. Thus, it is easy to use the biometric-based authentication system as compared to the token-based and knowledge-based authentication techniques. Thus, the convenience that this technique provides to the users had made it popular and will make it acceptable widely.

iii. **Increased Accountability:** With the use of the biometric authentication the accountability of the systems has improved greatly. The unique characteristic of the biometrics that it cannot be transferred to anyone has removed the buddy-punching systems [42]. However, this technique also provides the auditing of the transaction and helps in keeping a check on the customer and also the merchant using the payment application.

iv. **Non-repudiation:** Non-repudiation is the method that affirms the completion of a financial transaction. Non-repudiation is required so that neither the sender nor the receiver could deny about the completion of the transaction. Biometric authentication has come out as a solution to the problem of the repudiation [43]. Since biometric cannot be transferred to anyone thus it is believed that if an transaction is started it is a started by the intended user only and he cannot back out once he has started the transaction.

2.3.2.3.4 METHODS OF BIOMETRIC AUTHENTICATION

The various different categories of the biometric technologies available are as follows and are explained below:-

i. Face Recognition : This technique is used to identify people from the face of still or video pictures images [10]
ii. Fingerprint identification : This technology do the authentication using the fingerprint . A fingerprint is a pattern of ridges and grooves on the surface of the fingertip. [11]
iii. Retinal pattern recognition : This technology perform the authentication by scanning their eyes to verify people 's identity. The retina is the innermost layer of the eye . Vein pattern from the surface of the retina is formed beneath the sole of each individual [12] .

iv. Iris based recognition : This technology uses the iris scanning technique for authentication. Colored part of the eye is the iris. It is located in the front of the eye around the pupil. [13]

v. Voice recognition: Also known as speech recognition. This technology records the human voice and then uses it for the authentication purpose. The audile characteristics differ for different people in the world no two person has the similar audile characteristics and voice recognition technique makes use of this property of speech. These audile patterns presents both the physiology (i.e., the shape and size of the mouth and throat) and learning behavior (i.e., voice tone , speaking style) [41][13]

vi. Signature recognition : This technique is used to verify the individual 's signature. Signature varies widely. It is based on measuring the dynamic signature features, such as the use of speed, pressure and angle , when the standard of a person signed recording mode (e.g. signature) [41][13]

We have used fingerprints identification as biometric authentication method in this thesis.

2.3.2.3.3.1 FINGERPRINTS

1. **WHAT IS FINGERPRINT SCAN?**

   Fingerprint scan is also renowned as finger scan. It is oldest and widely used biometric technique of authentication. Fingerprints are considered ideal means of identification. Fingerprint scanning is the process of taking human fingerprints and then storing them in database. It saves image in digital form.

2. **FINGERPRINT PRINCIPLES**

   Some important facts about are given below:

   - Every individual has his own unique fingerprints. No two individuals can have same pattern of fingerprints.
   - Fingerprints remains unchanged for lifetime.
   - “Fingerprints of a seven months old fetus is completely developed and finger ridge configurations remains same throughout the life of an individual except due to accidents such as bruises and cuts on the fingertips”. (Babler, 1991)
   - Two unrelated persons rarely have any kind of generic similarity in their fingerprints.
   - There is some generic similarity in the fingerprints of parents and child.

- Identical twins have a lot of similarity in their fingerprints.[33]

3. TYPES OF FINGERPRINT SCANNER

Fingerprint scanner is a tool used for fingerprint scanning. There are two type of scanner:

1. Optical scanner
2. Capacitance scanner

These scanners get an image of humans fingerprints and then search for a match for the fingerprint in the stored database.

1. OPTICAL SCANNER

Optical scanners are oldest and most widely used scanner. These scanners are used by majority of companies. These scanners provide resolution up to 500 dpi and are fairly inexpensive.

Optical scanner look like the figure given below . An optical scanner operates by a shining light on their fingerprint and taking a digital photograph. If someone has ever photocopied his hand, he will get to know exactly how the scanner operates. Despite of generating a untidy black photocopy image is put into a computer scanner. The scanner possesses a device sensitive to light known as ACCD (charge coupled device) to generate a digital image chip. The computer analyzes the image itself, by choosing only the fingerprint, and then uses a advance pattern recognition software to get it changed into a code[32].

Fig. 2.6: Optical Scanner

CAPACITIVE SCANNER

Fig 2.7: Capacitive scanner

Capacitive scanner looks like the image given above. Capacitive scanner take measurements of fingers in electrical way. When the fingers are on the upper part, the lines in our fingers come in contact with the surface whereas the spacing between the lines stands clear of that. we can also say, between every part of finger and the upper part there are variable distances .the capacitive scanner makes a image of the fingerprint by taking measurement of these distances. these types of scanners are a little bit similar to the touch screen on devices[32].

METHOD OF STORING AND COMPARING FINGERPRINTS

In 1900, fingerprints scan were first used in the field of crime investigation by Sir Edward Henry of the Metropolitan Police in London, England. At that time, this technology of fingerprint scan was not developed, so it was very tedious task to compare two fingerprints. They were used to compare tardily and laboriously manually. At that time crime investigators used to took fingerprints from a crime scene and another fingerprint of the suspect then simply compare them manually using magnifying glass or microscope. So it was really a cumbersome and lengthy task to do[32].

But nowadays, it is not a tedious task. It just take few seconds to compare two fingerprints. Only specific characteristics that are unique to every fingerprint are used to being filtered and saved in encrypted form as biometric key or mathematical representation. Fingerprints are not saved in form of image, they are saved in digital form i.e. in a series of numbers(a binary code). Algorithm can not reconvert the digital image to original image.[52]

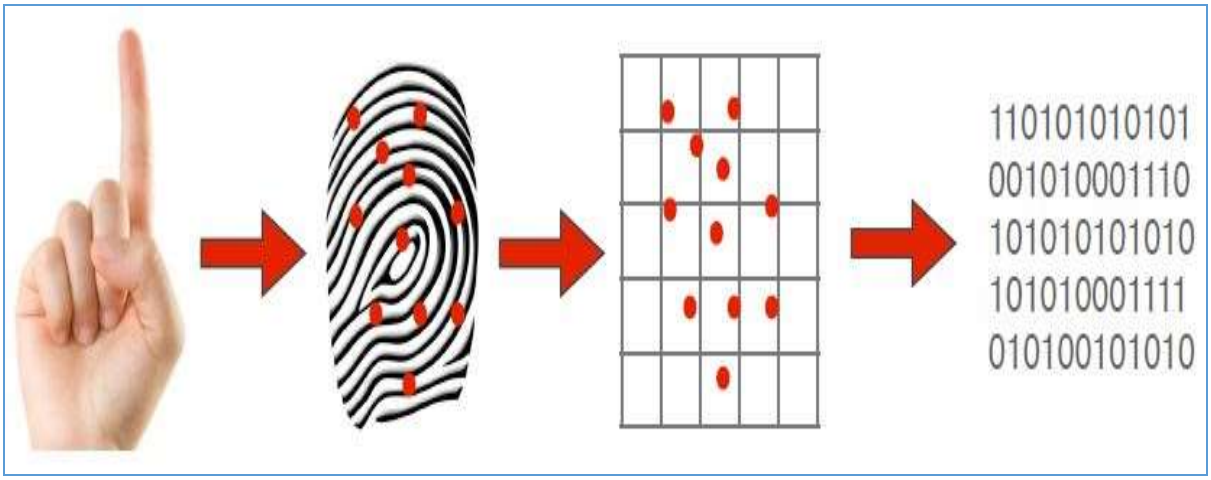


Fig. 2.8: Storing procedure of fingerprints[52]

FINGERPRINTS CLASSIFICATION

A large number of fingerprints are collected everyday. So database is always very large. Classification is basically required for reduce the search time and complexity. Fingerprints are made of ridges pattern. According to these ridges pattern, fingerprints can be in three classes[33].

- Loops
- Whorls
- Arches

1. **Loops**

   60-65% of the population has loops in their fingerprint. Loops are made of one or more ridges entering from one side, curvinf and then existing from the same side There are basically two types of loops:-

   - **Ulnar loop**

     Ulnar Loop tends to open toward right or the ulna bone. Figure given below shows the image of Ulnar loop.[33]

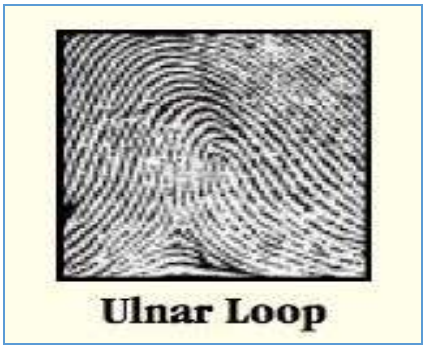


Fig.2.9: Ulnar Loop

- **Radial loop**

  Radial Loop tends to open toward the left or the radial bone. The image showing the Radial loop pattern is givan below:[33]

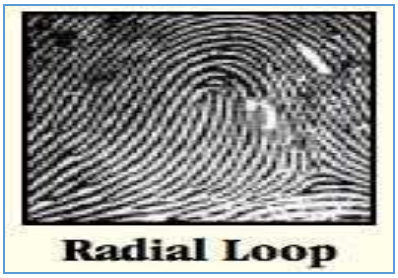


Fig.2.10: Radial Loop

2. **Whorls**

30-35% of the population's fringerprint are made up of whorls. Whorls patterns are made up of two type lines and two deltas. Type lines are ridges that are separated. There are basically four types of whorls[33]:

- **Plain whorl**

  Plain whorls made up of at least one ridge that makes a complete circuit, **and** an imaginary line from one delta to the other must touch a whorl ridge. Plain whorl looks the image given below:

Fig: 2.11: Plain Whorl

- **Central pocket whorl**

  Central pocket whorls made up of at least one ridge that makes a all over circuit, and an imaginary line from one delta to the other cannot touch a whorl ridge. Figure given below shows the image of central pocket whorl fingerprints.[33]

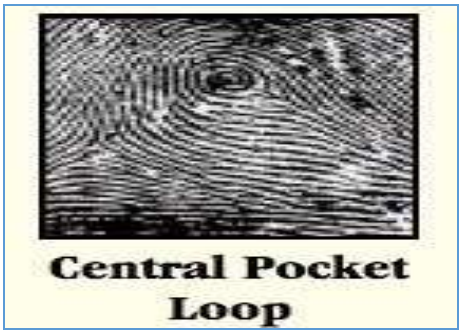


Fig.2.12: Central Pocket Loop

- **Double loop whorl**

Double loop is made up of combination of two loops to make one whorl. Figure given below shows the image of double loop whorl.[33]

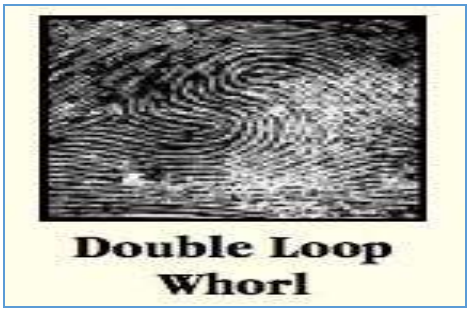


Fig.2.13: Double Loop Whorl

- **Accidental whorl**

  The other whole type patterns which come under these three basic whorl type patterns are called Accidental whorl. An example of accidental whorl pattern is given below[33]:

Fig.2.14: Accidental Whorl

3. **Arches**

Only 5 percent of the population has arches in their fingerprints. Arch ridges tend to enter from one side of the print and leave out the other side. There are basically two types of arches:

- **Plain arches**

  Plain arches used to show a wave like pattern. Pain arches looks like as image given below:

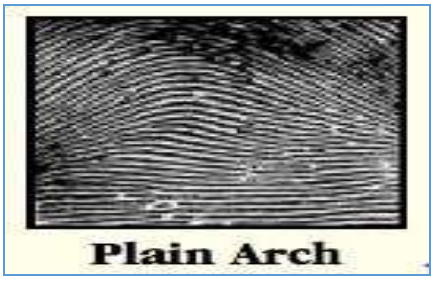


Fig.2.15: Plain Arch

- **Tented arches**

  Tented arches tend to show a acute heel at the centre of the arch. Tented arches looks like the image given below[33].

Fig.2.16: Tented Arch

APPLICATIONS OF FINGERPRINT SCANNING:

Fingerprint scan technology is being used in various fields. Some main appliation are given below:

- Bank security as in ATM card transaction and Mobile Money
- Physical identity(e.g. Airpot)
- ISS(Information System Security)
- UID(Unique Identification)
- Voting
- Passport
- Crime investigation
- Identificatio of missing child
- Secure e-commerce
- Secure m-commerce

2.3.3 AUTHENTICATION IN MOBILE MONEY

In the digital world, security is becoming an area of main focus, where the privacy and security of data is issue of concern mainly. The services provided digitally, especially the mobile services

are considered to be successful and widely accepted among the users only if the services or the system provided to the users are considered to be secure and reliable [45]. But in case of a payment system the main focus lies on the security aspects of the system and how strongly the system handles it. Krueger (2004) [46] has studied and provided a detail that approximately 15.8% people, around 13,000 only, find the mobile device safe when talking about the payment through the mobile devices. In an another interesting study conducted by the Wiedemann (2008) [30], Although the above study results do not exhibit the nature of people towards the m-money system system completely but it makes a little thing clear that people would not like to waste their time in enrolling themselves for an application they don't consider to be safe to conduct or perform. The study was conducted on 1123 people through a questionnaire, from which two-third people represented the "skilled" population [47].

According to the Oxford Dictionary definition of the word security is "the state of being or feeling secure". Application of this payment will be a secure payment in the actual a variety of fraud and privacy attacks a fixed transaction Consumers feel safe use of payment applications. Payment System can be considered safe if it is to meet five security parameters of the payment system.

2.4 SMS

2.4.1 WHAT IS SMS

SMS stands for short message service.SMS is also reffered as texting. Text message generally consists of 160 words including of qwerty keyboard and special characters. SMS texting supports t9 predictive dictionay which is very helpful for typing. With the help of T9 dictionary text messaging is faster on non-qwerty keyboard i.e. cell phones without full keyboard.

The "short" part refers to the size of message i.e. 160 characters including letter ,numbers or symbols(For other alphabets like chinese, size is 70 characters).

Now a days sms is used for checking bank accounts likewise getting message as soon as cash has been credited or debited to your account. SMS is also used for electronic communication.

One of the best purpose solving feature of SMS is "you can talk to a person without speaking".

These days mobile number verification is done through SMS either it is facebook or any other bank account number.

2.4.2 WHY SMS IS MOST WIDELY USED SERVICE?

There is no count of various services provided by Mobile Phones but SMS is most widely used and accepted service after calling service of phone.

It is basically a non-voice communication that allows people to communicate even without speaking. The service is available on all phones whether it a simple phone or a smart phone.

Some of the main reasons behind the popularity on SMS are given below:

1. It gives privacy as two people can have a conversation even without speaking. No one else can hear the conversation.
2. We can talk to a number of people simultaneously.
3. SMS does not required to be replied at the same time when it is received. Person can respond of it whenever he gets time.
4. Text message reduces traffic as it uses less amount of service signal compared to other services like phone calling or email etc.
5. Text message can be easily saved to phone.
6. There are many situation where it is not appropriate to make calls like in meeting, classes, in that case SMS is like blessing.
7. Phone calls generally leads to unnecessary talks. So SMS reduces time to be wasted on phone calls.

CHAPTER 3

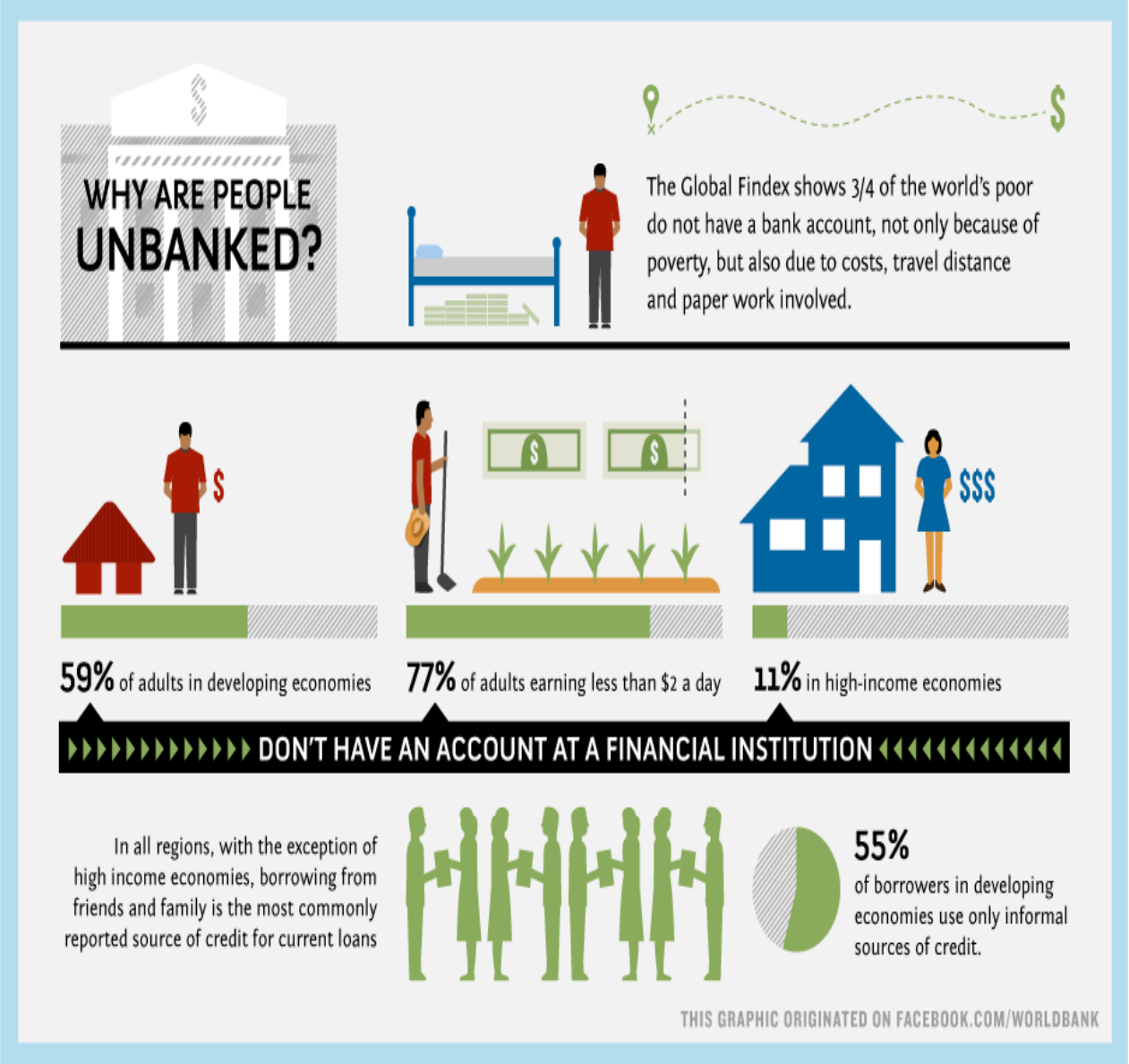
LITERATURE REVIEW

Mobile Money is the fastest growing technology of the day. It has great future in developing countries rather than in developed countries because in developed countries almost all the population is already have bank accounts and using bank facilities conveniently, so this is not required as they can use bank facilities easily. But in developing countries as peoples are not generally well educated and financially strong, so they hesitate to use bank facilities. So there is a strong need of facility like mobile money for unbanked users.[6]

Mobile money plays an important role in the development of any country as it not only reduces the dependency on cash but it also serve the people by providing a platform to access a much wider range of financial services[6].

According to the World Bank, "financial inclusion is defined as a lack of price or no price obstacle in the usage of financial services"[6]. In developing countries, financial services provided by various financial institutes are not being used as people are not well aware of facilities provided by banks. Also there is very limited number of payment tools and financial outlets. As a result a large percentage of the population operates on a cash basis only and keeps themselves outside from the formal banking system. In some cases, informal methods are also exploited to transfer money, which exhibits several risks. Underdeveloped transport systems and services expensive money transfer also help make mobile money more attractive.[6]

"From the regulator's perspective, the concerns involved in allowing mobile operators to offer payment services can be easily addressed. In fact, there is not a trade-off between the participation of financial intermediaries and mobile operators. […] In the end, by allowing all types of participants, the financial regulator leaves the market to figure out what works best, and the customers will benefit from the result.[6]" ,According to Narda Sotomayor Head of the Microfinance Analysis Department Superintendencia de Banca, Seguros y AFP, Peru.



Source: World Bank: Global Findex 2012,

http://www.flickr.com/photos/worldbank/6948286384/, CC BY-NC- ND 2.0.]

Fig.3.1: why people are unbanked

Many mobile money programmes for the unbanked are being funded and initiated by renown institutions such as the World Bank, GSMA and the Melinda and Bill Gates Foundation[6]

M-money application	Countries implemented	Main Features	Technology
M-PESA	Kenya, Tanzania, South Africa and Afghanistan	• P2P transfers • Pay school fees • Pay electricity bills • Pay for goods and services	STK[6], USSD[7]
Easypaisa	Pakistan	• Pay utility bills • Make P2P transfers • Increase air time credits • Save money • Pay for goods and services	USSD and Internet
T-Cash	Haiti	• Receive salary • Make P2P transfers • Pay bills	USSD
Globe GCash	Philippines	• Pay utility bills • Make P2P transfers • Use as a mobile wallet • Increase air time credits • Pay for goods and services	SMS, STK
Airtel Money	India and 14 African countries including Uganda, Tanzania and Kenya	• Make P2P transfers • Pay for goods and services • Bill payments	USSD
MTN Mobile Money	Africa, including Uganda, Ghana, Cameroon, Ivory Coast, Rwanda and Benin.	• P2P transfers • Buy air time • Check balances • Pay utility bills	USSD and STK
EKO	India	• Make P2P transfers • Bill payments • Loan payments	USSD
WIZZIT	South Africa	• P2P transfers • Buy air time • Check balances • View statements • Pay electricity	USSD

Table 3.1: Some popular mobile money applications in emerging economies[6]

3.1 MOBILE MONEY TRANSFER

Mobile Money is a latest technology which provides facility to make financial transactions using Mobile phone.

This technology is used for personal money transfers as well as international transactions. Basically Mobile Money transfer service is used for transaction between two persons or we can say that it is used for private transactions. Mobile Money transactions required sender to go to a nearest remittance center and submit money to be transferred along with a form which must be filled with recipient information. He also has to pay for it. Then receivers and sender both gets a notification message about the transaction then recipient go to the nearby remittance centre or a minor store or restaurant which must be authorized. Recipient has to pay a charge for collecting money[6].

The mobile remittance industry is growing owing to the increased penetration of mobile phones in remote regions and the mushrooming of various remittance service providers, both national and international, for global money transfers[6].

Several methods of money transfer (phone to phone, m payments, mobile money trasfers, etc.) can be performed in a convenient manner using mobile devices across platforms and applications provided by various banks and money transfer companies worldwide. These money transfer services are offered through a network of agents or association with banks, depending on the regulations of the Central Bank and other financial institutions of various nations.

In addition to the mobile wallet, mobile phones can be used for making P2P payments. Some successful implementations of mobile money transfer services, such as M-PESA, Easypaisa and GCASH, are covered in this section[6].

Vodafone M-Pesa is recently launched by Vodafone India with partnership to ICICI Bank in August,2013. It launched its mobile money transfer and payment service 'M-Pesa' here. It has plans to flatten this service in Mumbai and Lucknow in the next few days.

Vodafone M-Pesa is basically launched for unbanked or unbanked population of the India so that they can gain access to financial services without havin a bank account.

" Today, less than 5 percent of villages in India have a banking outlet. Financial inclusion is a national priority and we believe that with 'M-Pesa', we now have the ideal offering to facilitate the same across the country in compliance with all applicable regulations." ,Suresh Sethi, Business Head - M-Pesa, Vodafone India said [30].

This service has planned to be available for serve people through 1,400 specially trained authorized agents and across 130 Vodafone exclusive retail stores in Delhi and NCR region. Vodafone M-Pesa facilitates customers to transfer money to any mobile phone, remit money to a

bank account, make payments for utility bills and deposit and withdraw cash from designated outlets by registering themselves for the service.

M -PESA was launched in Kenya in 2007. It was launched by mobile network operator, Safaricom. It is most famous mobile money transfer technology. “within 5 years of it’s establishment, there are nearly equal 16 million users of mobile money in Kenya, conducting over 2 million transactions every day”. M -PESA now processes more transactions all over the country including Kenya than Western Union has globally and provides mobile banking services to more than 70 percent of the adult population[15].

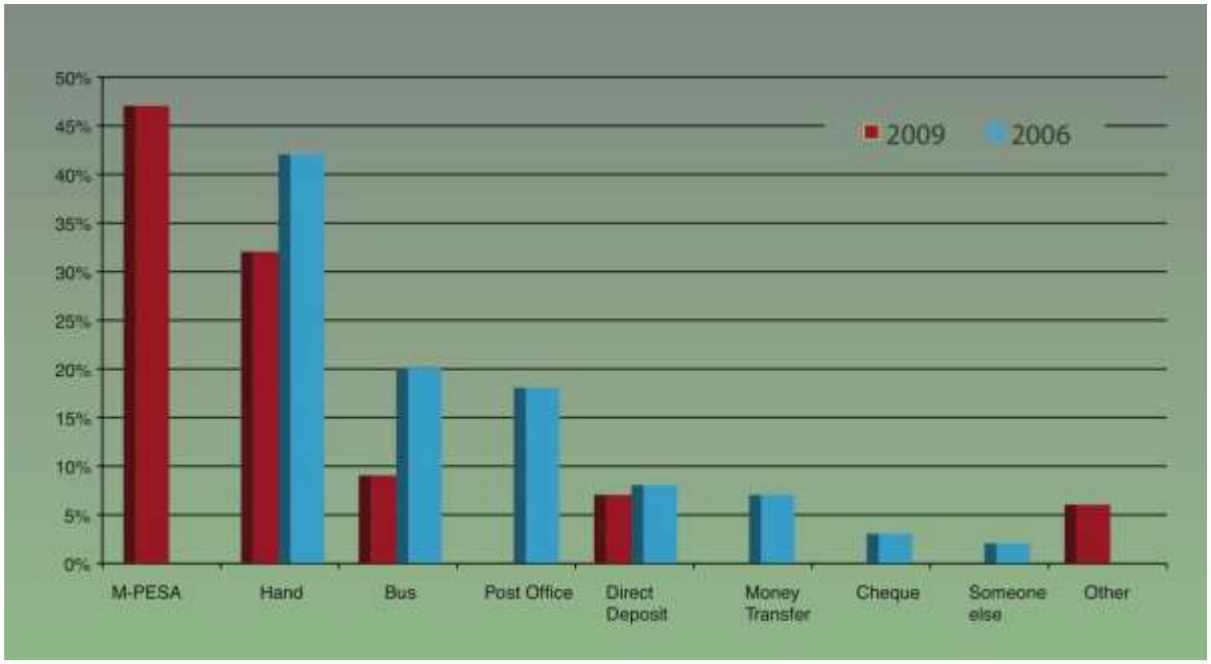


Fig.3.2: Money Transfer Behavior Before and After M-Pesa

Source: FSD-Kenya (2006) and FSD-Kenya (2009)

Basic facilities provided by M-Pesa include Mobile Money transfer, airtime purchase, pay salaries, utilities and other payment online using mobile device and online shopping. Now Mobile Money service M-Pesa is also being provide in Kenya by renown– Airtel, Orange, and Essar (Yu) – and other players have recently emerged to offer complementary services. In addition, many aid donors and their implementing partners have already begun to integrate mobile money into their programs and are at the forefront of this learning opportunity. [15]

Easypaisa Easypaisa was launched by telenor Pakistan partenerd with tamer Micro Finance Bank in 2008. It the first ever effort for introduce branchless banking in Pakistan. Easypaisa provides a easy, reliable and secure way for all Pakistanis to pay bills, transfer money and have a

bank account without having to wait for hours in que. Now easypaisa also provides the facilty to earn interest on savings usig Mobie phone[6].
In Pakistan, any individual can make use of Easypaisa just by visiting theis nearby easypaisa outlet which must be authorized. Easypaisa serve the people At over 22,000 outlets in more than 750 cities and towns in Pakistan. The outlets are open to serve the people 24 hours.
Accordind to the GSMA; Mobile Money for the Unbanked, Annual Report (2011,[16]), " More than 5 million unique users use Easypaisa services every month. Around 117 million transactions worth over Rs. 261 billion have been carried out through Easypaisa since launch." [16]

In India, the HDFC bank has provided a service called **Eko;** this services enables the people to open an accounts (savings account) with the bank at a very low cost. [18]To open such an account, the user visit to the nearby "Customer Service Point" (CSP) in the area and registers themselves with these CSPs. According to the Medhi (et al., 2009), "CSP is defined as the small companies that run more than one company at the same time and place". The service can be used by anyone using the mobile phones of any model. Various services that are offered by this are namely, money transferring, cash deposit or withdrawal, receiving salaries, conducting micro-payments, micro-insurance, etc.[18] Eko has provided the facility of real time transactions and cash management through offering prepaid services which ensures transparency in the system. Eko provided the service of operating an account at a very low amount, the service known as "SimpliBank". This system is marked by the three level security system, the three levels of the security are – first is the mobile phone, the other is provided by the company brochure and the last one is the use of PINs [17].

Airtel Mobile Money was launched in India in 2012. It is widely being adopted by Indian. Is is growing day after day and adding more features to serve the users at it's best[6]. This service is provided by Airtel. Airtel Money provides a quick, easy to use and reliable service that permit user to load cash on theis mobile devices and spend it to py utility bills,make recharges and online shopping.[6] Airtel Mobile money had been launched in 14 countries where Airtel operates, By July 2012. This is success improvements in the early product called Zap. With over 11 million registered users represent about 20 percent of Airtel users, Airtel money is destined to serve the unbanked. Airtel Mobile Money is configured as a separate company within the Airtel operation. It is with the aim of introducing new relevant financial products, main importantly savings and insurance. Besides serving as an easy alternative to cash and credit card payment options, Airtel Money also provides customers the facility to transfer money instantly from an Airtel Money wallet to another wallet Airtel Money and bank

accounts all country.

Framework for Mobile Money Implementation in Nigeria by Ayo, Adewoye and Oni (2011) is a framework proposed to facilitate the feature of transferring money directly by using mobile phones in Nigeria[18]. This system is a combination of the both, the account-based and electronic currency system. The authors proposed a framework with the two level of authentication, first using the mobile phone and the second level of security is provided by the national identity cards of the people. The model proposed will help in the money transfers with the help of the mobile phones in Nigeria [18].

AP Smartcard Impact Evaluation Project, May 2013 by Piali Mukhopadhyay, Karthik Muralidharan, Paul Niehaus and Sandip Sukhtankar relies upon customer service providers (CSP) to process payments last mile on behalf of the contracted banks, using the point of service (POS) for authentication. Since the program was led deploy smart card by the Department of Rural Development (DRD) of the GOAP, the program serves two large social welfare programs administered by the DRD: Mahatma Gandhi National Rural Employment Plan (MGNREGS) and social state-sponsored pension program security (SSP).[19]

A unified smartcard-based ATM card with biometric cash dispenser by Ayo and Ukpere was (2010) designed to deal with the problem of identity theft with the ATM services started in Nigeria. The system designed also helped to users to lower the number of cards they have to carry with them, which is a great significance of this system. While Ayo(2010) has proposed a unified identity system, that makes use of the unique eIDs (electronic-identity) for conducting different transactions across different platforms. The system thus proposed for Nigeria makes use of the national identity cards for the unique identification and as the payment cards [20][18].

GCASH is a Mobile Money application launched ad operated by Globe telecom in the phillippines. It which converts a mobile phone into a virtual wallet for, quick and convenient money transfers. Is is also known as instant money transfer via short message service(SMS). GCASH requires GCASH users to have a mobile phone along with an active SIM card to operate their GCASH account. Globe Telecom issues a GCASH account in which the sender sends money to be withdrawn by the recipient. Addressed an alert indicating the amount sent is sent to your GCASH account. It is basically used for make remote payments, making use of loan service even without visiting bank, pays bill without waiting for hours in long ques and online shopping.[21]

Ay et al. (2007) studied the possibilities for **m-Commerce application in Nigeria.** The author found that there is a lot of scope in the field of m-Commerce application in Nigeria essentially based on the mobile phones as it provides more and more people to get connected with their remotely located earning family members[18]. The author found tha seeing the number of mobile users in Nigeria there is a great scope for the m-Commerce applications[18].

Okereocha (2010) proposed **Quickteller** adoption services and other Internet platform which got huge acceptance by the banks in Nigeria. It was observed that every nine banks out of the fifteen banks use the services provided by the Quickteller[18]. Quickteller provided the services like paying bills using ATM, web portal and point of sale channels. It is also expected that soon it would provide services like money transfers from bank to bank, cash to mobile, ATM to ATM and internet banking [22][18].

.

CHAPTER 4

IMPLEMENTATION METHODOLOGY

Our proposed framework for "UID based Mobile Money implementation in Rural areas of India" is described in this chapter. This framework would enable the sender to transfer money without much overhead of bank processing; also it would reduce the receiver's transportation and processing cost, which will make our proposed model more suitable and flexible.

Here, we are using AADHAAR (UID) for individual's identity authentication. It employs a 3-level authentication using the Registered Mobile SIM, fingerprints and the AADHAAR (UID). Our purpose is to design a mobile money model for especially rural dwellers and unbanked consumers which will be reliable, easy to access, affordable, efficient and timeliness.

4.1 Registration and Authentication

Registration is the process for access restricted services / documents. The registration and authentication process are simultaneously applied in parallel. Actually, the main differences

between the two process is that the registration process is to give the user's personal information, such as name and login password , email id , address, phone , etc. However, in the process authentication verifies that this information is accurate and the information is not used by another person. When these processes are implemented in the Internet then it is called "electronic authentication (e- authentication)". Electronic authentication is achieved by the following factors:

- Knowledge - something the user knows (e.g. user name , password , PIN , questions and secret answers, etc) ;
- Possession - something the user has (e.g. digital signatures, smart cards, etc.);
- Be - something the user is (e.g., biometric fingerprint, iris pattern, face recognition, etc.) [23]

4.2 Authentication Service Provision

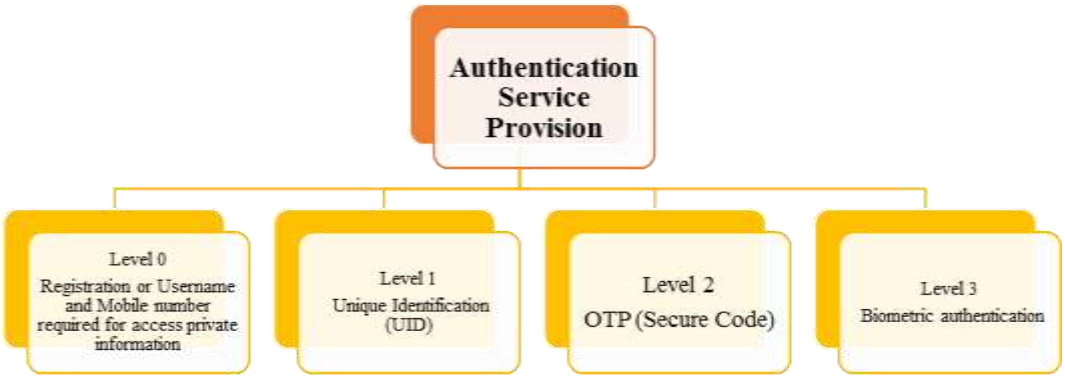


Figure 4.1 : Authentication Service Delivery

Level 0: This is the basic authentication mechanism using username and mobile number. Recipient must be registered by sender. User will have to give his name and mobile number for authentication purpose at this level,

Level 1: At Level 1, recipient will proves his identity using Unique Identification Card number (UID).

Level 2: At Level 2, the recipient would need to prove his/her identity through one time password. For this purpose, a secure code will be provided on his/her mobile phone no, this is entered at the time of transaction at kiosk.

Level 3: At Level 3, the recipient will prove his/her identity using biometrics authentication. This is the highest level of authentication security that would be available to a user. .

4.3 Design Consideration

This framework is for mobile money transfer requires senders to send money to the receiver online by filling some mandatory information. Then both sender and receiver receive a message on their mobile phone containing a unique secure code. Then recipient goes to nearest kiosk to collect the money. Recipient does not need to have a bank account.

Description of the proposed framework is given below:

I. Parties playing key role are:

- Mobile Telecom Operators(MTO)
- All the banks in India
- E-governance kiosks in India
- Kiosk's agent
- Sender
- Recipient

II. Instruments needed to implement the work are:

- National ID cards(Aadhaar)
- Fingerprint Scanner
- Mobile Device

III. Procedure involved is:

1) Registration of Sender
2) Registration of Receivers by sender specifying the following
    - Recipient's name
    - Recipient's mobile number
    - Recipient's address
    - AADHAAR Id of recipient
    - Amount to remit
3) A unique secure code is sent to Sender and receiver

4) Recipient
    - Get SMS notification
    - Shows SMS and UID for processing
    - Fingerprints scanning
    - Cash dispensed via kiosk
5) Bank
    - Debits sender's account
    - Sends notification to recipient and sender

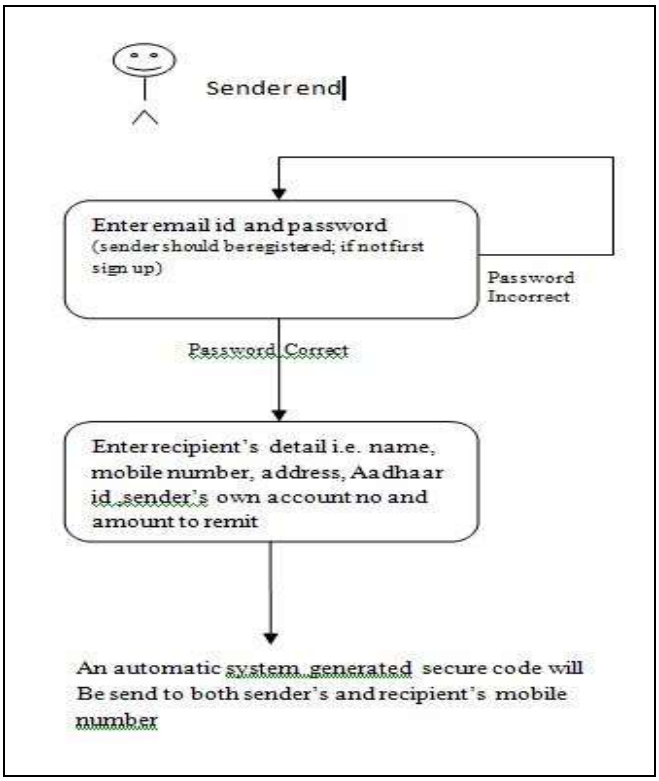


Fig 4.2: Implementation model of proposed work at sender side

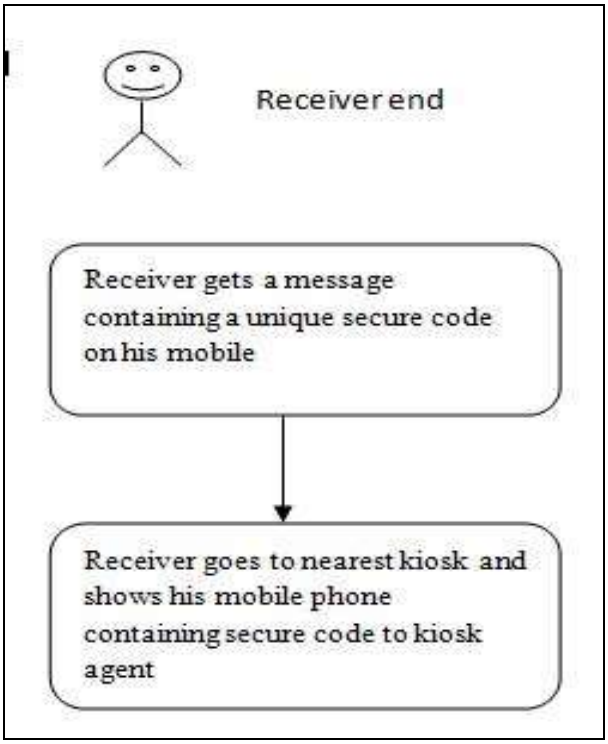


Fig 4.3: Implementation model of proposed work at recipient side

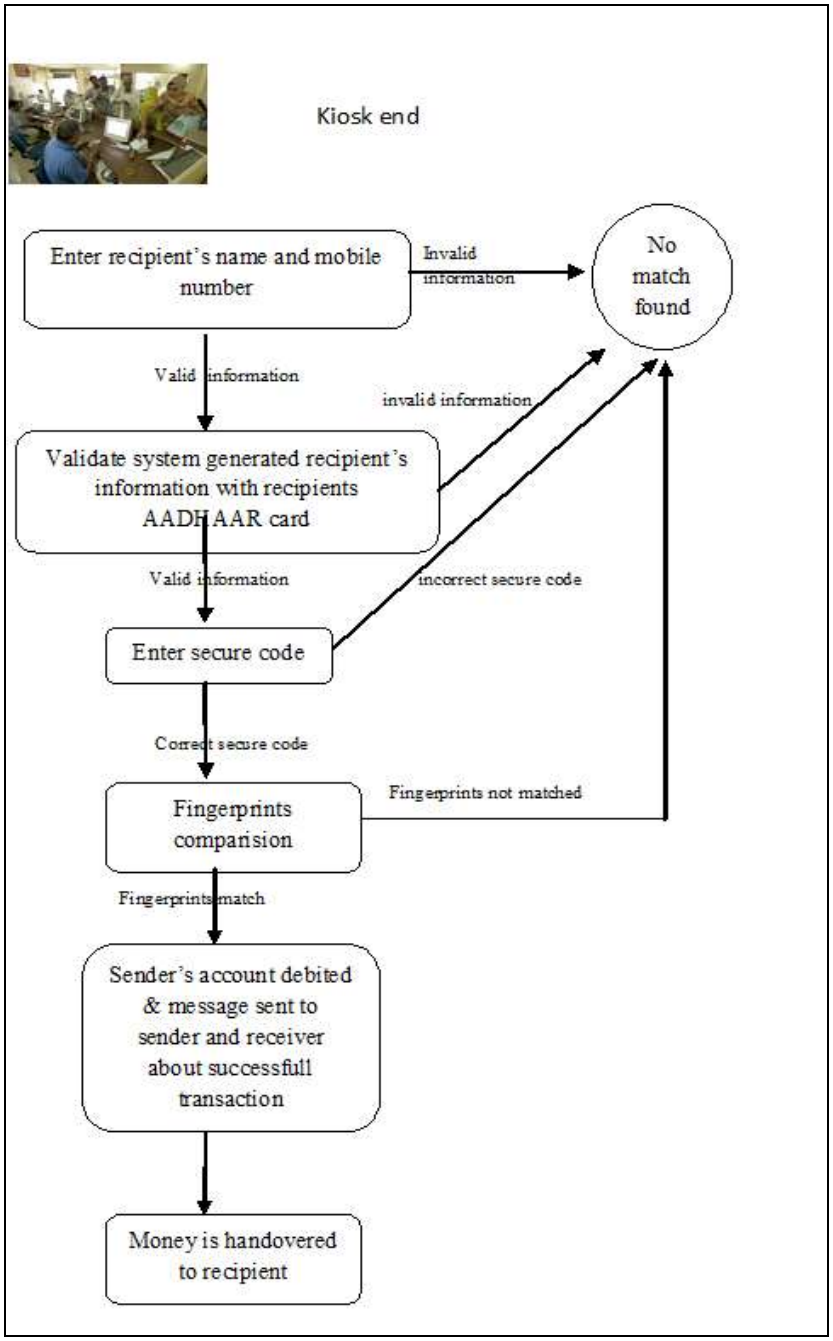
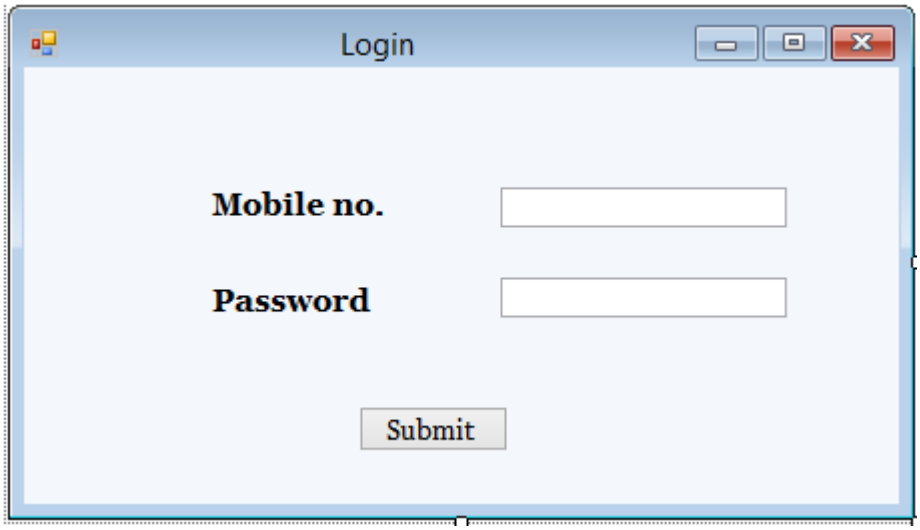


Fig.4.4: Implementation model of proposed work at kiosk side

4.4 Execution of Proposed framework:

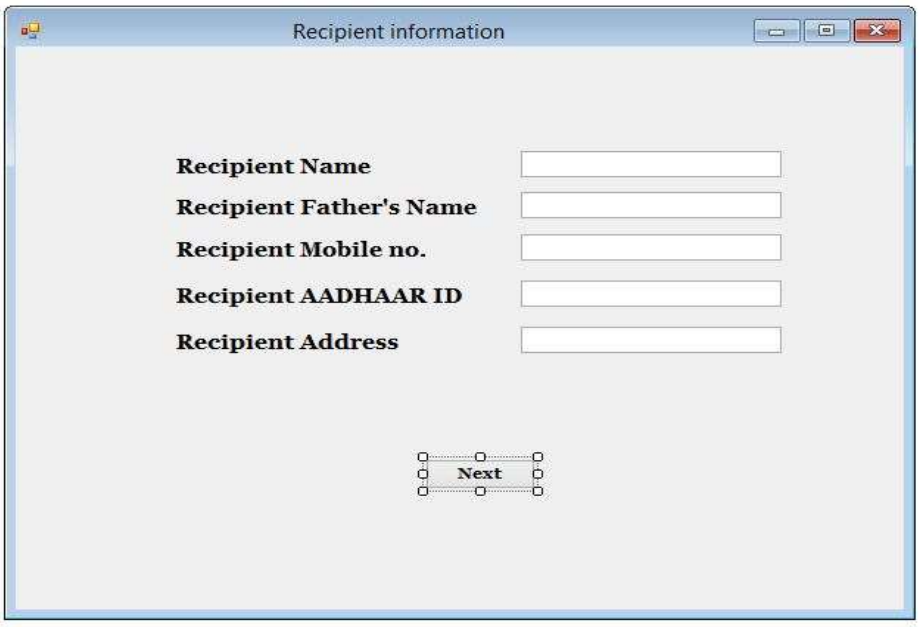
Below we outline the key steps involved in our proposed work. Below we present the system as it is designed to function:

STEP 1: Sender will login with her/his mobile no. and password.(Sender must be a registered user)

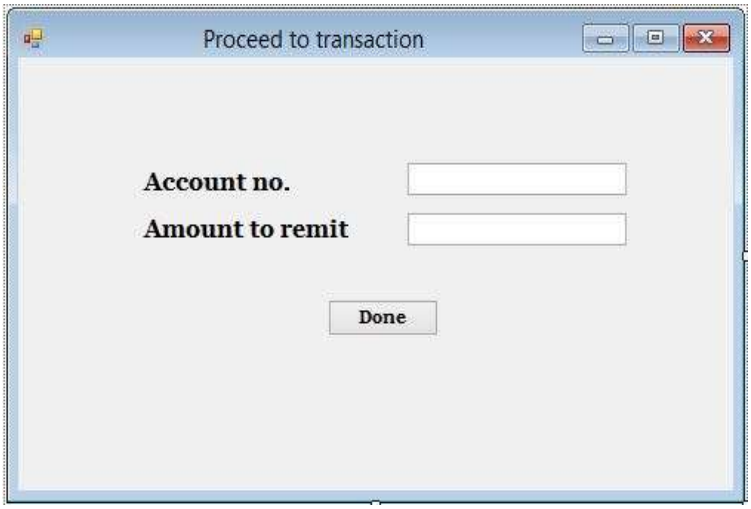


STEP 2: Registration of Receivers by sender specifying the following

- Name of recipient
- Father's name of recipient
- Mobile number of recipient
- Address of recipient
- AADHAAR Id of recipient



STEP 3 : Sender will proceed the transaction by entering his own account number and amount to remit.

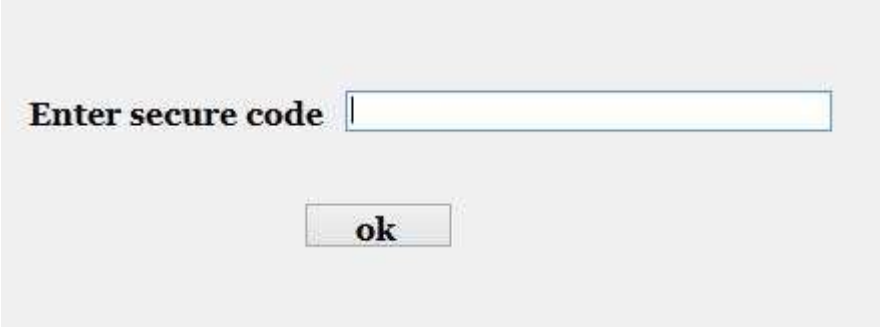


STEP 4: A unique secure code is sent to Sender and receiver which is valid only for one transaction.

STEP 5: Receiver gets the notification and goes to kiosk, then kiosk agent asks the recipient his name and mobile .no.

STEP 6: After entering recipient's name and mobile no. , system generate all the details of the recipient filled by sender and agent will authenticate the recipient by comparing all details with his AADHAAR card.

STEP 7: If recipient completes the first phase of authentication, then he will be asked to show his secure code.



STEP 8: After entering the secure code, system will generate following information about sender:

- Sender's name
- Sender's mobile number
- Sender's account no.
- Amount to remit
- Secure code

Now agent will again authenticate the recipient by comparing one time password(secure code).

STEP 9: If the recipient passes the second phase of authentication, then he will go for biometric authentication (fingerprints scan).

STEP 10: If the recipient passes the third phase of authentication, then cash will be dispensed to recipient and amount will be deducted from sender's account and then a notification message about successful transaction will be send to both sender and receiver.

CHAPTER 5

RESULT

5.1 RESEARCH FINDINGS

A number of Mobile Money transfer methods are currently being used in world. Many of the existing frameworks can be seen to build upon each other by extending earlier approaches with the aim of becoming more complete and robust. The recent development of mobile money has facilitated millions of people who are otherwise kept out from the formal financial system to perform financial transactions comparatively stingily, securely, and faithfully.

Our proposed framework for "UID based Mobile Money implementation in rural areas of India" is more reliable, easy to access, affordable, efficient and timeliness as compare to the existing one. It is especially designed for rural dwellers and unbanked consumers. This enables the sender to transfer money without much overhead of bank processing, also it releases the sender

from the transportation and processing cost, which makes our proposed model more suitable and flexible.

Every step is well defined. The authorization part has been done in every step so as to get the appropriate result. The data collected is more precise and accurate. Main concern for the security enhancement is on the flow of information of the framework and then the authentication planning along with UID's Biometric recognition. The proposed framework has helped to improve existing regulatory tools and mechanisms to minimize cost and time. It has helped to provide a systematic approach for storing citizen information and its implementation which will significantly reduce the costs and time of an internal and external implementation.

After studying all the techniques, the comparative study of the technology is displayed in the following table below:-

Parameters	**Existing Techniques**	**Proposed Model**
Security	2 level authentication	3 level authentication
Authentication	PIN and Password	UID, OTP and Biometric(fingerprint)
Convenience	Sender requires to go to a authorized centre for register himself	Sender does not need to go to anywhere for register himself

Table 5.1: Comparison of proposed model with previous existing techniques

CHAPTER 6

CONCLUSION & FUTURE SCOPE

6.1 CONCLUSION

The system involves 3 level security one of which a new integration is biometric verification of the user before money transfer at the kiosk. In this work an attempt has been made to analyse and develop a secure and cheap model of Mobile Money transfer which involves multi level security, without additional cost.

The proposed model ensure the leakage of information like pin or OTP will not bother the user as no transactions can be made without his biometric(fingerprint) verification.

Our proposed framework enables the sender to transfer money without much overhead of bank processing, also it releases the sender from the transportation and processing cost, which make our proposed model more suitable and flexible. Here, we are using Aadhaar for individual's

identity authentication. It uses a 3-level authentication using the mobile phone, fingerprints and the AADHAAR.

6.2 FUTURE SCOPE

In future this work can also be diversified in the field of mobile money transfer and implementing other type of biometric technique for authentication purpose. The field of biometrics and Mobile Money has to be still explored in a great depth.

The major limitation of existing web security framework is that it refers only to the registration and OTP (One Time Password) part of an authorization and issues such as the exchange of information, backup of data and intelligent search for user/government information are not addressed.

Also the proposed framework have 3 sub framework with sub phases, which give the advantage of more secure login and authorization of database with a time consuming job and hence delay in finding the information. Each sub-category added to the framework has made it more cumbersome to use.

One obvious area not touched upon in this framework is, the chain of risk management. Of course this is an important facet of any security enhance work. This framework assumes that a strong chain of risk management will be maintained throughout the duration of the security implementation. The absence of it on the model above makes no presumptions that it is not important, only that it is implied in any discussion of authorization.

CHAPTER 7

REFERENCES

[1] Dolan, J. (2009). "Accelerating the Development of Mobile Money Ecosystem," Washington, DC: IFC and the Harvard Kennedy School, available at: http://www.hks.harvard.edu/mrcbg/CSRI/publications/report_39_mobile_money_january_09.pdf

[2] OECD (2006) "Online payment systems for e- Commerce," DSTI/ICCP/IE/(2004)18/FINAL (unclassified), [online] available at: http://www.oecd.org/dataoecd/37/19/36736056.pdf

[3] "Implementing a Biometric Payment System: The Andhra Pradesh Experience" by Piali Mukhopadhyay, Karthik Muralidharan, Paul Niehaus and Sandip Sukhtankar, AP Smartcard Impact Evaluation Project,May 2013.

[4] A comparative study of the buying behaviour of rurak and urban consumers towards mobile money phone in by Prof. Mridanish Jha*

[5] The Mobile Money Revolution Part 2: Financial Inclusion Enabler ITU-T Technology Watch Report May 2013..

[6] Mobile Money: A Path to Financial Inclusion, Findings from the Tanzania Mobile Money Tracker Study,April 2013

[7] Authentication Methods and Techniques BY Christopher Mallow

[8] *http://www.UIDAI.gov.in*. , 08/06/2013.

[9] Mobile money adoption in rural India could lag http://www.zdnet.com/in/mobile-money-adoption-in-rural-india-could-lag-7000012538/ By Nitin Puri for Mobile India | March 14, 2013

[10] Yadan Li, Xu Xu. "Revolutionary Information System Application in Biometrics". IEEE International Conference on Networking and Digital Society 2009

[11] Ashbourn, J., Biometric Methodologies in Biometrics Advanced Identity Verification The Complete Guide, 2002, pp.45-63, Springer, London.

[12] Jain, A., Biometrics, WA: Microsoft Corporation, 2005.

[13] Fernando L. Podio: "Personal Authentication through Biometric technologies".Anil K. Jain, Arun Ross and Salil Prabhakar: "An Introduction to biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video- Based Biometrics, Vol. 14, No. 1, January 2004.

[14] Uchebnik cited 05.03.212 , Kriminalistika, cited 18.03.2012

[15] Better Than Cash: Kenya Mobile Money Market Assessment by Loretta Michaels

[16] Easypaisa – banking services made easy, Pakistan , 15 May 2013, See: http://telenor.com/corporate-responsibility/initiatives-worldwide/easypaisa-banking-services-made-easy/

[17] Eko India's Mobile Bank (2010). [Retrived August 20,2011] indias-mobile-bank accessed 2011-08-22

[18] Ayo, C. K., Adewoye, J. O. and Oni, A. A., "Framework for Mobile Money Implementation in Nigeria".

[19] "Implementing a Biometric Payment System: The Andhra Pradesh Experience" by Piali Mukhopadhyay, Karthik Muralidharan, Paul Niehaus and Sandip Sukhtankar, AP Smartcard Impact Evaluation Project,May 2013

[20] Ayo, C. K & Ukpere, W. I. (2010). "Design of a Secure Unified e-Payment System: in Nigeria a Case Study," African Journal of Business Management , 4(9), 1753-1760. [Online] http://www.academicjournals.org/AJBM, ISSN 1993-8233 ©2010 Academic Journals.

[21] ManiegoEala R. (2007). 'Telcos Extending Financial Access to the Unbanked: the Philippine Experience Siteresources,' [Online], [Retrived August18, 2011], worldbank.org/FSLP/.../RizzaManiegoEala_D eliveryChannels

[22] Okereocha, C. (2010). 'The Broadband Revolution,' Broad Street Journal, 29(47), 46- 54.

[23] Enhance security system of E-governance by Govind Singh Tanwar & Chitresh Banerjee, September,2013.

[24] Telecommunications statistics in India available at http://en.wikipedia.org/wiki/Telecommunications_statistics_in_India#cite_note-7

[25] Rural Indians pick up 3 million mobile phone SIMs in June 2013 By Telecom Lead

[26] India Could Surpass Kenya in Mobile Money Market: Clocked 67.5 Million Unique Users By August 2013 available at http://www.dazeinfo.com/2013/09/17/india-surpass-kenya-mobile-money-market-clocked-67-5-million-unique-users-august-2013/

[27] one -time password http://en.wikipedia.org/wiki/One-time_password

[28] http://www.mobileworldlive.com/mobile-money-tracker

[29] World Bank, Asli Demirguc-Kunt, L. Klapper: Measuring Financial Inclusion: the Global Findex Database. April 2012, http://go.worldbank.org/J3T8AZ4KX0

[30] http://indiatoday.intoday.in/story/vodafone-india-launches-mobile-money-transfer-with-icici-bank/1/300737.html

[31] Mobile Money Methodology for Assessing Money Laundering and Terrorist Financing Risk by Marina Solin and Andrew Zerzan

[32] Biometric fingerprint scanners by Chris Woodford,November 11, 2013

[33] http://shs2.westport.k12.ct.us/forensics/04-fingerprints/classification.htm
[34] http://www.myaadhaarcard.in/what-is-aadhaar/comment-page-2/

[35] Kashyap, P.. "The Rural Boom in India", International Journal of Rural Management, 2012.

[36] Imdian phone subscribers up by 3mn in june by telecom news,sep,2013 http://www.newkerala.com/news/story/63362/indian-phone-subscribers-up-by-3-mn-in-june.html#.Up-Bb8QW07w

[37] Replacement for One Time Passwords (OTP) http://security.stackexchange.com/questions/18410/replacement-for-one-time-passwords-otp

[38] OTP (One-Time Password) Registration Guide for PSO2 http://bumped.org/psublog/otp-one-time-password-registration-guide-for-pso2/

[39] Facing authentication threats: one time passwords and transaction signing.

[40] Banks Test One Time Password For Tele Payments In India; RBI Extends Deadline By Anupam Saxena on Jan 3rd, 2011

[41] Jain, Arun Ross and Salil Prabhakar: “An Introduction to biometric Recognition” IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video- Based Biometrics, Vol. 14, No. 1, January 2004

[42] Nanavati, S., Thieme, M., & Nanavati, R. (2002). Biometrics – Identity Verification in a Networked World. New York: John Wiley & Sons, Inc

[43] Rila, L. (2002, October). Denial of Access in Biometric-Based Authentication Systems. Paper presented at the Infrastructure Security: International Conference, InfraSec 2002, Bristol, UK.

[44] Bolle, R., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2004). Guide to Biometrics. New York: Springer Verlag

[45] Rannenberg, K., Albers, A., Figge, S., Radmacher, M., & Rossnagel, H. (2005). Mobile Commerce - Forschungsfragen am Scheideweg der Mobilfunkgenerationen. Paper presented at the MCTA 2005.

[46] Krueger, M. (2004). Internet Zahlungssysteme aus Sicht der Verbraucher: Ergebnisse der Online-Umfrage IZV7. Karlsruhe: Universität Karlsruhe.

[47] Wiedemann, D., Goeke, L., & Pousttchi, K. (2008). Ausgestaltung mobile Bezahlverfahren - Ergebnisse der Studie MP3.

[48] Bolle, R., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2004). Guide to Biometrics. New York: Springer Verlag

[49] Henkel, J. (2001b). Mobile Payment. In G. Silberer (Ed.), *Mobile Commerce*. Wiesbaden: Gabler Verlag.

[50] Currie, D. (2003). *Shedding some Light on Voice Authentication*: SANS Institute.

[51] Contius, R., & Martignoni, R. (2003, 04.02.2003). *Mobile Payment imSpannungsfeld von Ungewissheit und Notwendigkeit.* Paper presented at the Mobile Commerce - Anwendungen & Perspektiven, Augsburg.

[52] What is Biomertrics http://www.bioelectronix.com/what_is_biometrics.html