Design of Improved Algorithm For Mobile Payments Using Biometrics

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:
Jyotsana Goyal
SGVU081090964

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

"Design of Improved Algorithm For Mobile Payments Using Biometrics"

is submitted by

Jyotsana Goyal

SGVU081090964

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 "**Design of Improved Algorithm For Mobile Payments Using Biometrics**" 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.

(Jyotsana Goyal)

……..

Software Engineering

Enrolment No.: SGVU081090964

Counter Singed by

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

DETAILS OF CANDIDATE, SUPERVISOR (S) AND EXAMINER

Name of Candidate: Jyotsana Goyal

Dept. of Study: Engineering Department of Computer Science

Enrolment No.: SGVU081090964

Thesis Title: Design of Improved Algorithm For Mobile Payments Using Biometrics

<table>
<tr><th colspan="3">Supervisor (s) and Examiners Recommended
(with Office Address including Contact Numbers, email ID)</th></tr>
<tr><td colspan="3">Supervisor

Mr. Dinesh Goyal
Associate Professor (CS)
Suresh Gyan Vihar University, Jaipur
dgoyal@gyanvihar.org</td></tr>
<tr><td colspan="3">Examiner</td></tr>
<tr><td>1</td><td>2</td><td>3</td></tr>
</table>

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.

Jyotsana Goyal

CONTENTS

List of Figures

ABSTRACT

Mobile payment is a new and alternative mode of payment using phone. Instead of using traditional methods , such as cash , check or credit card , the customer can use the phone to transfer or pay for goods and services. Customers can transfer or by sending an SMS, use the Java application through GPRS, WAP services, IVR or other mobile communications technology to pay for goods and services

Mobile payment has become an important application of daily activities. The unique advantages of mobile payment over traditional payment have resulted in a tremendous growth of mobile phones. While the increasing demand for mobile applications has increased security issues for both the mobile applications and mobile devices. Development of new mobile devices has served different functions, such as storing sensitive information, access information, and transacting this information through the payment system. In order to protect this information and mobile devices, a well-defined authentication system is mandatory. Biometric authentication is more secure, and very easy to use.

Our goal is to embed biometric authentication systems proposed by us with existing payment model, which can be used to maintain security and access different servers (Websites).
In our model we will be designing a payment system for mobile phone that supports the most basic features like a camera in it. Our model will be not only for smart phone holders but also for the simple phones with a camera.

The process will ensure the verification of the user even though being at remote location before making any transaction. This will be done by designing an application which will be demonstrated on the desktop and in future will be extended to Mobile handsets too. The proposed work will be compared and analyzed with the existing modes of mobile payments.

The biometric authentication will be integrated with encryption of biometric data.

CHAPTER-1

INTRODUCTION

India is the world's second largest telecom market; with 929.37 million mobile phone users. Phone is quite common, even in remote villages. Mobile phone industry is growing at an annual rate of more than 2 million visitors annually. It is expected to reach 1 billion in 2013 to mark. Urban users share was 66%, while the share of rural users was 34%. In May 2011, the monthly increase in the number of users in terms of a net 13.35 million. The 13.35 million new subscribers, 7.33 million people from urban and rural parts of Section 6.02 million. Subscribe monthly growth rate of 55% of the urban segment, while the rural part of the 45% [1]. Given such a background, the phone can be considered as an economically viable tool that enables include access to financial services.

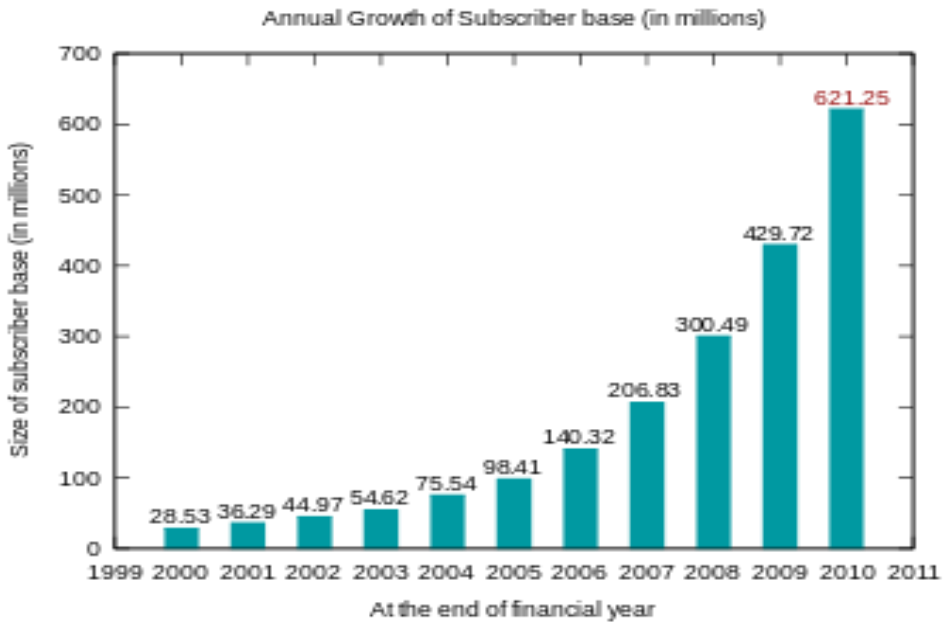


Figure-1 Annual Growth of Subscriber base in India (Source: TRAI, govt. of India [1])

Mobile payment can relax cash handling, storage, and transmission operations aspects related costs associated with cash-based transactions and financial inclusion by providing a strong platform to have a positive impact on social welfare.

With the increasing mobile technology, mobile payment system has paved its way in to people's life. But still not a large portion of people use mobile payment system mainly for two reasons. Firstly, still people in India have a question about the security of their payments made online. While the second reason is, that not all people possess smart phones hat support the mobile payment facility.

1.1 MOBILE PAYMENT

Mobile payment, also known as mobile money, mobile money transfer and mobile wallet generally means the financial supervision and implementation of payment services from or through a mobile device. Besides by cash, check or credit card, consumers can use the phone to pay for a variety of services and digital or hard goods.

Mobile phones, PDAs, wireless tablets, or other devices are the examples of the mobile devices that can be used to connect to the mobile telecommunications network to make payments.

Mobile technology landscape offers various possibilities to realize M-payment. SMS, USSD or WAP / GPRS are the three possible channels through which a GSM phone can send or receive information (mobile data services). Selection of the channel will affect the way mobile payment program implementation. Second, mobile payment client application may reside on the phone, or it may reside in a subscriber identity module (SIM).

A mobile payment system needs to take in to account a few parameters that help it to be accepted widely. The parameters that a mobile payment system needs to take into consideration are as follows - interoperability, usability, simplicity, universality, security, confidentiality, cost, speed, and distant payments. [2] Taking in account all the above parameters, the security parameter is of prime concern and needs to be tackled with more vulnerability in case of m-payments.

Authentication means verifying that the user is who that he claims to be. Authentication can be carried in the three ways :-

- The first method is by using a PIN (Personal Identification Number) or password which is a secret knowledge based technique. This technique is used widely since it provides low cost and fast authentication methods.
- The second method makes use of the technique based on token or SIM (Subscriber Identification Module). In this technique, user removes the SIM from the mobile phone when not in use. But this technique is not convenient to use. Using passwords

and tokens has a number of drawbacks with it, such as they can be copied or stolen or lost or shared or distributed or forgotten. So these payment systems has a greater chances of getting misused by others.

- The last method is the application of biometric technique. In this technique, the unique characteristic of a person is used for the purpose of identification and verification of individual, since each individual possesses the human characteristics that are unique with himself only.

1.2 BIOMETRIC

Biometrics is defined as the science of measuring and analyzing human body characteristics like fingerprints, retina veinal patterns, irises, voice patterns, facial patterns, and hand/finger measurements for the purpose of authentication or identification.

As defined by Nanavati [3] biometrics is the "automated use of physiological or behavioral characteristics to determine or verify identity."

Bolle [4] has explained biometrics in more detail 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".

Basically biometric technique is divided into two broad categories, viz – behavioral and physiological.

i.) Physiological biometric is based on bodily characteristics, such as fingerprints, iris scanning and facial recognition.

ii.) Behavioral biometric is based on the way people do things, such as keystroke dynamics, mouse movement and speech recognition.

Using biometric enabled payment technology people can make payments at market or shops or hotels simply by touching their fingers or by just moving their face or by using other biometric traits. Biometric enabled payment system is far different as compared to the conventional payment system as with biometric enabled payment system there is no requirement of using tokens or passwords for the purpose of authentication; the system

uses the biometric traits for authenticating and making payment or transactions. With the account information biometric payment system will be automatically recognized, in order to complete the payment process.

Biometric authentication is fast, simple and safe. The most important thing is that their biological characteristics are unique, so only the user can access the system. [5]

1.2.1 Various Categories of Biometric Technology

Biometric technology is classified into the following categories, which can be used for authentication purposes in m-payments:

- Face Recognition: The face recognition technology identifies people from the image of their faces taken from a still or video photograph. [6]
- Fingerprints Identification: The fingerprints identification technology uses the fingerprint pattern for making authentication. A fingertip consists of a pattern of ridges and furrows which forms a fingerprint. [7]
- Retinal Pattern Recognition: The technology to authenticate people through scanning their eyes. The innermost layer of the eye is called the retina. Each individual has a unique pattern formed by veins beneath the surface of the retina.[8]
- Iris Based Identification: the iris based technique uses the iris scanning method for authenticating purpose. The eye has a colored portion which is known as iris. Iris is the front portion of the eye that surrounds the pupil.[8]
- Voice Recognition or speech recognition is a technology that records the voice sample of the people and then uses it for authentication. This technology uses the audile or auditory features of the speech which is believed to be different for all individuals. Both the analytical (i.e. shape and size of throat and mouth) and behavioral patterns (i.e. voice pitch, speaking style). [9][10]
- Signature Recognition: This technology uses the signature of an individual for the purpose of the authentication. This is seen that signatures of the individuals differ considerably. The signature recognition technology measures the dynamic feature of the signature, like, speed, pressure and angle at which an individual does the signature and compares with the recorded sample.[9][10]

1.3 PROBLEM DOMAIN

The rapid growth in mobile payment (m-payment) activities has made it a high risk area with a potential for substantial economic loss due to its vulnerability to fraud. Every customer and banking organization has a great concern about the security of m-payment systems, and the ability of the technology to protect users from unauthorized access. One of the highest priorities in the world of information security is confirmation that a person accessing classified information is authorized to do so.

Today, the majority of mobile payment systems use password or personal Identification Number (PIN) and/or card as credentials to authenticate the user's identity. The major problem with this type of identification mechanism is that given a password or card, can it be confirmed that it belongs to the person who presents it? Moreover, passwords or PIN could be forgotten or stolen, which makes it more vulnerable. Hence, we need to design such a payment system for mobile phones that not only authenticate the user or the customer but also have increased levels of security too. A system integrated with a biometric authentication system which adds to the increase in security of the mobile payment system and overcomes the problem of stolen password or PIN. We need a system that could be easily implemented on mobile phones which would enable more and more people to rely on and have access to mobile transactions.

1.4 OBJECTIVE

The proposed model will provide the flexibility to perform any payment or transaction, without involving any external entity except the bank. Moreover, it will enable the user to perform any payment or transaction using the basic phones that supports GPRS and have a camera. This model will be based on customer centric and bank centric approach which is useful for both the bank as well as the user.

The idea behind this is providing a multi-level security checks to authenticate the user to enable any payment or transaction. To provide security, an image encryption algorithm would be designed which would be used to encrypt the biometric image (captured by the mobile phone) to be send over the network for verification purpose.

1.5 ORGANIZATION OF THE THESIS

Chapter 2 covers about overview of Mobile payments, Mobile payments technologies, important aspects of m-Payments, contemporary security in m-payments, biometrics and fingerprint.

Chapter 3 covers review of literature on projects proposed on m-payments and biometric authentication.

Chapter 4 deals with the final proposed framework of m-Payments using Biometric authentication.

Chapter 5 and 6 covers Result and the Conclusions of the research work and the proposed framework.

CHAPTER-2

TECHNOLOGY OVERVIEW

India currently has three hundred million mobile phones, and 100,000,000 are increasing every year. In a small presence, is expected to have over 500 million mobile phones in India. Mobile e-commerce business is a natural descent.

Using mobile devices for day to day communication, collaboration and commercial transactions, is increasing exponentially. More and more users choose mobile channels as part of their daily

lives, in order to manage various aspects of their business and personal activities.

Mobile payment is a normal evolution of electronic payment through which mobile business will be possible. Mobile payment is defined as any payment where a mobile device or machine is used to start, permit and corroborate an exchange of financial value in return for goods and services. Mobile devices or machines may include mobile phones, wireless tablets, and any other machine that communicates with a mobile telecommunication system and allow expenditures to be made.

Mobile payment is coordinated cash, checks, credit cards and debit cards. It can also be used to pay bills admission, taking into account based payment tools, such as electronic funds transfer, online bank charges, direct debit and electronic bill presentment.

With the continuous growth of mobile technology, the payment technology is also growing, which now enables end-to-end payment processing related business (sale) transactions in the background, so that it can carry out the entire business and related end-to-end payment transaction processing, through the mobile channel, that offers customers great flexibility, on how, where and when to process their business transactions in real-time.

However, with the ease of mobile payments there exist some serious security issues, especially, authentication issues. Therefore, we will design such a mobile payment system that integrates biometric authentication model that will equip the mobile payment system with increased levels of security.

2.1 MOBILE PAYMENTS

Also known as M-Commerce or mobile commerce , mobile commerce, is the ability to conduct commerce using mobile devices such as a mobile phone (cell phone), PDA, Smart phones, or other emerging mobile devices like dashtop mobile devices. Mobile Commerce has been defined as follows: “Mobile Commerce is any transaction, involving the transfer of ownership or rights to use goods and services, which is initiated and/or completed by using mobile access to computer-mediated networks with the help of an electronic device. [11]

Figure-2 Various Possibilities through m-payments

m-payments are simply defined as "*payments that are carried out via the mobile phone*". [12]

The basic idea behind the m payment system is that it cannot be carried off without the involvement of a mobile device. So, m payment can be defined as-

"M-Payment can be defined as a payment transaction carried out with the help of a mobile device in an m-Commerce, e-Commerce or POS environment, wherein the mobile device is used to either initiate, activate, confirm, authorize and/or realize the payment process or transaction. The mobile device can also simply be the storage unit that warehouses the significant payment details".[13]

The term Mobile banking (also known as M Bank , m-banking, SMS Banking etc.) means performing balance checks , account transactions , payments etc. using mobile devices such as a mobile phone or personal digital assistant (PDA). Today, mobile banking (2007) is most frequently performed using SMS or mobile Internet , but also a special Program , called a client , can be downloaded to the mobile device and can be used to perform mobile banking.

Mobile business is any activity that involves mobile banking and is conducted through a wireless telecommunications network or from a mobile device. This includes business-to-customer (B2C) and business -to-business (B2B) commercial transactions and also the transfer of information and services through wireless mobile devices. [14]

2.2 Mobile payment technologies

Mobile communication technology offers a variety of methodologies for implementing the m-payments. Essentially, GSM mobile phone can send or receive messages (mobile data Services) through three possible channels - SMS, USSD, WAP / GPRS. The selected channel affects the way for mobile payment schemes. Secondly, the mobile payment Client application that resides on the phone, or may reside in the user Identity module (SIM). We briefly describe the NFC technology as another possibility.

2.2.1 Short Message Service (SMS)

This is a text message service by which the short message (140-160 words) can be transmitted from the mobile phone. SMS Centre stores and forwards the short messages. SMS messages have a different channel of access to phone which is different from the voice channels.[15] SMS can be used to provide information about the account status information with the Bank (information) or can be used to send payment instructions (Transaction) from mobile phones.

2.2.2 Unstructured Supplementary Service Delivery (USSD)

Unstructured Supplementary Service Data (USSD) is a unique GSM technology. This technology is built into the GSM standard and is capable of sending information over the network signalling channel in the GSM network. USSD provides session-based communication, which can support a variety of applications. USSD is a session-oriented transaction-oriented Technology; while on the other hand, SMS is a store and forward technology. The Turnaround response time is shorter for USSD than SMS for Interactive applications.[16]

2.2.3 WAP/GPRS

General packet radio service (GPRS) is a mobile data service for the GSM users. GPRS network provides packet-switched data on the GSM network. GPRS provides various services on the mobile phones, for example, access to the Wireless Application Protocol (WAP), Multimedia Messaging Service (MMS) and Internet communication services like electronic mail and for accessing World Wide Web.

2.2.4 Phone-based applications (J2ME/BREW)

Mobile payment client application can reside on a mobile phone of the customer. For the GSM mobile phones, this client application can be developed in Java (J2ME) and for the CDMA

phones, it can be developed in Binary Runtime Environment for Wireless (BREW). Moreover, mobile phones could be personalized over the air (OTA).

2.2.5 SIM-based applications

In the GSM mobile phone there is a smart card called the subscriber identity module (SIM), i.e., it is a small chip having processing capabilities (intelligence) and memory.

Cryptographic encryption algorithms and keys are used to protect the information in the SIM cards. This makes the applications that reside on the SIM card relatively safer than the client applications that reside on the mobile phones itself. Moreover, whenever the customer acquires a new mobile phone only the SIM card has to be moved. [17] If the application is placed on the mobile phone, then the handset has to be again personalized.

2.2.6 Near Field Communication (NFC)

NFC technology is the integration of contactless smart card (RFID) and a mobile phone. The mobile Phone , can be used as non-contact cards. NFC-enabled phone can be used as RFID tags or Readers. This creates opportunity for innovative applications, in particular in ticketing Coupon.[18] "Pay to buy mobile phones launched by the GSM Association projects (14 mobile operators part of the plan) goals and nine million mobile subscribers Using NFC global common approach.[19]

Figure-3 NFC – Nokia and Visa Cooperation for MPS in Malaysia

2.2.7 Two-chip

Generally the mobile payment application resides into the SIM card. Generally, SIM card is purchased in bulk by the telecommunication company, and then before selling the SIM it

is customized. If the mobile payment application service provider writes a mobile payment application on the SIM card, this has to be done by collaborating with the telecom operators (the owner SIM card) . To avoid this situation, dual SIM phones has two card slots, one for the SIM card and other for the payment chip cards. Financial institutions prefer this method because this way they can exercise complete control on both the chip and mobile payment process.[20] But Customers have to invest in a dual-chip mobile devices.

2.2.8 Mobile Wallet

Mobile wallet is a m- payment application software that resides on the mobile phone , and consists details of the customer (his or her bank account information or credit card information) , which allows customer to make payments using a mobile phone. Single wallet also facilitates the customer to multi-home several debit and credit payment instruments. Several implementations of wallets that are company-specific are in use globally.

2.3 Essential Facets of m-Payments

A number of attempts have been made all over the world to develop successful and efficient mobile payment applications. Among various attempt that have been made the most successful and feasible application of Mobile payment has been in purchasing the parking tickets, the application known as mobile ticketing. UK, Germany Ireland and Australia are examples of countries where the facility of M-Park is being offered. This facility enables to make payment for the parking using the m-payment technique.

2.3.1 Network operator classification of transactions

As mobile payment involves the use of mobile devices, therefore, the physical location of the user or the mobile devices is not important. Thus, m-payments could be used in any environment. Relating to the environment, carriers transaction is classified into the following types [21]:

(A) Local transactions:

Karnouskos [22] defines local transaction as “A local transaction is where the mobile device is present at the payment terminal like a store POS or an ATM and it communicates locally with the payment terminal.”

While Hampe describes local transaction as “Local transactions are known as proximity payments or contactless payments because the payments take place in close proximity to the terminal via short range wireless communication technology” [21] examples of short range wireless communication technology are Bluetooth, NFC or infrared. MNO, Telstra in Australia provides a service called “Dial-a-Coke” is an example of the local transaction; it pays for a drink from selling machine offered by MNO. Using this service the consumer first dials a number provided on the selling machine and chooses an appropriate drink and follows the instructions to choose drink and payment option; and the amount is charged in the next bill [39].

(B) Remote trading :

Karnouskos has defined remote transaction where the payment for the transaction does not depend upon the physical location of the consumer [22]. The consumer could be anywhere or the location of the consumer could be anywhere while purchasing a bus ticket or a logo or a ringtone or game (digital goods). In all the above examples, present a remote environment in which the locality of the consumer is not important while he pays for the transaction. These payments are the case of the browser-based payments such as in the case of digital goods or SMS-based such as in case of m-ticketing [21].

(C) Trading in the individual's environment :

The individual transactions Environment is a payment occurring between a pluralities of devices by the user [21] control. An example of this might be from another mobile credit top-up prepaid mobile account Devices use network operator. A parent can be transferred to mobile calls Devices, such as a child. Mobile payment application, an NGPay in India, plans to move through their remittances provide. Lists these transactions environmental reasons, because biometrics Operators described in this paper is a ubiquitous application, you can use any of these environments.

2.3.2 Different Types of Players in the telecommunication scenario

In an m-Payment scenario players are different bodies or objects or individuals that dive contribution in the m-Payment setup in the ways according to their ability and functionalities. These bodies or objects could be organizations, companies or individuals. In the mobile payment, the players who have a direct involvement in the process of m-Payment are called active Players. They have a direct impact or are a part of the payment

life-cycle Shown in Figure 4. Examples of the active players are Banks and mobile network operators (MNO). While the passive player's are the players that do not directly contribute to the m-Payment life cycle, but plays a supporting in the m-Payment life-cycle.

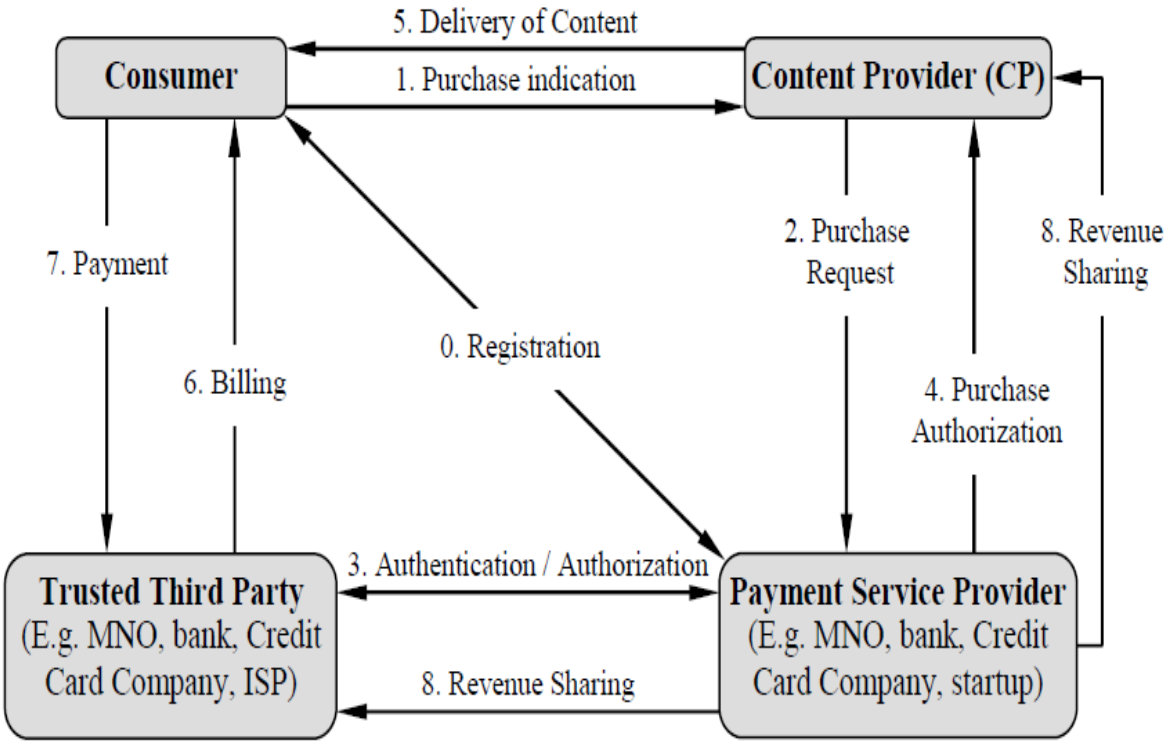


Figure 4 – The Payment Life – Cycle [37]

(A) Active players

- **Mobile network operators :** The main responsibility of the mobile network operators (MNO) is to maintain the framework of the network, i.e., they are the telecommunication providers. The main gist of the MNOs is to efficiently run the mobile network [23] and to dill the customers according to the usage and demands. Practically talking, MNOs and the Mobile Virtual Network Operators (MVNO), are the two types of the telecommunication providers. MNO uses its own network framework while the MVNOs provide the services using the network framework of the MNOs. The contribution of the value chain is to provide some MNO services [24]. Easymobile [40] is an example of an MVNO in Germany, which makes use of the T-Mobile which is a network of the MNO.

  MNO can be seen as an optimal contender to provide m-Payment services. Because the MNOs has a direct billing relationship with the customers, so the bills involving the m-Payment transactions involve the least costs, if applicable [24]. Second,

MNOs provide Mobile telephone services while they also own and control technology infrastructure. Provided that they have a huge customer database [22], mobile network operators can be exposed to potential Carriers consumers their marketing goals, their efforts directly based on the existing consumer behavior. For example, the early adopters who are technology consumers may More prone to try m-Payments, or at least be what is m-Payments.

Mobile operators provides three types of services with respect to the telecom solutions. They offer m-Payment services while acting as a mobile payment services provider (MPSP). That MNO is charging entity can take effect. In many cases, Operators in the Field of micro-payment applications, the MNO finals the bills of the customer purchase using the m-Payment, they provides services similar to the banks which provides credit cards for the card payment applications. Downloading logos, games and ringtones are the best examples for this. Customers Purchase goods and MNO with his normal billing. As a pure carrier, MNO has a minimum participation. Being in this position, the MNO is only liable for transferring the payment data among the different players. Position from MNO minimum participation is as a pure carrier. In this case, MNO is just responsible for data transfer between the various payments other players. Without the MNO the m-Payment cannot take place, regardless of the level of participation.

- **Banks:** Banks and other financial providers, such as credit card companies constitute other players in the telecom scene. What makes the bank's attractiveness Telecom provider is the customer's trust, they enjoy [12]. Bank of long-standing business and customers entrust him with the bank's money. Introduction of mobile payment application under the banner Bank to improve the customer's approval, because the customer's trust in the bank Transfer payment applications. In addition, their core competencies is Currency trading, the bank has the necessity for the experience and risk management facilities not to show that they deal with a large amount of database or has an existing payment infrastructure but to handle and manage the m-Payment transactions successfully [25]. As the acquirer, merchant bank has an existent number of merchants that cooperate with debit card and credit card payments. This gives the bank good if the business cooperation, and agreed to provide a starting point for Carriers as an application payment options.

In the bank -led model, the bank is in the value chain of the major players. In the present scenario based on the MNO data carries, the bank is the player or the entity that provides mobile payment applications. Although the bank does not "bill " customers, but it is the duty of the bank to collect payments from the side of the m-Payment providers by debiting the amount from the customer bank account (if the customer has a At a given bank) or by initializing the money transfer from customer account to the other bank. Degree of participation differs for the banks also, if talking about the MNOs. MNOs sometimes play the role of the m-Payment providers or they could liable for the payment infrastructure or they could be just dealing with the funds clearance and settlement.

- **Merchants :** businesses in the successful operation of the network operator 's role Systems are often underestimated. Merchants also important to end users Network operator scenarios. A consumer accepts m-Payment system only if the m-Payment option is provided by a large number of merchants. It is advantageous for a merchant to implement the m-Payment system only if the number of users for the given m-Payment system is quite large. While on the other hand, it is advantageous for a user to start using the m-Payment system only when there are a large number of merchants providing that payment system [41]. Thus, it gives rise to a heinous situation where the customer seems to be uncertain about using the new payment system if he is not able to use it widely around everywhere. While the other situation is for the merchant, where the merchant is uncertain about offering the new payment system for the customers if he is not sure about the huge acceptance from the customers.

  It is believe and seen that the nature of the merchant is believed to be more passive as compared to the active players. But still, however, since the merchant have a direct impact on the success of the payment system and also that they are straight away related and connected to the payment system, so they could fall into the category of the active players.

  The author found that due to the success of businesses strongly influenced m-Payments Because they are directly involved, they can communicate with payment systems as active players .

- **Third-party player :** It is an independent mobile payment service provider that provides a mobile payment solution but it is neither a bank or an MNO. Third-party players lays the foundation and they rely on mobile operators, both in the partnership, or just as a Carrier. Players involved in the establishment of such a bank or MNO help Third-party player to better promote its mobile payment application - an aspect of the required to obtain the trust of its customers and provide mutual customers access to a large Merchants to use new mobile payment solutions. The main role of the third-party players is to promote the mobile payment application more effectively together with the involvement of the players like bank or an MNO. Promoting the mobile payment application is the key feature needed in order to get the customers belief and interest to use the mobile payment solutions.

(B) Passive players

- **Mobile device manufacturers :** The mobile device manufacturers has as an indirect relation to the m-Payment system, so they act as a passive player. The key responsibility of the mobile device manufacturers is to make the mobile devices capable of using the m-payment applications by providing the mobile devices with appropriate software and hardware requirements. Thus, the mobile device manufacturers do not have a ample role to play in the m-payment life cycle. M-Wallets and payment enabled applets etc could be the possible software that needs to be installed on the mobile devices. Moreover, now a days trend is to make the software available on the internet; from where they can be downloaded by the user on their respective mobile devices and used. No special hardware is required for the present day Mobile Payments applications. But if the payment system includes the use of biometric authentication method in addition, then the hardware required is the fingerprint reader.

  When talking about the role of the mobile device manufacturers in the m-payment value chain, the only responsibility of the device manufacturers is to provide with the hardware required for the m-payment application.

  An example of how the mobile device manufacturers can become a part of the m-payment value is chain is by enabling the mobile device to use m-Wallet. These m-Wallets are protected by the passwords. However, a two-level security check is provided in the m-Wallet; first the user enters the PIN for the SIM based

authentication and it enters the PIN for accessing the m-Wallet. Thus this provides a more secure and reliable option. Despite the fact that using this two-level authentication provides more security to access but still it is not very much convenient for the users to use this method since he has to memorise two PINs for the same device. If the mobile device is switched off, then the PIN das to be re-entered to authenticate the mobile device. While if the mobile is switched on then the two-way authentication does not amply apply to the technique as in the switched on state there is no need to re-enter the PIN, so two-way authentication does not hold in this case. Along with this, in many countries like India and UK, MNOs do not have a need to enter the PIN for activating the SIM card. The SIM card gets activated as soon as it is put into the device and the device is switched on. N this case too, the provision for the two-level authentication scheme does not hold good practically.

Dahlberg (2002) [26] explained and found that if the authorisation techniques uses two PINs with the mobile device then it is easy to use the m-payments systems. Although this is concluded in the reference to the electronic and internet banking. However, the convenience with which the payment system could be used or employed by the people has to be compared to the other payment options available in the market; specially those options should be compared that are rendered over the m-payments solutions. The examples of such payment options are credit cards, debit cards and cash. In all the above mentioned payment options only the one step is required to complete the payment cycle, i.e., either by signing or by memorising a PIN for the credit/debit cards; but in the case of two-level authentication the whole process of completing the payment life cycle is inconvenient to be used by the customer as the customer has to memorise two PIN codes.

- **The End-User/Consumer:** Consumer is the most important entity in the value chain as it is the consumer who eventually is using the m-payment application or the solution. Lesser the number of consumers using the m-payment system, then the chances of the failure of the m-payment system id more wide. While the larger the number of consumers using the m-payment system, greater are the chances of the betterment of the system [42].

  Precisely defined and understood composition of the target population is crucial for any business ideas [27]. The likes and dislikes of the target group should be

properly analyzed and the demands of the people should be duly fulfilled for the better acceptance of the payment system. The entire life cycle of a product is more or less affected; Brand, marketing methods and channels. It all depends on Target customers. It has a good m-Payments'.

2.4 The contemporary security in m-payments

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 [28]. 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) [29] 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], the people were asked if they were interested to get enrolled for an m-payment application and the results show that only 8.2% people denied to get enrolled for an m-payment application. Although the above study results do not exhibit the nature of people towards the m-payment 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 [30].

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.

2.4.1 Security Parameters in Payment system

In e-transactions or electronic transactions, basically there are five security parameters upon which the stability and acceptance of any payment system relies. These five security parameters are named as follows: authentication, confidentiality, encryption, data integrity and non-repudiation [21]. All these five parameters are explained in details below.

- **Authentication :** Authentication is the ability to identify a person against the identity he claims to be. In other words, it is the ability to identify a person uniquely and to proof the validity of the identity [43]. In payment transactions, it is important that both the Customers and merchants to authenticate, because these two equally prone to fraud attacks. While the merchant might have to deal with a customer with a fraud identity or in the other case, the customer might have to deal with the merchant with a false identity through phishing. Phishing is the method of stealing the identity. Through phishing a merchant tries to steal an identity and pretends to be genuine identity; this generally is done by pretending to be a merchant of some brand name or of a bank and the customer is asked to disclose its personnel information to it [31].

- **Confidentiality:** Confidentiality is the method of hiding the user information and identity from being accessed by others, which are not meant to access it [44]. In the payment of any transaction, the data about the customer like his address, purchased items, and most likely the credit card or bank details are recorded. Although this information or data is necessary to complete the transaction but the data must be kept secret and must not be provide to anyone else except in case of some legal action, that too with prior legal permission. The confidentiality of the data must not only maintain during the transmission of the data while it should be taken care of also when it is stored. Most of the times the identity theft or the stealing of the information of the credit cards or the bank account does not happen during the transmission of the data but are stolen from the database where they are stored. The hackers attack the central repository and steal all the details of the people.

- **Encryption:** Encryption is the technique used to transmit the data safely and originally without any attack or changes in its contents. This technique uses a key to encode the data in such a format that neither it could be read nor could it be decoded unless the same key is provided for the decoding of the data. Thus, encoding of data using a key is known as encryption while the decoding process is known as the decryption process. Encryption of data during the m-payment transactions is of main concern.

- **Data Integrity :** Data integrity means maintaining the originality of the data. Data integrity is the property which is holds prime concern in m-payments. It means that no one could modify or change the data in any sense. Only the legitimate persons are

allowed to access the data. During an m-payment transaction the data provided by the customer should only be provided to the merchants and from merchants to the payment providers only; no other party or person in between is allowed to access the data of the customer. In all cases, protection of the data from the attacks is the major issue [44].

- **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. In case of m-payments the transaction involves the transfer of the money so it is highly likely that such a system should exist in between that could affirm the transfer taking place between the two entities in exchange of goods or services. For end-users non-repudiation is of great importance as it affirms them that they would receive their payment [32].

To confirm that all the above mentioned five security parameters are satisfied to the level of satisfaction required can be judged by having answered to all the questions mentioned below [13]:

- **"It is the customer, who he claims to be?"**
- **"It is who he claims to be a businessman do?"**
- **"Is my data in the right hands? Pass it to a third person?"**
- **"Can my data be read during transmission?"**
- **"Merchants have received my payment?"**

If all these five security parameters are affirmed properly in a payment system then this raises the customers' trust and acceptance towards that payment system. If the customer knows that the money he is transferring and the information he is providing is going to the legitimate person only and that the information provided is safe and is not shared with anyone else, then this automatically increases the trust of the customer in that payment system and chances of that payment system are brighter.

2.4.2 Authentication - important security issue

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 [4]:-

- **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 [3]. 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 payment 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 m-payment applications provides a far better and secure method. As in case of using an m-payment 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 [45].

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 [33].

From the above study we can conclude that so far the best method for authentication is the use of biometric. 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 [33][46].

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 [33].

Authentication is the essence of the mobile payment system [47] and a valid authentication method would enable the users of the payment system to build faith in the application's security mechanism.

As authentication being the essence of any m-payment 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 payment system.

We here now analyse all the three types of authentication methods one by one taking into consideration every aspect of the security in payments.

- The first technique is the token-based authentication technique. In this method the user have to carry an additional card or token for the verification purpose. Thus, it is a serious drawback for the m-Payment system if the user still have to carry with him an additional item or card etc in order to verify his identity. So, token-based authentication is not an appropriate option to be used in case of m-payment systems.
- Next we have the knowledge-based authentication technique. This technique is widely used today in most of the applications available in the market. This technique is also not an appropriate option to be included in the modern m-payment systems as it makes use of the PINs or passwords which tends to be forgotten or cracked or lost. This shortcoming of knowledge-based technique leaves us with the last option, i.e., biometrics.
- The biometrics-based authentication technique overcomes the shortcomings offered by the above mentioned option. This technique uses the human traits such as facial expression, retina scanning, iris, voice, fingerprints, etc. for the purpose of the authentication. These traits are carried by a person all the time and there is no scope for stealing or cracking of these traits. Moreover, these traits are non-transferrable which makes it a strong option against repudiation. Thus, biometric is seen to be the best option which could be applied to the m-payment systems to improve their security and acceptance widely.

2.5 BIOMETRICS

As defined by Nanavati [3] biometrics is the "automated use of physiological or behavioral characteristics to determine or verify identity."

While a more detailed definition is provided by Bolle [4] 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).

2.5.1 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.

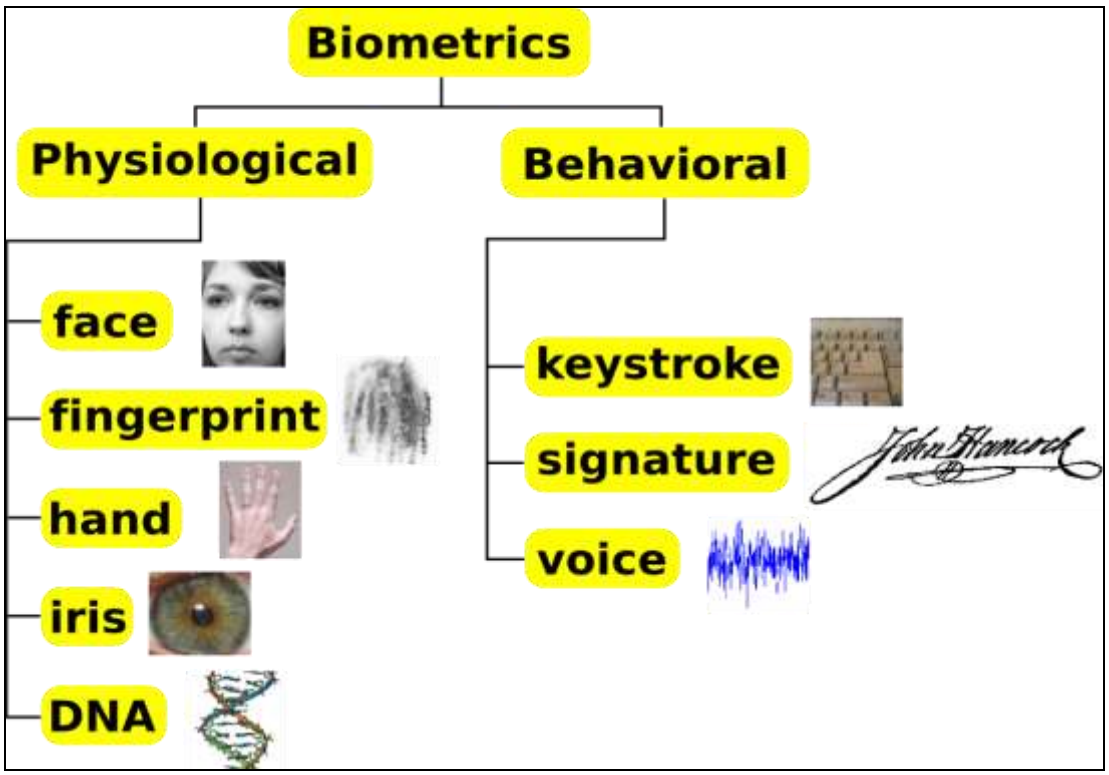


Figure - 5 types of Biometrics [38]

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. 10). 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 [3].

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 [6]

Figure-6 Face Recognition

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. [7]

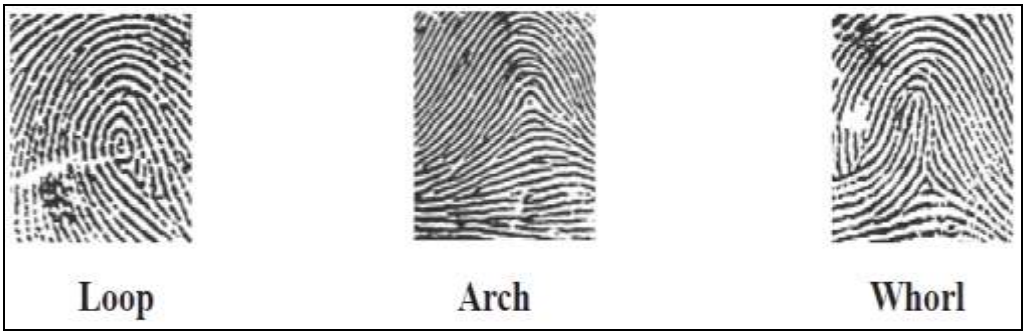


Figure-7 Fingerprint patterns

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 [8] .

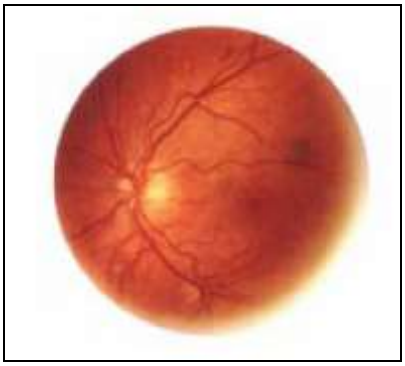


Figure-8 Eye retina

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. [8]

Figure-9 Iris

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) [9][10]

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) [9][10]

2.5.2 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 [3]. 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 [46][3][33]. 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 [3]. 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 [33]. 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.

2.6 Fingerprint

2.6.1 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.

2.6.2 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 are completely developed and finger ridge configurations remain 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.[49]

2.6.3 Types of Fingerprint Scanners

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 human's 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 [48].

Figure-10 Optical Scanner

2. CAPACITIVE SCANNER

Capacitive scanner looks like the image given above. Capacitive scanner takes 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 [48].

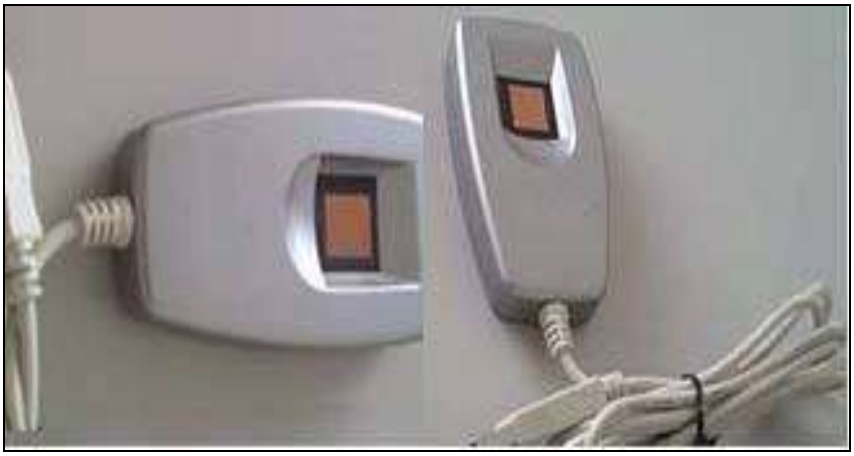


Figure-11 Capacitive Scanner

2.6.4 Method for Storing and Comparing

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.

But nowadays, it is not a tedious task. 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.

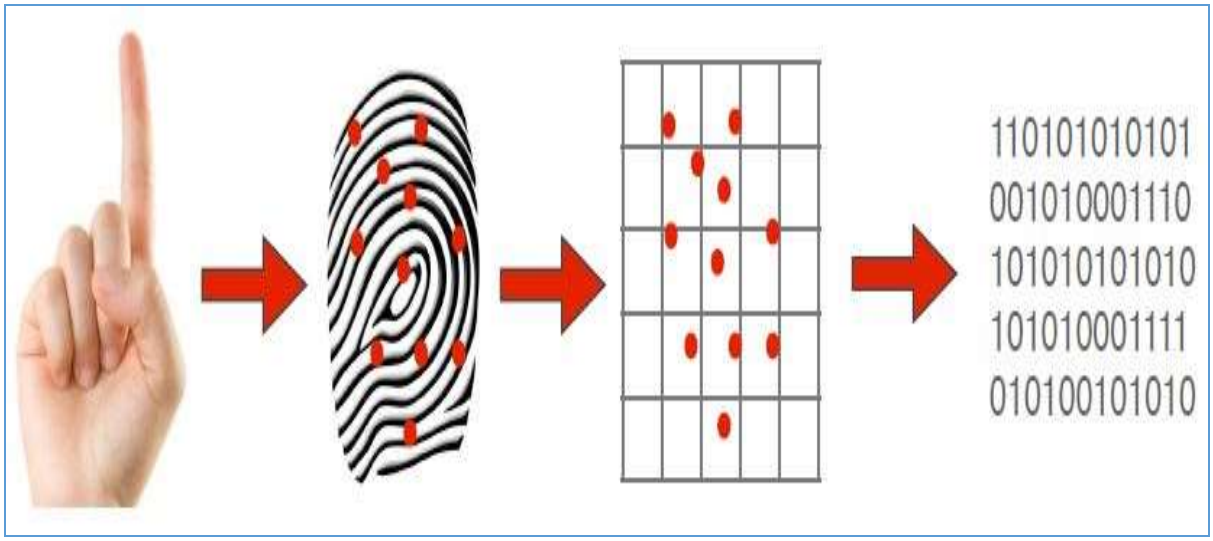


Figure-12 Storing Procedure of Fingerprints

2.6.5 Fingerprints Classification

A large number of fingerprints are collected every day. 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 [49]:-

- Loops
- Whorls
- Arches

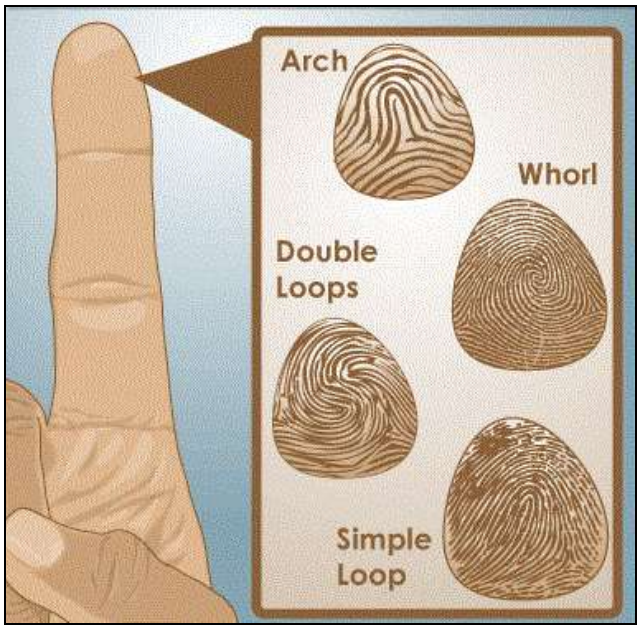


Figure-13 Different patterns of fingerprint

1. **Loops**

60-65% of the population has loops in their fingerprint. Loops are made of one or more ridges entering from one side, curving 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 [49].

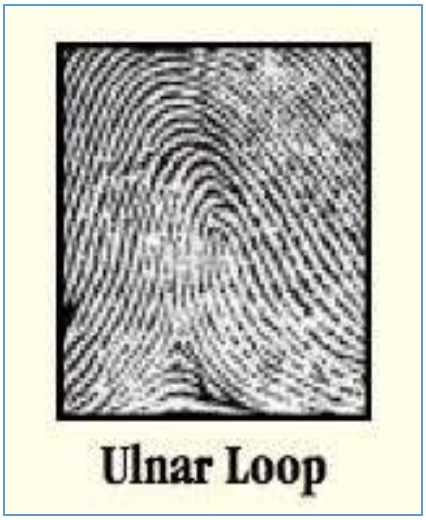


Figure-14 Ulnar Loop

- **Radial loop**

  Radial Loop tends to open toward the left or the radial bone. The image showing the Radial loop pattern is given below: [49]

Figure-15 Radial Loop

2. **Whorls**

30-35% of the population's fingerprints 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 [49]:

- **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:

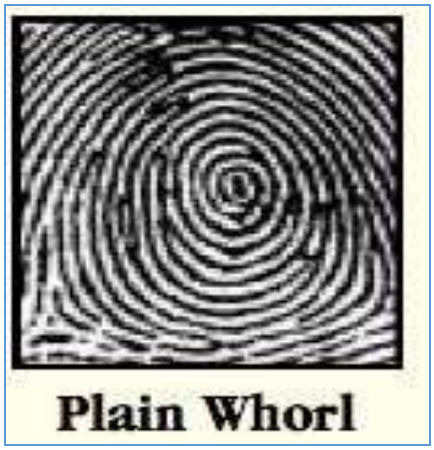


Figure-16 Plain Whorl

- **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 [49].

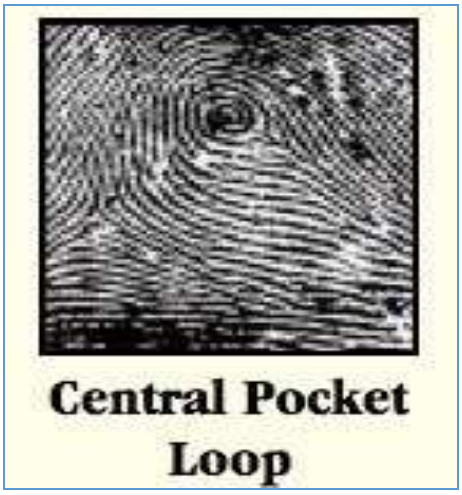


Figure-17 Central Pocket Loop

- **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 [49].

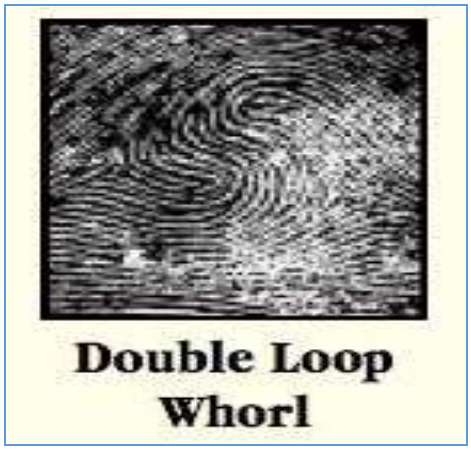


Figure-18 Double Loop Whorl

- **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:

Figure-19 Accidental Loop

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:

Figure-20 Plain Arch

- **Tented arches**

  Tented arches tend to show an acute heel at the centre of the arch. A tented arch looks like the image given below [49].

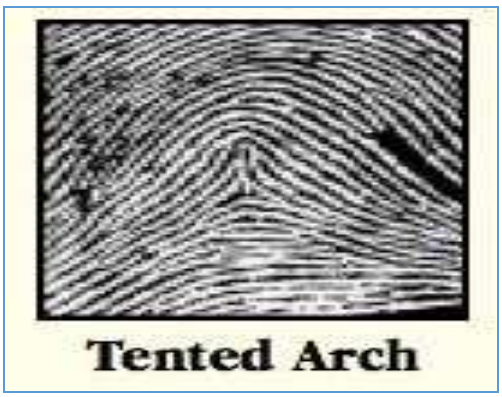


Figure-21 Tented Arch

2.6.6 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

CHAPTER-3

RELATED WORK

India is the world's second largest telecom market; with 929.37 million mobile phone users. Phone is quite common, even in remote villages. Mobile phone industry is growing at an annual rate of more than 2 million visitors annually. It is expected to reach 1 billion in 2013 to mark. Urban users share was 66%, while the share of rural users was 34%. In May 2011, the monthly increase in the number of users in terms of a net 13.35 million. The 13.35 million new subscribers, 7.33 million people from urban and rural parts of Section 6.02 million. Subscribe monthly growth rate of 55% of the urban segment, while the rural part of the 45% [1]. Given such a background, the phone can be considered as an economically viable tool that enables include access to financial services.

Mobile payment can relax cash handling, storage, and transmission operations aspects related costs associated with cash-based transactions and financial inclusion by providing a strong platform to have a positive impact on social welfare.

With the increasing mobile technology, mobile payment system has paved its way in to people's life. But still not a large portion of people use mobile payment system mainly for two reasons. Firstly, still people in India have a question about the security of their payments made online. While the second reason is, that not all people possess smart phones hat support the mobile payment facility.

Vishal Goyal , Dr.U.S.Pandey, Sanjay Batra (2012) revi.e.ws the emerging research literature on m-banking. It presents a classification framework for m-banking research based on 65 m-banking papers published between 2000 and mid-2010 in Information Systems (IS), technology

innovation, management, and marketing journals, and major IS conferences. These papers are classified into five main categories: m-banking overview and conceptual issues, Features & Benefits of Mobile Banking, Current operating practices of commercial banks, Mobile banking/payment practices in Indian Commercial Banks and Challenges in India strategic, le.g.al and ethical issues.

Vibha Kaw Raina (2011) proposed an idea for integrating the proposed framework with the multi-server authentication model in order to maintain security and for accessing different servers, i.e., websites. The author proposed a multi-modal biometric authentication process in relation to the payment system and has integrated it with the existing payment system.

Kanaan A. El Bhissy(2011) proposed a payment system for mobile phones for mobile the people of Palestine. The author has designed and programmed the speaker - verification system which does not depend on the text, i.e. the system can verify the speaker regardless of the phrase pronounced system work entirely on a mobile phone to pick up the sound and analyze it to extract the characteristics of the vocal tract ,then the verification process ,which compares the extracted speech's features with the stored vocal model audio of the speaker which can be modified when necessary.

Shiny Sreekumar (2010) has explained the key issue of authentication in the m-Payments and has also explained and proposed a model on how biometrics can be used for authentication in m-payment system. Further, the author has provided a detail on how the enrolment process should be carried out as it is the basic step in the correct authentication procedure. Also the customer acceptance about the m-payment system is based on the enrolment process.

Uludag et al.(2004) provides the definition of the biometric technology as "an automated method recognition based on behavioral or physiological characteristics of people. These features include features such as hand, face, fingerprint, vein, voice, retina, iris." Moreover, the authors has explained that the biometric technology can be used in a wide range of applications for providing strong authentication services.

Welzl (2004) found out that the biometric technology makes use of the pattern recognition technique in order to identify and verify an individual, since each user has a unique physiological and behavioral traits.

Jain el al.(2003) , has described the significant difference between the physiological and behavioral biometric characteristics. Physiological biometric data gathered by the measurement

part, and direct measurement of the human body. These samples include, but on the other hand, behavior characteristics of the human body are not limited to hand geometry, face recognition, fingerprint, and iris scan. These samples include, but are not limited to, the signature scanning, the scan key, speech recognition. Time can be used as a measure of behavioral characteristic, as it passes through the process of considering a given (behavior shoniregun, 2003 year schedule measures; strasser et al, 2001; putteand keuning, 2000).

Jain and Uludag (2003), and soutar (2002), which includes noted that an ideal biometric system should be universal, unique, permanent and collection value. It must be universal, everyone has the characteristics and unique, no two people share the characteristics and permanent; where the characteristics should neither be changed nor is variable the final characteristics must be recovered, and at any decent sensor and easy to quantify (uludag, et al,2004). Some other studies have found to meet all the above requirements may be impractical or characteristic of a useful practical biometric identification system (Linnartz andTuylus, 2003).

Schneir (1999) and Timmers (2000) has studied and has integrated the biometric technology with the application using a software developers kit (SDK's). However, a recent study concluded that a standardized biometric application programming interface, bioAPL phase, was set up in the specification, version1.1, released in 2001, in order to enhance the portability of internal application-independent biometric technology (suter, 2002; jain and uludag, 2003; adler, 2004).

CHAPTER-4

IMPLEMENTATION METHODOLOGY

In this section we have described our proposed algorithm of biometric authenticated payment system designed especially for implementing m-payments. Since our model will be typically based on biometric authentication and we have used fingerprint (thumb impression) biometric.

4.1 Biometric Authentication Process

The biometric authentication process consists of two phases– Enrollment process and Verification process.

i.) Enrollment Process

Enrollment relates to the process of registering the fingerprints of a customer against their other demographic data as a record of their biometric identity. It will be a one-time process in which a customer will be asked to present their fingers on a scanner and the fingerprints will be recorded and stored.

The enrollment process is carried out at the related bank as the registering processing is all done and maintained by the bank itself.

ii.) Verification Process

The verification process involves the customer verifying their identity through a live fingerprint to authenticate a payment. This process will be carried out every time the customer is carrying out a payment. In verification process the customer will enter their customer identity number into the verification system. The system will then prompt the customer to present their live fingerprint on the scanner. The live fingerprint will be then compared with the biometric template stored against the customer identity number in the biometric server.

In case the verification is successful the payment transaction will be considered authenticated and the transaction will be sent to the bank for processing.

In case of a failure the customer may be asked to present the finger again up to a certain maximum number of tries.

In order to implement a biometric authenticated payment system we will require three primary system elements that are put in place by a bank or acquirer. These are:

i.) **Enrollment system**: This system will be used for enrollment of the customers on to the program and recording their fingerprint identity.
ii.) **Verification system:** This system will be used at retail locations for verification of the live fingerprints with the stored fingerprints for authenticating the payments.
iii.) **Biometric server:** This system will be used for storing the fingerprints, extracting and verifying fingerprints during a payment process and providing an interface to banks and acquirers for managing the customer data and reports.[35]

4.2 Components Required For Biometric Payment System

The different components that are be required for the biometric payment systems are:

i.) **Secure Online Banking Server (SBS):** It will have access to customer's data; establish connection with the Online Banking Software (OBS); conduct capital transactions and will be able to identify a Biometric Trusted Device (BTD) as a communication partner to establish a secure connection.
ii.) **Online Banking Software (OBS):** It will be stored on the client and will communicate with SBS in order to process different transactions.

This model provides flexibility to make any payment or transaction without involving any external entity other than the bank. This model is useful for both the user and the bank, and it is based on the customer-centric and bank-centric approach. This model will be having three levels of security for authentication of the user. [36]

The first step in the proposed model will be to check the first level of security i.e. in the form of account number and password. After entering the account number and password the system will check the validity of the user credentials. If the user enters the right account number and password the system will enter into second level of security otherwise will again ask for the account number and password.

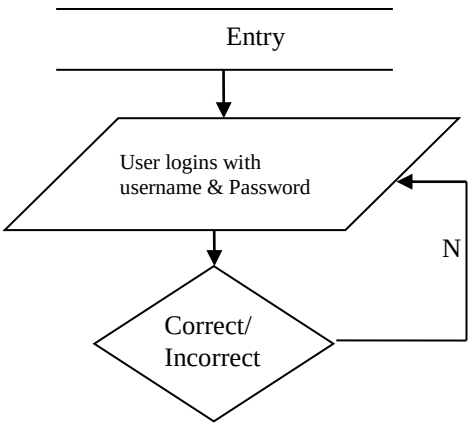
After authenticating the first level the system will ask for the second level of security which will be the biometric template of the user. The system will verify the biometric template of the user with the stored biometric template in the database. If the user enters the valid biometric template then the system will enter the third level of security i.e. registered mobile number.

The system will verify if the biometric template is received from the registered mobile number. Otherwise the system will again ask for the biometric template. After verifying the mobile number, the system will be checking for its validation.

If the validation is right then the system will proceed and enter into the mode of transactions/payments otherwise it will continue asking the valid set of credentials till the loop ends. Also, if the user opts for making any kind of payment or transaction then again the system will ask the user to enter the biometric. This additional step in the authentication while making any transaction will make the transactions more secure.

Various options provided in the model are as follows:-

a) The first option provided in the model will be to check the current balance of the account holder. By this option the user will be able to check the details of the balance in the account.
b) The second option will be updating of the account.
c) The third option will be for transferring the funds from existing account to another account in any of the banks (money transfer). For this option again the user will have to go through the authentication process.
d) The fourth option will be the payments with the help of mobile wallets. This option will be further having different choices that include payment with Pay Pal, M-check, Obapay, Pay mate. These payment options are useful for P2P transactions providing the facility to do transactions with electronic money. For this option too the user will have to go through the authentication process.



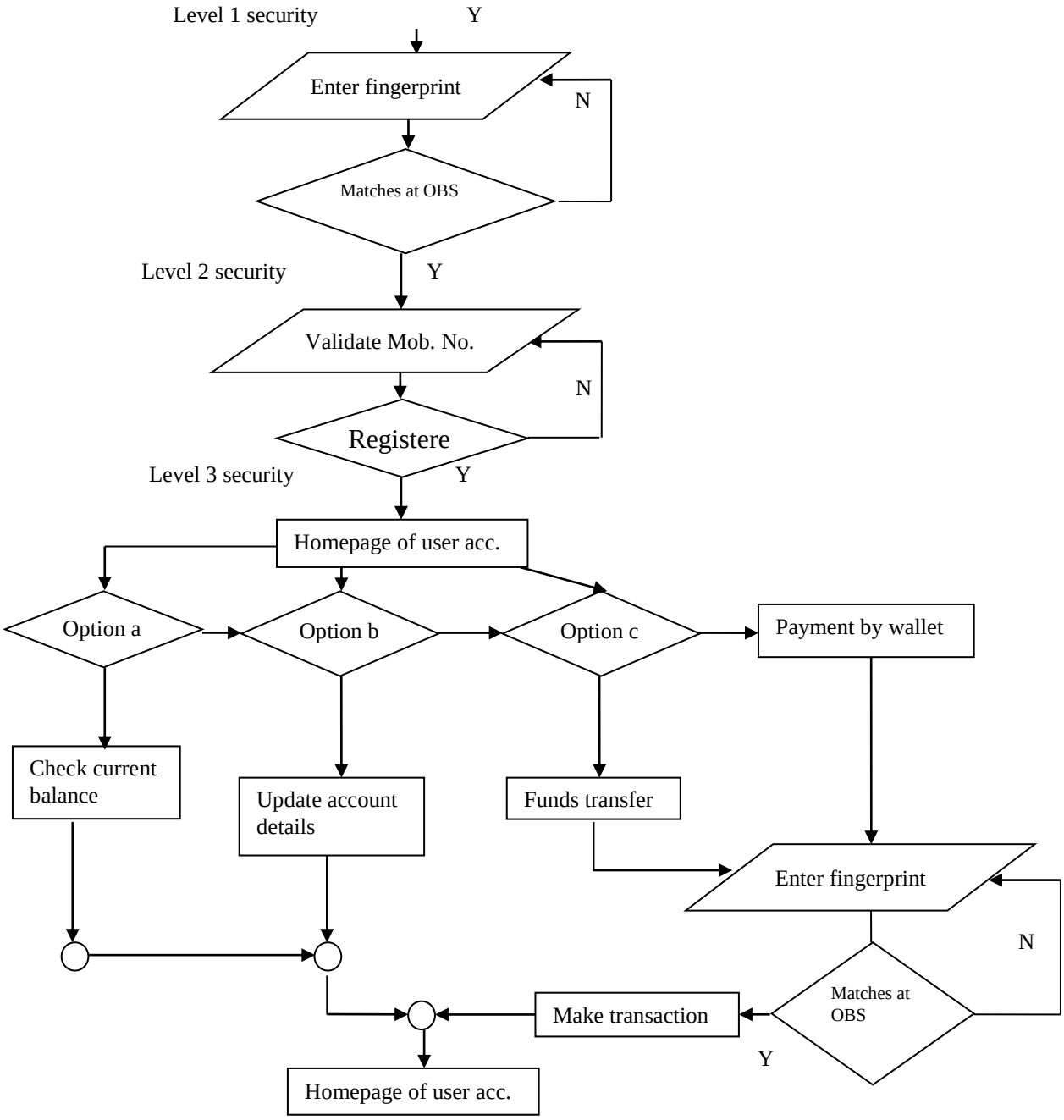


Figure-22 The flowchart of the proposed model

4.3 Execution Of The Proposed Framework

The whole procedure is shown by a demo desktop application which is explained below.

I. The step is that the user enters the username and password, and tries to login to his account. The system checks for the validation of the password, if valid then the user is passed on to the next step.

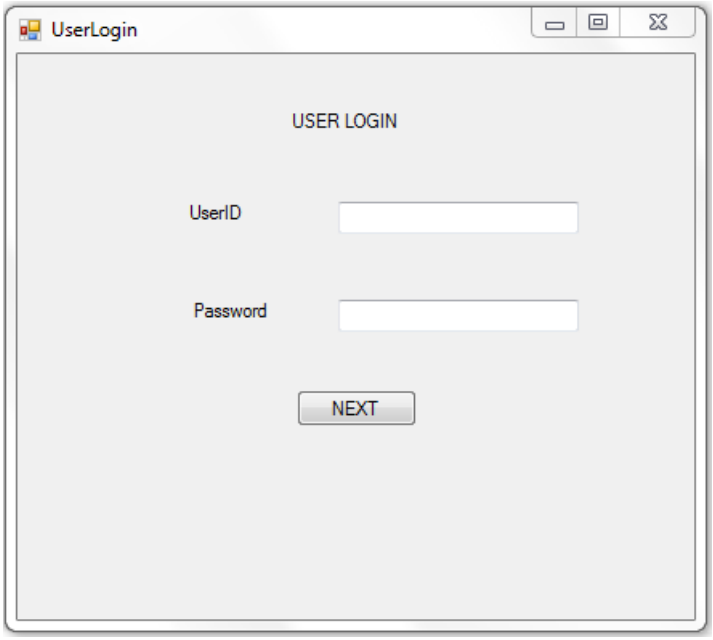


Figure-23 showing login page

II. This step is of biometric authentication, in our model fingerprint is used. The user clicks an image from his phone and it is then send to the server for the validation purpose. (In demo desktop application we have uploaded the image). The user fingerprint image is compared against the fingerprint template stored at the bank server. One more thing is done at this step; the image that is send to the server for the comparison is first encrypted and then sends. Again at the server side the image is decrypted and then compared with the stored template.

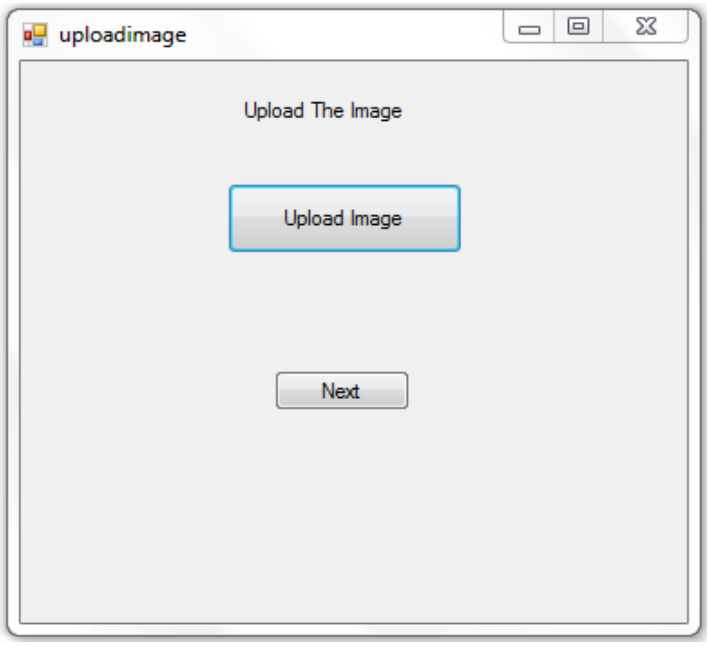


Figure-24 showing biometric upload page

III. The next step checks if the image that is received is from the registered mobile number or not. If the user clears all the security credentials then the user enters into the mode of transactions.

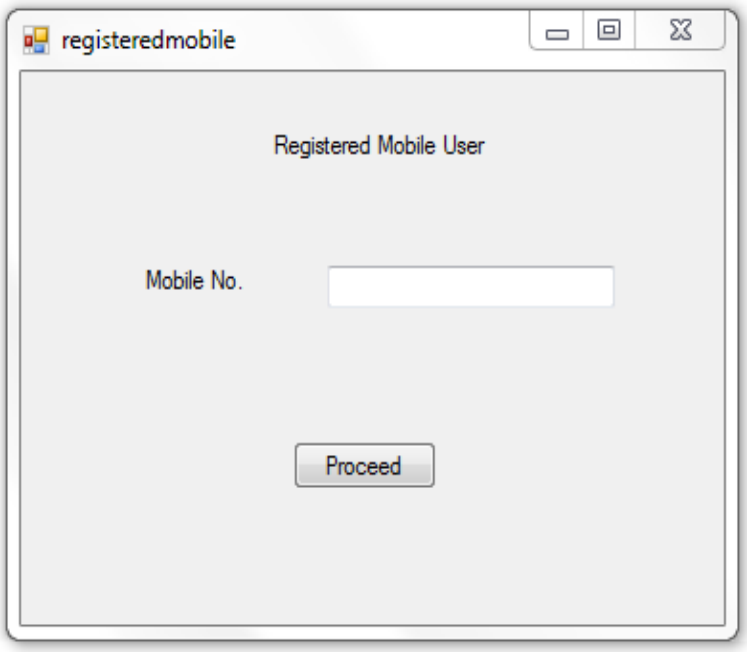


Figure-25 showing registered mobile number page

IV. Again the user is offered various banking services from updating his account to making transactions. If the user chooses to update his account or simply check its account status then after clearing all the security checks he can simply have access the account. But if the user wants to make funds transfer or make transaction using wallet then again the user has to go through the security check. Biometric authentication is again applied at this stage.

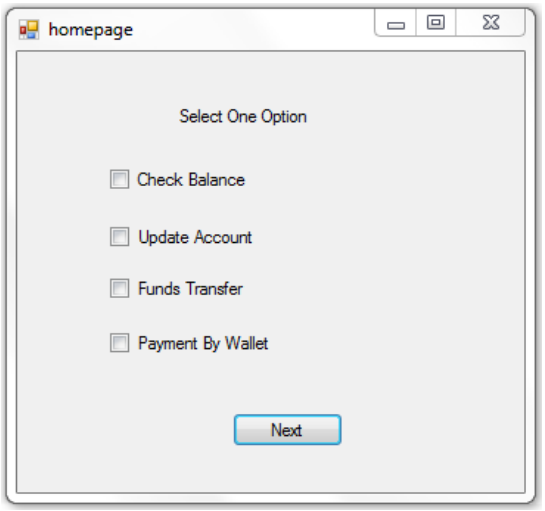


Figure-26 showing the homepage of user account

V. After making transactions, the user can logout successfully.

CHAPTER – 5

RESULT

5.1 RESEARCH FINDINGS

The increasing number of mobile subscribers is paving a way for the m-payments not only in the developed countries but in the developing countries too. Inspite of having a few m-payment applications the ratio of using m-payments to the number of mobile subscriber is quite low. The reason behind this scenario is obvious, that is, security threats and the belief that is the m-payments safe to do? Moreover, the concept of m-payments and the biometrics is not new in the market but still number of applications offering these two services is few.

Today, mostly all mobile payment applications present in the market, commonly use a method for authenticating the user is by the using the PINs. The kind of authentication technique used in the payment system depends not only on the geographical distances but also on the mode of purchase used. Now a days, it is seen that inspite of using the traditional way of using a 4-digit PIN to authenticate; the m-Payments applications in the

market is using a 6-digit PIN for authentication purpose. Since the m-Ticketing applications largely involve the micro-payments which are low risk prone, so these do not require an explicit authentication system. Example of such application is RMV Hanau HandyTicket. Biometric is used as an authentication tool in a very few cases or application till now; like Pay by Touch is an example of such application that has employed fingerprint verification technique for the authenticating the users. However, on the other hand, digiPROOF is an application which is not a payment application, uses the fingerprint verification technique for authenticating the user.

The authentication systems used today on the whole does not seen to have any problem but still we recommend using biometric authentication technique because of the reasons mentioned below:

- Basically the methods of authentication used in the contemporary and the object based technique involve the use of methods like PINs, passwords and tokens. But they consist of risk of being getting cracked or stolen or lost. However, with biometric authentication techniques this is not an issue. Biometric methods are more secure since they cannot be stolen or cracked.
- The PINs and passwords used in the conventional methods are prone to be forgotten or stolen while the tokens used in the object-based methods have a risk of getting misplaced. Thus, biometrics provide a convenient option here as neither it can be lost nor there is the need to memorise it.
- Since biometric traits cannot be transferred or shared with anyone thus it prevents from fraud and "buddy-punching". Payment transactions are better analysed using the biometrics methods.
- Once the user has started a transaction he cannot refuse the initiation. Thus biometric authentication provides a strong solution against the repudiation as it cannot be transferred from one person to the other.

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	3 level
Authentication	PINs and Passwords	Biometric(fingerprint)
Convenience	PINs and Passwords can	Don't have to remember

	be forgotten or stolen	biometry or can't be stolen or lost
Transactional Authentication	OTP or PINs are used	Has additional level of security for transactions. Again uses biometric authentication

CHAPTER – 6

CONCLUSION & FUTURE SCOPE

6.1 CONCLUSION

In this work an attempt has been made to analyse and develop a secure model of M-payments which involves multi level security, without additional cost.

The system involves 3 level security one of which a new integration is biometric verification of the user before logging in to the system and also making use of the same for all kinds of m-Payment transactions.

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.

And multi-level authentication mode provides the user much better security. Moreover, this model provides a payment system for mobile phone that supports the most basic features like a camera in it. Our model is not only for smart phone holders but also for the simple phones with a camera. Thus, this feature of our model will make the mobile payment system acceptable by more and more number of people, providing a m-payment system that is more secure, reliable, easy to use and adaptable at the same time.

6.2 FUTURE SCOPE

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

The proposed model makes use of the fingerprint image for the purpose of biometric comparison of the fingerprints. This limitation provides the scope for research in this area. The research in the field of extracting the fingerprint template from the camera image has a great scope in future.

Another limitation is that if the user gets his finger injured or damaged than he may not be able to access his account as biometric security check is the essence of the model proposed, so ways to overcome this situation needs to be explored.

Also the quality of the image taken from the camera must be of good quality, so that fingerprints could be extracted from it. Thus, the camera quality must be good enough to accomplish this.

Also, there is a great need of a secure system that can be used for encryption of the image or data.

CHAPTER- 7
REFERENCES

[1] Annual Report, 2009-10, TRAI, Govt. of India.

[2] Praveen Chandrahas, Deepti Kumar, Ramya Karthik, Timothy Gonsalvis, Ashok Jhunjhunwala and Gaurav Raina " Mobile Payment Architectures for India", National Conference on Communications,2010.

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

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

[5] JuCheng Yang "Biometric Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment Systems". IEEE International Conference on Management of e- Commerce and e-Government 2010.

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

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

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

[9] Fernando L. Podio: "Personal Authentication through Biometric technologies".

[10] 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.

[11] Tiwari, R.; Buse, S. (2007). The Mobile Commerce Prospects: A strategic analysis of opportunities in the banking sector (PDF). Hamburg: Hamburg University Press. p. 33. ISBN 978-3-937816-31-9.

[12] Krueger, M. (2001). The Future of M-payments - Business Options and Policy Issues. Electronic Payment Systems Observatory (*).

[13] Shiny Sreekumar, “Biometric Authentication In Mobile Payments”,2010

[14] E Turban, D King, J Lee, M Warkentin, H Chung, “Electronic Commerce-A Managerial Perspective", 2010.

[15] E. Valcourt, J. Robert, & F. Beaulieu, (2005). Investigating mobile payment: supporting technologies, methods, and use. IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, (WiMob'2005), Aug. 2005 Page(s):29 - 36 Vol. 4 Digital Object Identifier 10.1109/ WIMOB.2005. 151 2946.

[16] GSM 04.90 (ETSI EN 300 957, V7.0.1) Specification (USSD) – Stage 3 at 3Gpp.org.

[17] Visa and SK Telecom to launch mobile payments Card Technology Today, Volume 19, Issue 2, Page 6, February 2007.

[18] J. Ondrus & Y. Pigneur, “An Assessment of NFC for Future Mobile Payment Systems. International Conference on the Management of Mobile Business”, 2007, 9- 11 July 2007 Page(s):43 - 53 Digital Object Identifier 10.1109/ICMB.2007.9.

[19] GSM Association aims for global mobile payments using NFC Card Technology Today, Volume 19, Issue 2, February 2007, Pages 1, 3.

[20] S. Karnouskos & F. Fokus (2004). Mobile Payment: a journey through existing procedures and standardization initiatives, IEEE Communications Surveys and Tutorials. 6(4) 44-66.

[21] Hampe, J. F., & Ding, M. S. (2003b). Changing Technological and Business Landscapes for mPayment. Is Local Mobile Payment Emerging as the Winner? Paper presented at the Conference Name|. Retrieved Access Date|. from URL|.

[22] Karnouskos, S. (2004). Mobile Payment:A Journey through existing Procedures and Standardization Initiatives. IEEE Communication Surveys & Tutorials, 6, 44-66.

[23] Pousttchi, K. (2004). An Analysis of the Mobile Payment Problem in Europe. Paper presented at the Mobile Business Systems, Mobile and Collaborative Business, Techniques and Applications for Mobile Commerce (TAMoCO), Essen

[24] Pousttchi, K. (2005). Mobile Payment in Deutschland – Szenarienübergreifendes Referenzmodell für mobile Bezahlvorgänge (1 ed.). Augsburg: Deutscher Universitäts-Verlag.

[25] Zmijewska, A., & Lawrence, E. (2006, January 23-25, 2006). Implementation Models in Mobile Payments. Paper presented at the Advances in Computer Science and Technology (ACST 2006), Puerto Vallarta, Mexico.

[26] Dahlberg, T., & Mallat, N. (2002, June 6-8). Mobile Payment Service Development - Managerial Implications of Consumer Value Perceptions. Paper presented at the ECIS, Gdansk, Poland.

[27] Hammer, C., & Wieder, G. (2003). Internet-Geschäftsmodelle mit Rendite. Bonn: Galileo Business.

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

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

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

[31] Chellam, R. (2005, 16.06.2005). Phishing scams seen surging this year. Retrieved 25.08.2005, 2005, from http://it.asia1.com.sg/newsdaily/news001_20050618.html

[32] Hampe, J. F., Swatman, P. M. C., & Swatman, P. A. (2000, June 19-21, 2000). Mobile Electronic Commerce: Reintermediation in the Payment System. Paper presented at the 13th International Bled Electronic Commerce Conference, Bled, Slovenia

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

[34] Uchebnik cited 05.03.212 , Kriminalistika, cited 18.03.2012

[35] Innoviti Simplifying Communications “Online Biometric Authenticated Payment Systems. 2008.

[36] Vibha Kaw Raina: “Integeration of Biometric authentication procedure in customer oriented payment system in trusted mobile devices”, December 2011

[37] Ondrus, J., & Pigneur, Y. (2004). Coupling Mobile Payments and CRM in the Retail Industry. University of Lausanne, Lausanne, Switzerland.

[38] Biometric Access Control Systems http://iwatchsystems.com/technical/2011/03/03/biometric-access-control-systems/

[39] Dial-a-Coke http://www.ccamatil.com/files/1/FINAL%20Coke%20Perth%20release.pdf

[40] Easymobile, Germany www.easymobile.de

[41] Henkel, J. (2001a, 16.08.2001). Bezahlen per Handy - viele Anbieter, aber noch kein Standard. *Frankfurter Allgemeinen Zeitung*.

[42] Henkel, J., & Zimmerman, F. (2002). The Political Dimension of Payment System Innovations: The Case of Mobile Payments. *IPTS Report 63, Special Issue: e-Payment Systems Challenges for Europe*.

[43] Creese, S., Goldsmith, M., Roscoe, B., & Zakiuddin, I. (2003, 12-14. March, 2004). *Authentication for Pervasive Computing.* Paper presented at the Security in Pervasive Computing, Boppard, Germany.

[44] Dannenberg, M., & Ulrich, A. (2004). *E-Payment und E-Billing*: Gabler Verlag.

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

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

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

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

[49] Classification of Fingerprints, The Crime Lab: Staples High School Forensics