**Introduction to the Study**

**1.1 Introduction**

Mobile banking has proved to be the easiest and most convenient way to access banking services throughout the world. (DalitsoKalitera, 2017) It offers customers time independence, convenience and promptness, as well as cost savings (Lee, 2007)

Mobile banking can be defined as a service provided by a financial institution enabling clients to carry out financial transactions, (NEMANJA MAČEK, 2017) For example, electronic bill payments and transfers of funds, using the mobile device and software provided by the above institution. (NEMANJA MAČEK, 2017) Though mobile banking has its upsides, financial transaction security is a very important issue that needs to be addressed very carefully, because online banking is one of the most sensitive tasks performed by general users. (Oorschot, 2007) Though many traditional banks offer secure mobile banking, (Y.S. Lee, 2010) It should be remembered that there is no silver bullet which provide a 100 percent security guarantee to the customer. According to (Armour, 2017), The Bureau of Financial Institutions conducted a survey on 75 banks and credit unions and found out that the analyzed institutions were losing more than US$ 2.1 million in total due to data security breaches. This is a major loss that financial institutions must overcome to minimize fraud rates and protect users around the world. (W. Jeon, 2011) List out three assets (which can be specified as targets for mobile devices attack): computer, application, and private information (W. Jeon, 2011). The above-mentioned authors described a threat as anything that can act against an asset in such a way as to cause harm (W. Jeon, 2011). (Ashra, 2012) Identified that there are essentially two types of threats, those caused by external (adversary) factors and those caused by internal (user unconsciousness) factors. According to a report by Deloitte (Chuvakin, 2015) (Evangelatos, 2007) the majority of individuals aged 16-24 view security measures, such as passwords, as "an annoying extra step before making an online payment". It probably would have been more bearable if this annoyance really ensured secure transactions. Nevertheless, 2017 saw some of the biggest data breaches ever. Financial institutions were not spared, with as many as 400,000 accounts compromised in one attack alone. Aware of all that, management of banking institutions have been experimenting with various other methods. Some of them include passphrases, social sign-ins, multiple devices, or even multi-factor authentications that may include various combinations of those methods with a password for increased security. Even the sheer number of these methods shows that there is no clear winner. All of them compromise either security or user experience to some extent. (Agidi, 2018)

Security in mobile banking applications is established by means of successful user authentication. Authentication can be defined as “the ability to confirm” a claimed identity (Creese et al., 2003, p. 2). The most common form of authentication in payment systems is carried out by means of knowledge-based techniques like Personal Identification Numbers (PINs). Authentication can also be carried out using object-based authentication and biometric-based authentication.

Since authentication essentially opens the access gateway to whatever object it secures, it could be said that the level of security of any application depends on how robust the authentication process is. If the user considers the authentication process to be foolproof, he would potentially perceive the application to be secure. This leads to the question of which authentication method and process would be best suited for use in mobile banking applications in order to gain the trust of the user. Would the traditional PIN/password authentication method suffice or would a more sophisticated, “newer” method be required?

Enter Biometrics. Biometrics can be defined as “the automated use of physiological or behavioural characteristics to determine or verify identity” (Nanavati et al., 2002, p. 9). Biometric authentication is used in various sectors like law enforcement, healthcare, the government sector, travel & immigration as well as the financial sector (Nanavati et al., 2002). Major European airports like Amsterdam Schiphol, Fraport Frankfurt, various UK airports as well as airports in Canada and the United Arab Emirates (UAE) use iris recognition for automated border controls (Bohnet, 2009). Many European Union (EU) passports employ face recognition with machine readable passports (or ePassports). The United States of America (USA) use fingerprint verification to verify travellers to their country as well as using face recognition in e-Passports (US Bureau of Consular Affairs, 2009). Biometrics are also used in more commercial contexts like simply securing a laptop with fingerprint verification.

With regard to financial transactions carried out via mobile devices, the following security aspects should be addressed: physical protection of the device, security of the application running on the device, authentication of the user and the system to the service provider, encryption of the transmitted data and data stored by the customer in the device for subsequent review. Variety of authentication methods are being implemented in mobile banking today, both having upsides and downsides. Customers who secure data with passwords or PINs for example are at risk of fraud. Major companies have recognized the need for comprehensive countermeasures to security and are producing new hand-held products with integrated biometric devices. According to (Armour, 2017)“The biometrics market size is expected to reach $24.59 billion over the next six years and a lot of growth from the banks will be seen.” According to Gartner, More than 40 per cent of mobile devices now use biometrics; banks will see this as an advantage, not an obstacle to adoption. (Stamford, 2014).

As research and development of biometric technologies progresses, more and more banks joined the cause. Lloyds Banking Group, a major British bank, collaborated with Microsoft to offer their customers a new way to access their accounts from Windows 10 devices via fingerprint or facial recognition. What is important, the device can recognize the face of the user as opposed to an image, ensuring that no impersonator will be able to exploit it. Aside of clear security benefits, Lloyds' representatives believe that getting rid of passwords in favor of this quick and highly personalized method will greatly improve user experience. (Agidi, 2018)

Though users of biometric devices do not need to remember passwords or carry tokens, biometric characteristics are distinctive in nature and un-revocable (Y. C. Feng, 2008), Therefore it offers un-repudiation (Venkatesan, 2012), It should be remembered that biometric prototypes may be intercepted, compromised, replayed or manipulated if an unencrypted biometric device is connected to a network or if the attacker gains direct access to the device. This strengthens the need to prevent identity theft with technological countermeasures, such as cancelable biometrics, such as un-invertible transformations presented in (N. K. Ratha, 2007)and strong cryptography.

**Problem statement**

The Internet changed banking by offering convenient novel services. Mobile Banking systems give everybody the opportunity for easy access to their banking activities. These banking activities may include retrieving an account balance, money transfers between a user’s accounts, paying into someone else’s account, downloading account history. Some banks also allow services such as stock market transactions and the submission of standardized accounting payment files for bank transfers to third parties.

However, these advantages give rise to potential problems. A user authentication method is a required security element in mobile Banking. The use of simple authentication information has severe problems. We need individual authentication procedures. Many alternative authentication solutions have been proposed. These include ID/PW, Certificate with Security Card and Certificate with OTP Card. Although Certificate with OTP Card is one of the most secure methods, it is not a complete authentication method.

This paper proposes a fingerprint based secure authentication protocol using OTP (one time password). (Wan Yi, 2009)

**Motivation and Challenges**

Mobile banking is an essential part of daily life. If it's a retailer going to a daily brick-and-mortar shop, a retailer of digital goods, a tourist, a customer on a sales platform or a payer of bills they all have to pay for their products and or a parent paying these children's school fees.

These transactions usually take place via cash, credit or debit cards, which the customer carries on at almost all times.

In principle, it meets all the criteria a banking system requires. Skyrocketing market penetration levels for mobile devices and the fact that a person who owns a mobile device brings it with him nearly all the time will make it a more convenient alternative to banking with. Very far from being a common form of payment, though. The explanation for this is the lack of consumer approval based on perceived protection, the costs associated and the lack of need for a new payment option. (Pousttchi, 2004).

Likewise, biometric protection has been around for quite number of years, and is not technically a new innovation. With the latest global security risks, however, biometric technologies are being given new significance, which can provide better protection against fraud. (Sreekumar, 2010).

**Scope of the Thesis**

There are a number of issues that need to be resolved for mobile banking to become a successful mode of payment. These include standardization of the mobile banking procedures, alliances and partnerships between the players, customer acceptance and security (ECBS, 2003; Hampe et al., 2003a; Henkel, 2001a), amongst others. For the scope of this thesis, the issues concerning security and customer acceptance have been analyzed and discussed and a business model is proposed.

Security is an umbrella term that encompasses authentication, encryption, data integrity, non-repudiation and confidentiality (Hampe et al., 2003a). This thesis will concentrate on the authentication aspect of security as implemented in an mobile banking system. It considers the present authentication techniques and explains how biometric authentication can be used as a counterpart to the existing methods. In the context of biometrics, this thesis narrows down to the methods of speaker verification and fingerprint reading as appropriate authentication methods in mobile banking. A criteria catalogue is developed and used in Chapter 3 for this purpose. Enrolment plays a major role in successful biometric authentication and is also highlighted within this thesis. The hypothesis of amalgamating mobile banking and biometric authentication and the factors that need to be considered for its implementation is the focus of this thesis.

**PROJECT AIM/OBJECTIVES**

The objective of this study is to develop a design model that implements the concepts of using biometric authentication method to reduce risks of fraud and to improve customer’s trust in mobile banking[8][9]. Fingerprint takes only 256 bytes and its accuracy is high. The biometric device first captures the user’s finger print and creates a reference template and it is stored in database and that ends the enrolling processes of user’s finger print [10].

**The objective also includes the following.**

* Identifying reasons why customer distrust mobile banking
* Making a basic mobile banking transaction model and identifying security risks in mobile banking.
* Proposing Biometric finger-print mechanism for authentication to improve customer trust and self-satisfaction for mobile banking adoption for money transaction.

**Expected Outcome**

The authors propose transaction model for mobile banking. The basic model of mobile banking shows security issues and risks. The authors propose biometric model for mobile bank transaction and bio-metric (Finger Print) authentication method for mobile banking.

**Research Questions**

This thesis aims at answering the following questions by the end:

1. Why does customer not trust on Current Mobile Bank Transactions?
2. How is customer authentication done in contemporary mobile banking applications and what are the security issues in current mobile banking?
3. Is biometric authentication more suitable than contemporary authentication methods?
4. If yes, what factors should be considered during the biometric enrolment process?
5. Which biometric is best suited for use in mobile banking? Why?

Research Methodology

This work being a working hypothesis, there are only few references that directly address the issue under focus. The research work for this thesis was of exploratory nature. Academic resources and conference proceedings form a large part of the literature review for mobile banking, it being a rather young research domain. Seminal literature in the field of biometrics was used and was supported by conference proceedings and journal articles. Surveys, forecasts, professional websites, patents, news reports, press releases were also referred to in order to get a picture of the present market.

## Core Modules:

These are the main functionalities and the core of the project

* Image processing and enhancement
* Fingerprint (template) matching.
* Database module for storing the fingerprint images.

## Enhanced function:

Additional to validating the authenticity of user and capturing the time, the system also aims at including features to make the system more complete. Such features include:

* Generation of appropriate reports that are useful for the management/user to take appropriate actions.
* User profiling, where user can view their weekly or monthly-summarized transaction statement.
* Account management such as monitoring, adding, updating and deleting user.

Project Scope:

Functionalities of the system:

# Functionalities of Profiles & Management System:

## User Authorization:

This function is to grant access to user using username and password as well fingerprint authentication. This will give the user access to the system depending on their specified level (user or admin). Different level users are granted different level access in the system in order to increase the accuracy of the report collected as well as eliminating unauthorized access to the system.

## User Management

**Admin Functions:**

* Add user
* Edit user
* Delete user

**Account manager Functions:**

* Add new user account
* Delete user’s account

# Project Constraint

## 1.6.1 Limitations

Thus to complete the system, there are some limitations in the app that the developer will not be attempting on:

* Although this app could be implemented in a network environment, it is planned to simulate as standalone app.
* In case the fingerprint scanner does not capture clear and high quality images of the fingerprint, 2D images of fingerprint would be tested instead.
* The system also assumes that fingers are undamaged which means to say that this system is not capable of dealing with major changes that has taken place to the finger due to damages and/or scars.

## Time

Time needed to develop this mobile banking app is defined on the Gantt chart attached to the documentation. The Project includes many tasks that should be completed on less than three months including analysis, design, implementation, testing evaluation and documentation. However developing a system in short period of time is a challenging task that requires a transaction between different project phases and concentration on the critical areas rather than consuming time on tasks that have a little impact on the system.

## Manpower

In this project, the whole phase of an industrial based project in a comparatively short period of time was handled by the student only. In real situation there is more than one person specialized on deferent areas and have to communicate with each other in order to deliver a quality product that meet, the usually excessive and often unrealistic clients/system requirements.

# **Project Stakeholders**

Project Stakeholders are anyone who has an interest in the project, or whose interests maybe affected because of the project execution or project completion. Project Stakeholders for this project can divide into:

**Project manager**: Since this is an individual work, the student, who is the developer, will be responsible for the development of this project from the start until the end.

User: Users will be the organization that will use the project’s product, mainly the bank customers who are going to use the product to login. In addition, an admin in the bank who will be responsible for managing and maintaining the system.

# Literature view

# 2.0 Introduction

## This chapter starts by shading light on what mobile banking and biometric manager for mobile banking is all about. Consequently, the chapter continues with the brief history and profile of the fingerprint system from the commencement until today and the establishment of the finger print system offered good and valuable benefit to the customers and the banking institute when strictly implemented. This chapter goes on to identify the literature review comprising of findings. Every financial institute has a certain criteria to be meet before the customer can get access into their online banking system in order to prevent unwarranted access into the system or fraud.

**2.1 DEFINITION OF CONCEPTS**

(Siegel, 2011)defines mobile banking as the platform that enables customers to access financial services. (Drexelius, 2001)defined mobile banking as the ability to conduct bank transactions via a mobile device, or more broadly to conduct financial transactions via a mobile terminal. (N., 2009)define mobile banking as 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. They further indicate that mobile banking refers to provision and ailment of bank-related financial services with the help of mobile telecommunication devices. The scope of offered services may include facilities to conduct bank and stock market transactions, to administer accounts and to access customized information from the bank. On the other hand, (Barnes, 2003)defined mobile banking as “a channel whereby the customer interacts with a bank via a mobile device, such as a mobile phone or personal digital assistant (PDA)”. Mobile banking services can be classified based on the originator of a service session, either “push” or “pull” (Technologies, 2007)‘Push' is when the bank sends out information based upon an agreed set of rules, for example the banks sends out an alert when the account balance goes below a threshold level. On the other hand ‘Pull' is when the customer explicitly requests a service or information from the bank, for instance requesting the last five transactions statement. The other way to categorizing the mobile banking services is based on the kind of services, either transaction-based or enquiry-based (Technologies, 2007). A request for the bank statement is an example of enquiry-based service while a request for our fund's transfer to some other account is an instance of transaction-based service. According to (Technologies, 2007) presently, mobile banking is being deployed using mobile applications developed on one of the following four channels: (i) IVR (Interactive Voice Response) (ii) SMS (Short Messaging Service) (iii) WAP (Wireless Access Protocol) and (iv) Standalone Mobile Application Clients. Mobile banking offers many benefits and advantages to not only customers or users, but also to the telecommunication providers and financial institution that provides the services. (Goswami, 2009) noted that based on best practices in mature mobile-banking markets, the advantages of mobile banking to end-users include (i) secure authentication, transaction and data transmission, and easy deleting of content in event of handset loss (ii) icon driven, user-friendly interface (iii) contactless payment that offers quicker checkout at the point of-sale and replaces all current payment solutions (iii) dynamic credit facility and innovative point-of-sale offers (iv) dynamic account monitoring and around-the-clock alerts (v) convenience of micro-payments (parking meters, vending machines) (vi) real-time access to account information, outstanding debt, and bill payment (vii) ubiquitous access to banking services. With mobile banking, telecommunication providers can expand their services portfolio, promote their brands and create strategic marketing differentiation, hence attracting new customers (Gemalto, 2011). (Aslam., 2009) Suggests that for a banking regulator it is important to provide adequate protection for consumers, ensure economic stability, provide interoperability of electronic system and guarantee security of transactions and Anti-Money Laundering and Know-Your-Customer principles must also be applied to mobile banking. (Comninos, 2008) Suggest that unbanked will only transact electronically (online/mobile banking) if there is convenience and security. (Singh, 2011) State that mobile banking user are specially concern with security issues like financial frauds, account misuse and user friendliness issue - difficulty in remembering the different codes for different types of transaction, application software installation & updating due to lack of standardization.

Since there are an increasing number of channels to transact financial information, the amount of security to protect these channels is increasing as well. With the increase in the electronic channels offered through retail organizations and financial institutions, there is greater access through the Internet to individual information that was once considered private. The result is an augmentation of identity theft and account hijacking.

**Important Aspects of mobile banking**

To establish the framework and area covered by this thesis, a few essential characteristics of mobile banking will be described in this section. Till date, there have been numerous attempts at introducing a successful mobile banking application around the world. While many have had to cease operations like Paybox (Ding, 2003)and Simpay (Finextra, 2005)for instance, a few mobile banking systems have crystallized out successfully. The most successful and sustainable employment of mobile banking has been in mobile ticketing in different transportation facilities and online transactions. mPark is a facility that offers paying for parking using mobile banking and is available in the UK, Germany, Ireland and Australia1. *Deutsche Bahn* in Germany offers mobile ticketing facilities.

**Classification of mobile banking**

Mobile banking can be used in different environments, independent of the physical location of the user and the mobile device. With reference to the environment, mobile transactions can be classified as follows (Hampe, 2003b):

* **Local transaction:** A local transaction is where the mobile device is present at the payment terminal like a store POS or an Automatic Teller Machine (ATM) and it communicates locally with the transaction terminal (Karnouskos, 2004). Local transactions are also known as proximity transaction or contactless transaction because the transaction takes place in close proximity to the terminal via short range wireless communication technology (Hampe, 2003b) like Bluetooth, Near Field Communication (NFC) or infrared.
* **Remote Transaction:** A remote transaction is a mobile transaction that takes place irrespective of the consumer’s location (Karnouskos, 2004) When buying a bus ticket, shoe, ringtones or games (digital goods), the customers could be anywhere. These are examples of remote environments where the location of the consumer while initiating the payment is insignificant*.* Such transaction can be browser-based as in the case of digital goods or SMS-based as in the case of mobile Ticketing (Hampe, 2003b).
* **Transactions in a personal environment:** A transaction in a personal environment is a transaction that takes place between several devices that are controlled by the user (Hampe, 2003b). An example of this could be topping up the credit on a prepaid mobile account from another mobile device using mobile banking. A parent could transfer airtime to the mobile device of a child, for instance. NGPay, one of the mobile banking applications in Nigeria, plans to offer such intra-mobile money transfer through their application.

The reason these transaction environments are listed is that the biometric mobile banking application as described in this thesis is a ubiquitous one that can be used in any of these environments.

**Players in the mobile banking Scenario**

Players are the different entities involved in a mobile banking scenario who contribute to the mobile banking set-up in one way or the other depending on their core competency. These entities can be organizations, companies or individual persons. The players directly involved in the mobile banking process are referred to as active players. These are the players that directly influence or are a part of the mobile banking life-cycle depicted in Figure …. Banks and Mobile Network Operators (MNO) are examples of active players. Passive players are players who do not directly contribute to the mobile banking life-cycle, but who have a supportive role in the provision of mobile banking.

**Banks:** Banks and other financial providers like credit card companies constitute the other large player in the mobile banking scenario. What makes banks attractive as the mobile banking provider is the customer trust that they enjoy (Krueger, 2001).

Banks have long existed in business and the customer is used to entrusting his money with the bank. Introducing a mobile banking application under the banner of a bank boosts customer acceptance since the trust the customer has in the bank is transferred to the mobile application. Also, their core competency being monetary transactions, banks have the required experience and risk management facilities to handle mobile banking transactions (Zmijewska, 2006) (Henkel, 2001a)not to mention that they have an existing service infrastructure and vast merchant database. As an acquirer, banks have an existing number of merchants who partner with them for debit and credit card, saving and current account. This gives banks a good starting point if the merchants cooperate and agree to offer the given mobile banking application as a banking option. In a bank-dominated model, the bank is the prime player in the value chain. In such a case the bank is the player offering the mobile banking application, relying on the MNO as the data carrier. Although banks do not “bill” customers, they can still be responsible for accepting the transaction/payment on behalf of the mobile banking provider by simply deducting it from the customer’s bank account (if the customer has an account in the given bank) or by initiating the transfer of money from the customer’s account in another bank. As in the case of MNOs, the degree of involvement can vary for banks too

**Merchants:** The role of merchants in the successful functioning of a mobile banking system is often underestimated. Merchants are as important as the end-user is in the mobile banking scenario. For a consumer to adopt mobile banking, a substantial number of merchants need to offer it as a service option. The greater the number of users for a given banking system, the more worthwhile it is for the merchant to implement the system, and conversely, the greater the number of merchants, the more worthwhile it is for the customer to start using the mobile banking system (Henkel, 2001a). This unfortunately forms a vicious circle; the consumer may hesitate trying out a new banking system if he cannot use it widely. The merchant, on the other hand, may not be willing to offer a new banking system if he is not convinced of a strong consumer acceptance. It could be argued that merchants are more passive than active players. However, the author finds that since merchants strongly influence the success of mobile banking and since they are directly involved with the banking system, they can be classified as active players.

**Third Party Players:**A third party player is an independent mobile banking service provider who is neither a bank nor an MNO, but who provides a mobile banking solution. NGPay for instance, is an example of a third party driven mobile banking solution. Third party players are usually start-ups and they depend on MNOs, either in a partnership or just as a carrier. The involvement of an established player like a bank or MNO helps the third party player to market its mobile banking application better – an aspect required to gain the trust of its customers and to obtain a large number of both customers and merchants to use the new mobile banking solution.

**Passive Players**

**Mobile Device Manufacturers:** As a passive player, the mobile device manufacturer only indirectly influences the mobile banking system. In present day mobile banking scenarios, the mobile device manufacturers do not have a big role to play. Equipping mobile devices with adequate software and hardware required for mobile banking could possibly be the responsibility of the mobile device manufacturer. This software could include mobile Wallets, payment enabling applets, etc. However, most software that would be required can also be made available to the users as downloads from the internet and there is no additional hardware requirement for the present day mobile banking applications. If however, the mobile banking application is to use biometric authentication, then additional hardware such as the fingerprint reader are required. In terms of its role in the mobile banking value chain, the device manufacturer is primarily responsible for the hardware components required for mobile banking. The role of the mobile device manufacturer can be illustrated using proximity banking as an example. The NFC interface/unit over which the transaction data are transmitted needs to be implemented in the device. An example of such a contactless mobile banking solution is the mobile Ticketing facility in the city of Stuttgart Germany.

**End-User/Consumer:** Possibly the most important link in the value chain, the consumer is the entity that eventually uses the mobile banking systems. If there aren’t enough customers using mobile banking, it is unlikely to be successful. The greater the number of users, the more valuable the banking network (Henkel, 2002). Precisely defining and understanding who constitutes the target population is vital for the functioning of any business idea (Hammer, 2003). The product has to fulfil the demands of the target group and should be tailored to their likes and dislikes. The entire life-cycle of a product is more or less influenced by this; the branding, the marketing approach and the channels used. All this depends on the target customer. This holds good for mobile banking too. As described earlier, the adoption of the mobile banking system by the merchant greatly influences consumer acceptance and vice versa. If the merchant does not see a substantial number of customers using or wanting to use a particular banking system, it is not feasible for him to provide it as a transaction option. It can be seen here how the network effect could affect the acceptance of the merchant. Conversely, if the customer cannot use a banking system at a number of merchant establishments, the banking system would not be attractive to him.

**Security Features**

There are five features to security in an electronic transaction. These are authentication, confidentiality, encryption, data integrity and non-repudiation (Hampe, 2003a).

**Authentication:** Authentication refers to the ability to uniquely identify the parties involved in a transaction and to determine the validity of this identity (Creese, 2004). In a banking transaction, it is important that both the customer and the merchant are authenticated (Dannenberg, 2004) since both are equally prone to fraudulent attacks. While the merchant could be faced with a fraudulent customer with a stolen identity, the customer could be faced with a fake merchant through attacks such as phishing. Phishing is a method of attempting identity theft, where the offender sends out emails pretending to be a merchant or the user’s bank and requests personal data from the user such as his password or banking details. This often involves misdirecting the user to a site that looks like the merchant’s or the bank’s official site. Although phishing is more predominant on the internet, it is slowly finding its way to the mobile world, too (Chellam, 2005).

**Confidentiality:** Confidentiality refers to the user identity and user information being kept concealed (Dannenberg, 2004). In any banking transaction, data pertaining to the customer like his address, the purchased item and probably the credit card details or bank account details are collected. While this information is necessary to carry out the transaction, the collected data should not be disclosed to any third party unless legally required to do so. It should be used only in context with the payment. Confidentiality of the data should be maintained not only during the transmission but also when it is stored. In many situations of identity theft, stolen credit card details and similar kind of frauds, it is not during transmission of the data that the information is stolen, but by hacking into the central repository where this data is stored.

**Encryption:** The safe transmission of data requires it to be encrypted. Encryption means that the data is encoded and cannot be read/ deciphered without the key to decrypt it. This ensures that data transmitted cannot be tapped during the transmission, which is vital in a mobile banking situation where the transaction details have to be transmitted.

**Data Integrity:** Data integrity means that the data cannot be modified in any way by unauthorized persons. The data should be transmitted to the merchant and from the merchant to the payment provider in the same state as it left the customer. The data should be protected from intentional as well as unintentional attacks (Dannenberg, 2004).

**Non-Repudiation:** Non-repudiation is the assurance that the financial transfer has taken place. Non-repudiation is necessary to ensure that neither the sender nor the receiver can deny having sent/received the data, or in the case of mobile banking, the money. This non-repudiation of the end-user is of great significance to merchants/vendors (Hampe, 2003a)), since it ensures that they receive their money. Ensuring that these five features are met would mean that the following questions are answered:

* **Is the customer who he claims to be?**
* **Is the merchant who he claims to be?**
* **Is my data in the right hands? Will it be passed to a third person?**
* **Can my data be read during transmission?**
* **Has the merchant received my transfer?**

Assuring these five security features also increases the trust of the customer in the mobile banking system. Knowing that the transaction get to it intended destination, that the data is kept both safe and secure and that the transaction is carried out with no problem would possibly remove all doubt from the consumer’s mind.

**Authentication – The Key Security Issue**

Authenticating a user can be done in numerous ways like using passwords, PINs, smart cards or tokens. Based on the method used, authentication can be divided as follows (Bolle, 2004; Currie, 2003)

(i) **Knowledge-based authentication (K):** Something the user knows like PINs and passwords.

(ii) **Object-based authentication (P):** Something the user owns like smart cards or tokens.

(iii) **Biometric-based authentication (B):** Something the user possesses like measurable personal traits of the user.

(Ratha, 2001) Include in their list of current user authentication techniques a fourth, hybrid form of authentication, (Bolle, 2004)also state that, you make use of a combination of knowledge and possession as in the case of using an ATM with the ATM card and a PIN see table 1.

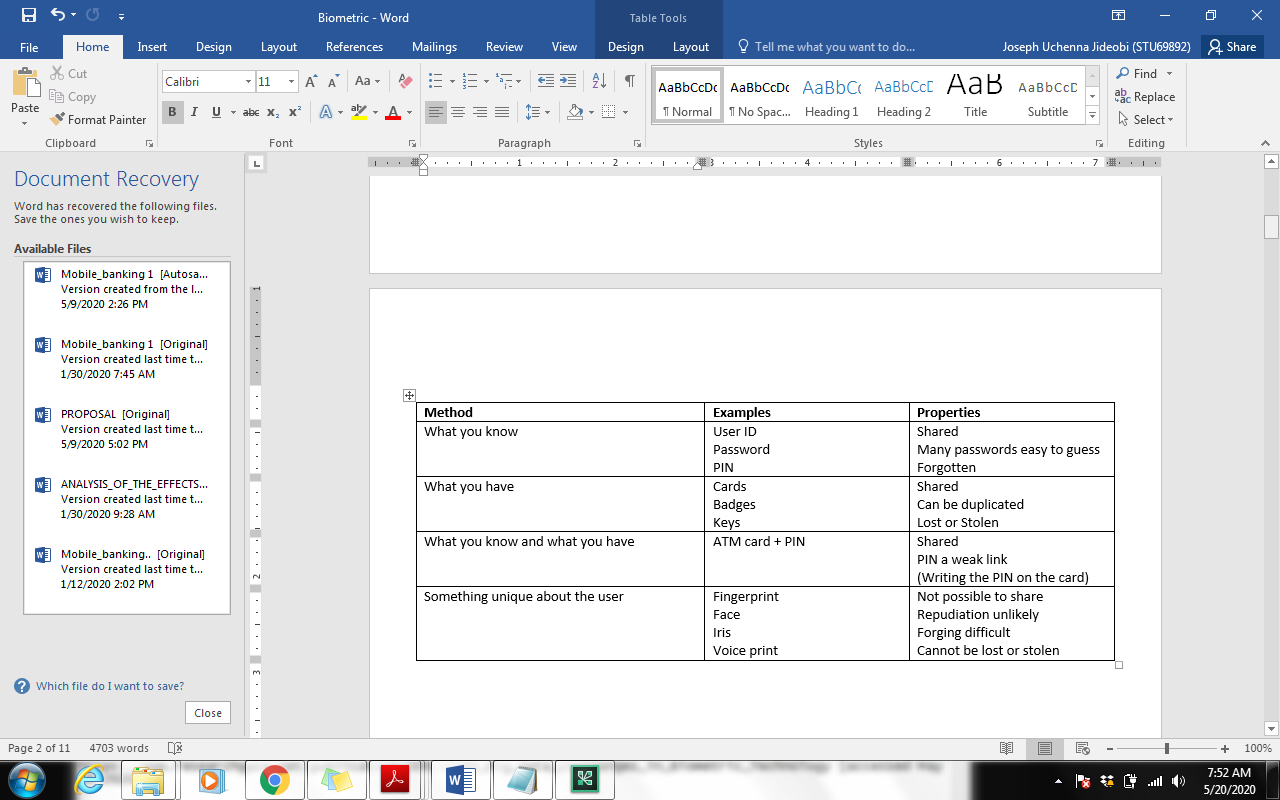


Figure ….. showing different type of authentication (Author, 2013; Ratha, 2001)

Here, the plastic card is the object the consumer has and the PIN is the knowledge he possesses. An identification card with the biometric feature of the person embedded in them would be: (P,B)→(ID,FINGERPRINT)

Here, the user has his ID, which is something he possesses, and it makes use of the user’s biometrics, which is a part of the user. The current most widely spread authentication form is the usage of PINs (Nanavati, 2002)). By force of habit or merely having no other choice, most consumers have become accustomed to PINs. In many mobile banking systems, authentication takes place within the mobile device usually by entering the PIN. When using a mobile device, there is a clear identification of the user as he enters the PIN to access the SIM card and thereby more security than when using debit cards or credit cards which require only a signature. Forging a signature is far simpler than cracking a PIN (Henkel, 2001b). PINs can be a secure mode of authentication if the PINs are long enough and complicated enough so that they cannot be cracked; but this is rarely enforced as such PINs are difficult to remember. This in turn might cause user to write them down, thereby bringing back the security to almost null (Rila, 2002). (Ratha, 2001) Argues that, luckily, automated biometrics in particular can provide an accurate and reliable method of identity verification. They illustrate that there is swift progress in the field of biometrics in identifying an individual based on his/her physiological or behavioral characteristics. According to (Ratha, 2001). User authentication methods may be broadly categorized into three categories as shown in Table 1.

Authentication can also be provided by biometric methods. As mentioned in Chapter 1, biometric authentication refers to the automated use of unique human characteristics to verify a person. There are quite a few advantages that make biometrics better than PINs. The key advantages of biometrics over knowledge and token-based authentication techniques are that biometric characteristics cannot be forgotten like a password, or lost like a key (Currie, 2003; Rila, 2002); nor can they be stolen or given willingly to another person. Also, the fact that biometric authentication information is non-transferable makes it powerful against repudiation (Rila, 2002)

Effective authentication is the central activity within the mobile banking value chain (Contius, 2003). Ensuring that only the rightful owner has the ability to use a given payment system would increase the trust the customer has in the security of the system. Also, ensuring good authentication would minimize fraudulent usage of a payment system, thereby reducing the risk factor for the merchant and the payment provider. Hence, ensuring that there is an authentication process in place that the user is comfortable with, that the user trusts as secure enough is an important factor for any mobile banking application. Since authentication has been established as a key factor in mobile banking, the choice of which authentication method should be used to ensure a safe payment environment arises. Of the three methods of authentication, token-based authentication does not qualify for use with mobile banking since it requires the user to carry an additional item on him, which defeats one of the purposes of using mobile banking, namely the reduction/elimination of carrying cards, cash or other items for payment utilization. This leaves us with biometric-based and knowledge-based authentication. As knowledge-based authentication methods are widely in use today, it has been decided to explore the possibilities of using biometric-based authentication in mobile banking systems. The main reasons for this are the advantages that biometric authentication has over knowledge-based authentication. PINs can be forgotten, shared and are easy to guess. Users nowadays are subject to remembering PINs for various applications – their cards, the mobile SIM, phone banking etc. This can lead to the user getting confused between the various PINs or forgetting them. Biometrics on the other hand are always on the person and are almost never subject to change. They are unique and cannot be easily forged. Therefore, biometrics seem to be a more secure option than PINs as they satisfy the 5 security features better than PINs; additionally, they are more convenient to use than PINs since the user does not need to remember anything. The reason why biometrics are chosen is discussed in detail in Chapter 3; the chapter will also deal with identifying a biometric that would be best-suited for use in mobile banking.

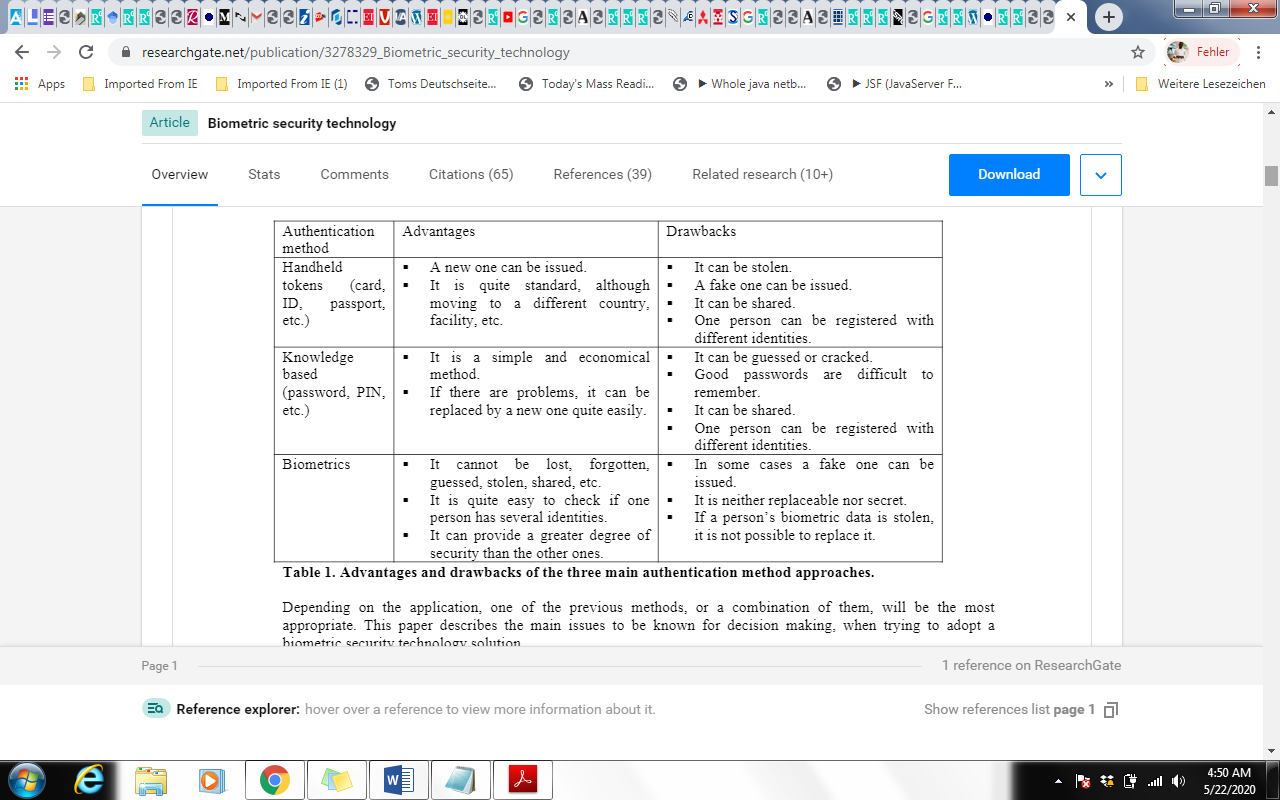


Table 2 Advantages and drawbacks of the 3 different concept to authentication.

**Identifying a Biometric for mobile banking Systems**

Identifying people by means of their physical and behavioural characteristics is used everyday by everyone (Nanavati, 2002). We recognize people by their face; on the phone we are able to identify people we know based on their voice. Sometimes, we are even able to recognize the people we know by the way they walk. This kind of manual recognition however is not biometric recognition: biometrics is the **automated** recognition of people based on their physical or behavioural characteristics. Biometrics are finding their way into different fields as a means of establishing secure identification and authentication as described in Chapter 1. Early adopters of biometrics were government agencies and the military (RCMP, 2002). Today, biometrics are used in relatively trivial applications, such as securing laptops, to more conscientious applications like citizen ID cards, airport security.

**In this chapter, the researcher try to describe:**

* why biometrics could be considered as an authentication method in mobile banking and
* given the various biometric methods available, filter out the biometric methods most suitable for mobile banking applications.

**The Basics of Biometrics**

To identify a suitable mobile banking biometric, a basic understanding of the biometric subject matter is required. This includes the definition of biometrics, how the consumer’s biometric data is captured, defining how biometric accuracy is measured, and differentiating between identification and verification.

**Biometric Definition**

As defined by (Nanavati, 2002) biometrics is the “automated use of physiological or behavioral

characteristics to determine or verify identity.”

The (Author, 2013) define biometrics as “the development of statistical and mathematical methods applicable to data analysis problems in the biological sciences.”

The term is derived from the Greek words bio (life) and metric (to measure).

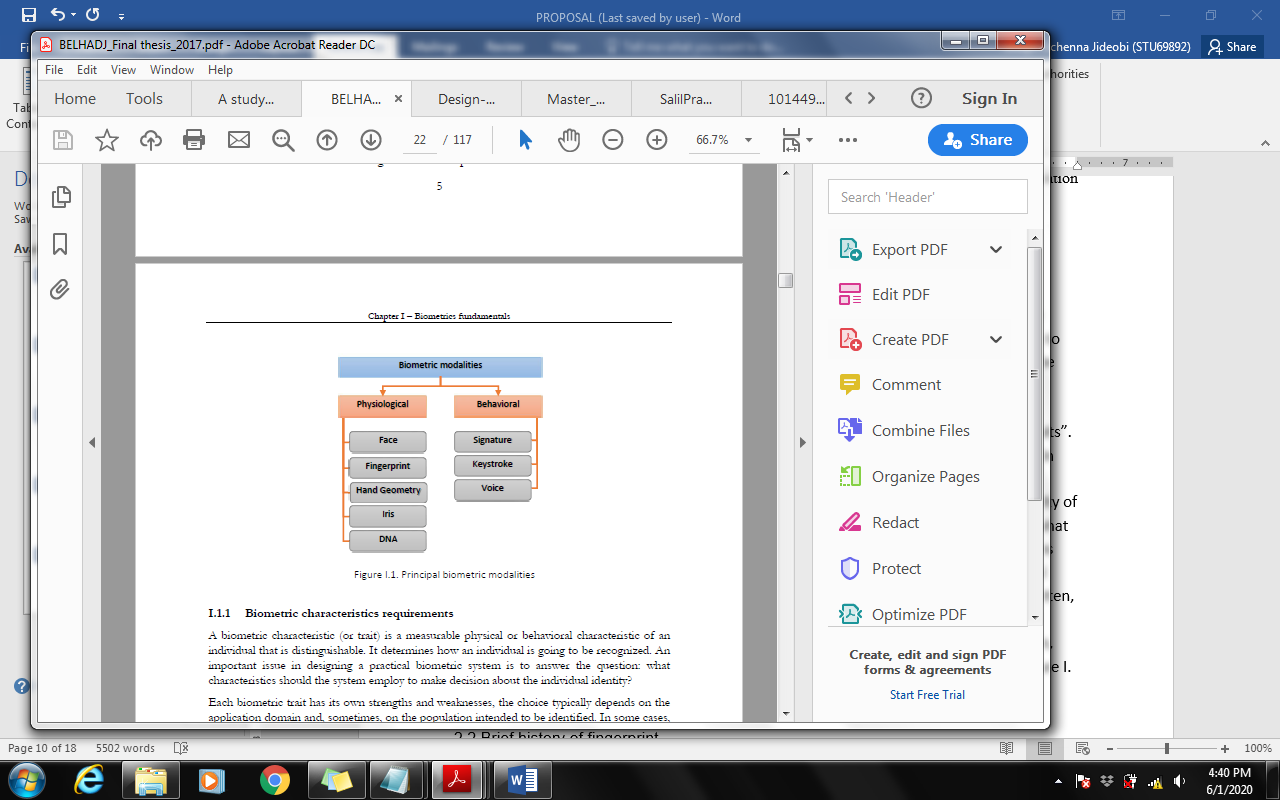
(Bolle, 2004) Has explained biometrics in more detail as: “Biometrics refers to identifying an individual based on his or her distinguishing characteristics. More precisely, biometrics is the science of identifying or verifying the identity of a person based on physiological or behavioral characteristics”.

Biometric technique is divided into two broad categories, via – 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.

The International Standardization Organization (ISO) defines the term biometrics, or biometric recognition, as being “the automated recognition of individuals based on their biological and behavioral characteristics” (ISO/IEC2382-37, 2012). The definition uses the word ‘automatic’ to imply the design of algorithms to be executed by a machine system to recognize individuals. The system could be assisted by a human to get better results. The ‘recognition’ aims to associate an identity with an individual based on some physical characteristics exhibited intrinsically by his body parts and/or some behavioral characteristics created by the body. These characteristics are called “identifiers” or “traits”. Examples of physical characteristics include among others: fingerprints, face, iris, etc. On the other hand, behavioral characteristics may include: signature, voice, keystroke dynamics, etc. Differently to the classical identification systems that establish the identity of an individual based on what he knows (secret information such as passwords) and/or what he has (possession of objects such as tokens, smartcards, licenses, …); biometric systems are based on what the person is (biological attributes) and/or what he does (behavioral attributes). These identifiers are directly related to the individual, thus cannot be forgotten, neither copied nor transmitted. Biometric systems exploit a variety of biometric characteristics (or modalities) including fingerprint, face, ear, iris, retina, palm print, vein, voice, signature, gait, odor, etc. The most leading biometric modalities are listed in Figure I.



Figure…… biometric modalities

**Biometrics Technology**

Biometrics is a method of identifying individuals that has been in operation for several years. Each of us routinely uses biometric identifiers such as voice and facial characteristics to recognize family and friends. Recent prominent security lapses have brought an increase in awareness of the need for greater security measures, so biometrics have been transformed into an authentication technology that can be automated. There is an increase in the level of security for an individual’s account because biometric systems reliably validate that the enrolled account holder is the one requesting authorization. This is the main difference between the use of biometrics and passwords because passwords can be compromised, shared, or forgotten. A basic definition of biometrics involves the use of physiological or behavioral characteristics to verify an individual’s identity (Bolle, 2004) Physiological biometrics is a physical measurement such as the verification of a fingerprint, hand, eye or face. Behavioral biometrics takes a measurement of how an action takes place, such as a signature. In order for a measurement to qualify, as biometric, certain requirements must be met (Zorkadis, 2004); (Prabhakar, et al., 2003) (Jain, 2004)):

* **Universality:** Each individual ought to have the trademark.
* **Distinctiveness:** This can also be alluded to as uniqueness, see table 1 (Yun 2002). Any two people ought to be sufficiently diverse to recognize them from one another dependent on this trademark.
* **Permanence:** The trait should be sufficiently stable (with reference to the corresponding set of criteria) over time, different environments condition, etc. (JAMMI ASHOK, 2010)
* **Collectability:** Trait must be acquired, and quantitatively observable.
* **Acceptability:** Users should embrace the biometric program, and not believe its intrusive, creepy, etc.
* **Performance:** Accuracy of authentication and the time needed for a positive recognition must be strong.
* **Circumvention:** The possibility of fraudulent individuals and tools to pervert the biometric system ought to be marginal. (JAMMI ASHOK, 2010)

With all biometric measurements and corresponding requirements, there are two methods of authentication.

In the beneath table 3, Universality show how basic the biometric is in every person; uniqueness show how well the biometric recognizes one individual from another; permanence show how well the biometric opposes the impact of maturing; and collectability quantifies that it is so natural to procure the biometric for the procedure. performance show the feasible precision, pace and robustness of the biometrics while acceptability means the degree of open acknowledgment of innovation in their regular day to day existences and circumvention demonstrates the difficulty of circumventing or tricking the framework into tolerating an impostor.(Yun 2002)

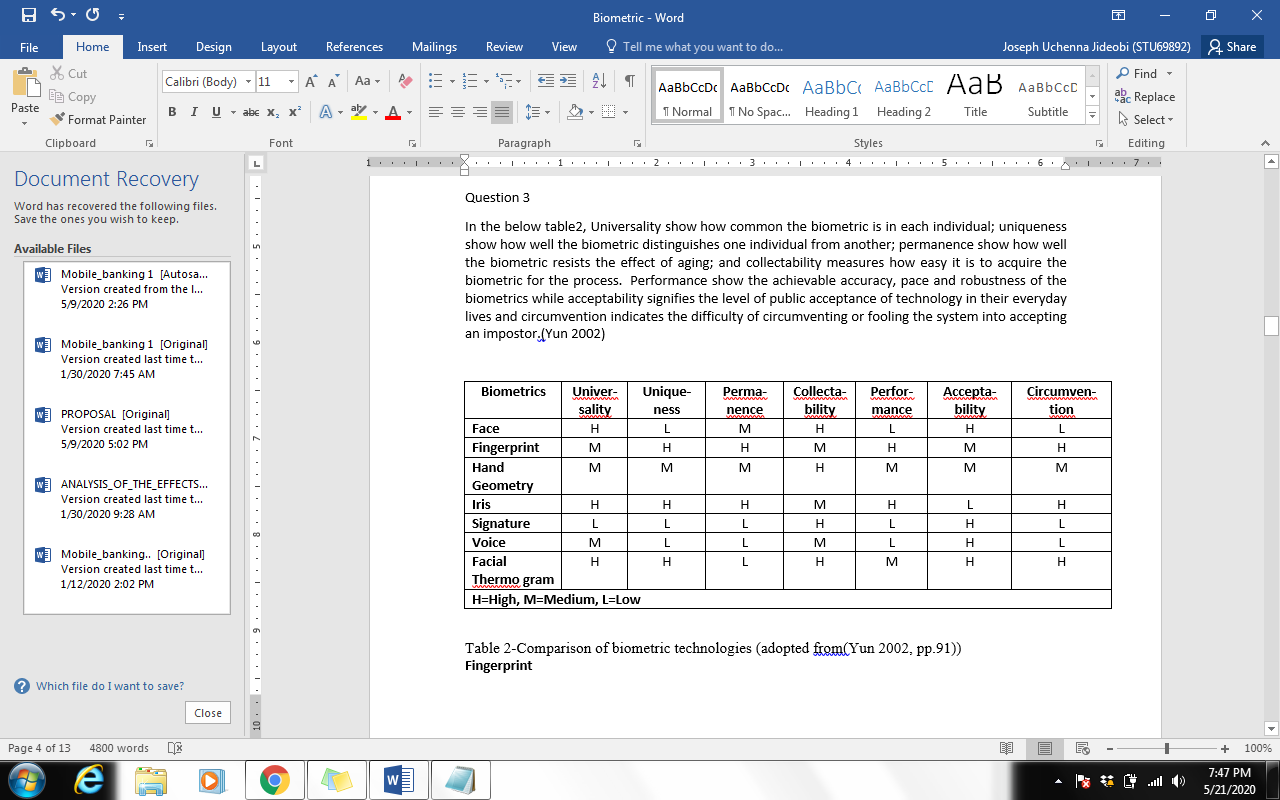


Table 3-Comparison of biometric technologies (Yun, 2002)

**Biometric Authentication**

Authentication is described as the process of determining the identity of a communicating party (Bolle, 2004) as stated before, there are two types of biometric authentication methods that can be used: identification and verification. If the method chosen is identification, it is a one-to-many search in a database of participants’ biometric records. It would be the sole means of identification for an individual requesting access. The alternative method is verification. It is considered a one-to-one or one-to-few search in the authentication process. (Jain, 2004) Each individual’s biometric record is stored in a database along with an additional unique identifier such as an account number. When an individual attempts to perform a transaction on a biometric system that uses the verification system, it first performs a search on the database for the submitted identifier and then verifies that the biometric scan from the sensor matches the individual’s stored biometric record assigned to that particular identifier. In either method, individuals are authenticated with something that is unique to them that cannot be shared, borrowed or lost. Once an authentication method is chosen by an organization, the next step is the enrollment process.

**Enrollment Process**

In the development of the enrollment process, it must first follow a determined enrollment policy due to the fact that very private information will be supplied to the organization that will in turn be required to protect it (Bolle, 2004)As stated before, the concept of biometric authentication is that the system verifies the identity of the individual requesting access by confirming a unique physical or behavior characteristic that matches a similar stored record in a database. This is why it is imperative that the identity of the individual enrolling is in fact correct. The biometric verification method is not capable of determining the true identity of an individual. The enrollment policy has the responsibility of verifying a person’s identity even before the technology portion of enrollment begins. Once an individual is verified, the physical enrollment can proceed. Depending on which type of biometric is used, a template or model is created from the unique characteristics of an individual for that particular biometric reader. In order to create the template, the reader, or sensor, takes specific samples of data from the subject and converts the data into a mathematical record to be stored in a database. In the case of a verification method, this mathematical record would be coupled with a unique number (for instance, an account number). A template can contain multiple records for the same individual for an improved acceptance rate when the opportunity comes to apply it beyond the initial enrollment period. Once the enrollment process is complete, the subsequent attempts for access behind a biometric authentication system will compare the individual’s live scan to the stored template in the database ( (FDIC, 2004); (Bolle, 2004)). The behavioral biometric method uses the same general process except that it uses models instead of mathematical templates. One of the drawbacks in the biometric enrollment process is that it is not 100% accurate.

**Error Rates**

There are two classes of errors in the accuracy of biometric authentication. The first issue is called a False Acceptance Rate, or FAR. The FDIC report describes a False Acceptance Rate as “the probability that the system will accept a false biometric credential as legitimate” (FDIC, 2004). FAR occurs when, for example, an individual requesting access to his or her account, instead is given access to another person’s account. The other issue is called a False Reject Rate, or FRR. The FDIC report describes a False Reject Rate as “the probability that the system will reject a valid biometric credential” (FDIC, 2004).

This would be an issue when a legitimate individual is denied access because the biometric authentication system cannot match the person’s live scan with any records in the database.

These issues are the reason why current biometric authentication systems are primarily an additional level of security versus a sole method of authentication. There are many biometric identifiers currently under development, but the more common biometrics technologies in use and in production is described in the following section.

**Selecting a Biometric – The Criteria Catalogue**

To select a biometric best-suited for mobile banking, a set of criteria were established based on factors that are of significance to mobile telephone and banking. These criteria serve to compare the different kinds of biometrics and in the process, to find out which one is best suited for mobile banking. On a high level, these criteria have been classified as *technical factors, security, business factors* and *consumer* *acceptance*.

**Technical Factors**

The **device size** of the biometric reader should be small enough to fit into the mobile device. Mobile devices today are becoming smaller and smaller and if the size of the biometric reader impacts the overall device size, it would possibly not be attractive to the consumer who looks for his mobile device to be as small as possible.

Another factor is the **technical reliability** of the biometric (Teletrust e.V., 2002). Technical reliability would mean that the hardware used to read the biometric and the software that processes it function consistently.

The chosen biometric should be **robust** and able to perform accurately under all circumstances. External factors like background noise, dirt, heat or humidity shouldn’t affect the system.

**Security Factors**

The **accuracy** of the biometric used is paramount in the choice of the biometric. The accuracy of the biometric greatly depends on the threshold value and the quality of the enrolment process. The chosen biometric must be **secure**. This security is dual-fold; not only must the

biometric secure the data it is protecting, but the biometric data, namely the template, needs to be secure (Teletrust e.V., 2002) in terms of the five security factors described in Chapter 2. Security in this context refers to how secure the biometric template is. It should neither be easy to forge the template, nor should it be possible to circumvent the biometric and gain access to the data it protects.

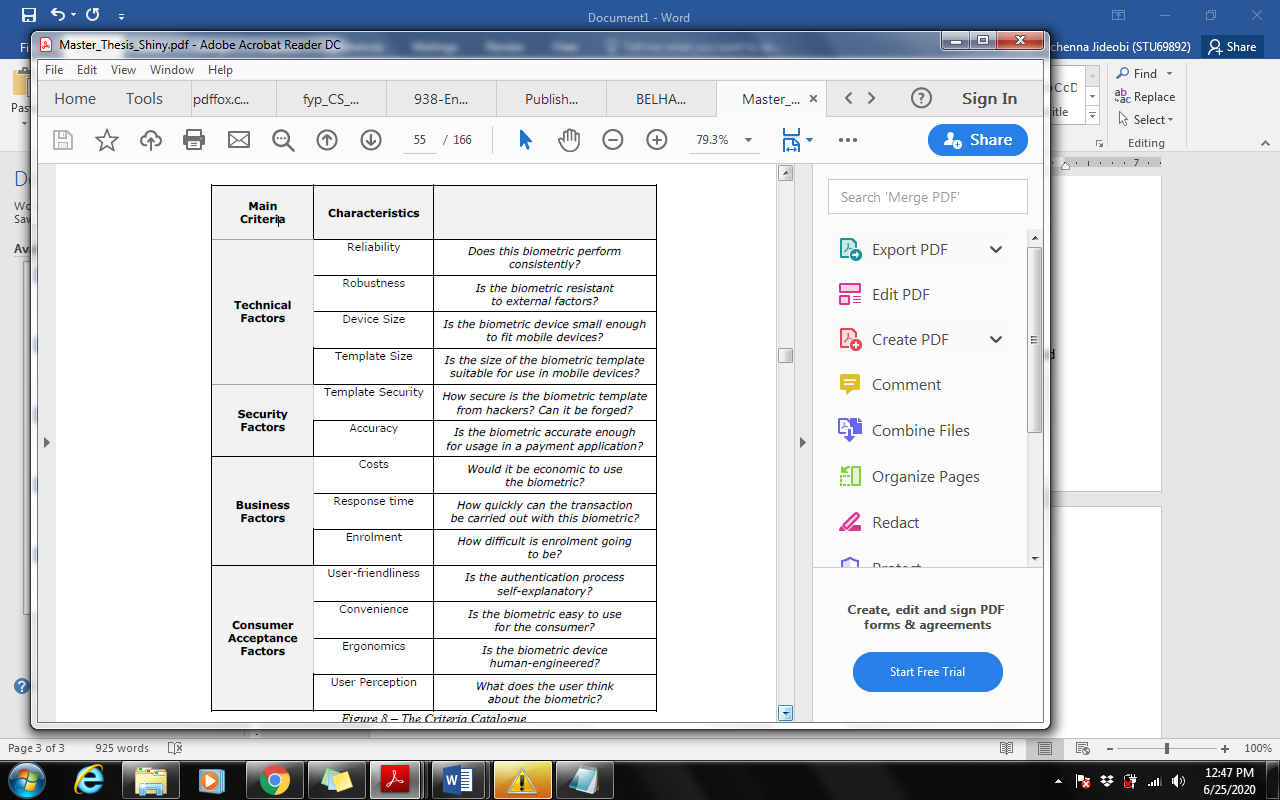
**Business Factors**

Using biometrics should be **cost-effective** for all parties involved and especially for the customer. The biometric-based mobile banking system should be cost-effective enough that the customer chooses it over other banking options. The more expensive the implemented hardware in the mobile device, the more expensive the device becomes, which in turn would deter the consumer from trying out the service. Response time is another significant criterion to be considered. Response time refers to the time taken to authenticate the consumer. It is “the time required to measure the human characteristic in order to create the template and the storing time of the template” (Royal Canadian Mounted Police, 2002). The response time starts at the initiation phase when the app is being open and ends with the transaction authorization after which the consumer receives his service. This whole process should ideally not take more than a few seconds. A normal card transaction takes around 10 – 15 seconds. Given this, a mobile banking transaction using biometric authentication should not exceed the same time. Longer response times, even if only by a few seconds, can make the process seem time-consuming and can annoy the customer.

**Factors affecting Consumer Acceptance**

For the customer to use a new technical system, it needs to be user-friendly. Biometrics like iris-scanning and retina reading tend to be rather user- “unfriendly” since it requires the user to look into an object, which can be a bit awkward. This could make him uncomfortable and not very keen on using the system.

The ergonomics of the biometric device plays an important role in customer acceptance (Teletrust e.V., 2002). The biometric should be convenient and intuitive to use without making him feel that it is too technical.

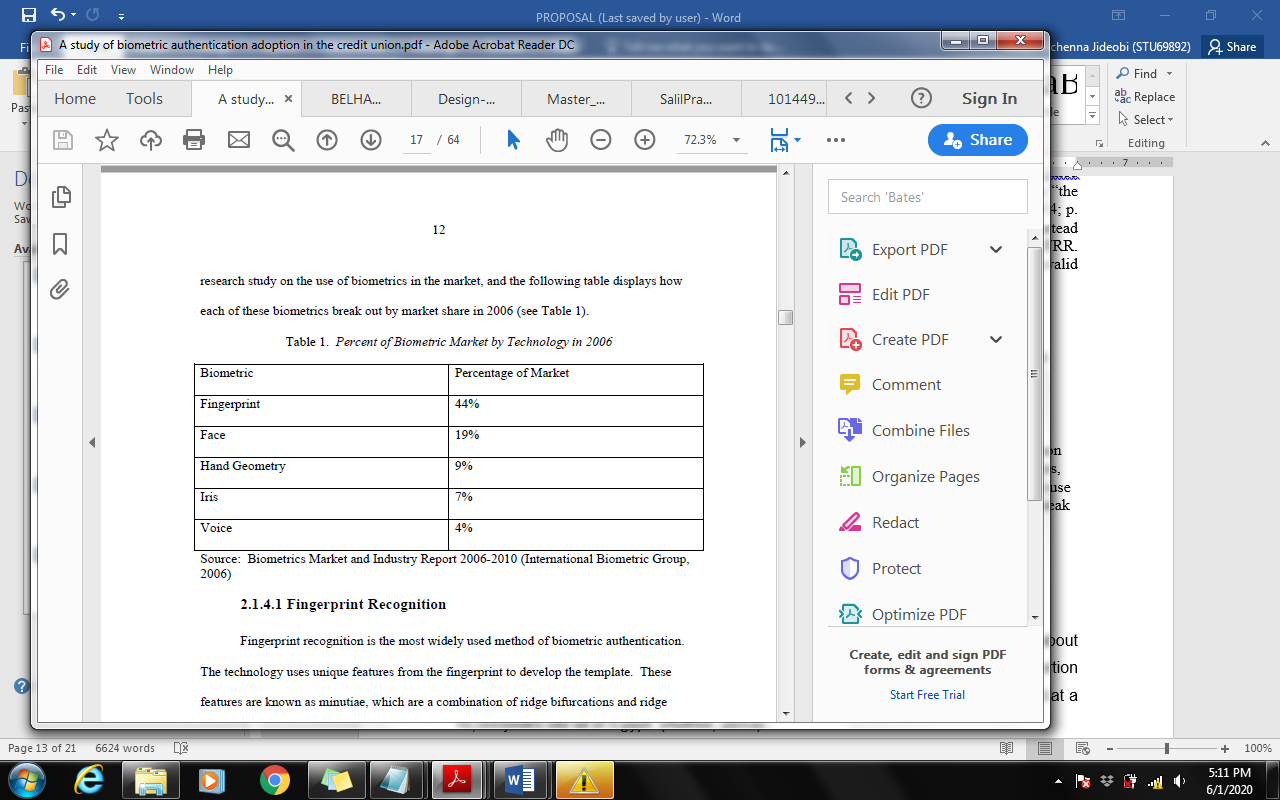


Another factor influencing customer acceptance is the **user perception** of the biometric (UK Biometrics Working Group, 2002). Fingerprint verification, for instance, is easily associated with criminal records and therefore, users may not be comfortable using this as a verification technique.

# **Types of Biometrics (**Current Applications in Biometrics)

There are various biometrics in research that can vary with anything from a person’s fingerprint to the way that he or she walks, but for the purposes of this study, the most common biometrics will be described. These include fingerprint, facial recognition, hand geometry, iris, and voice recognition. The International Biometric Group performed a research study on the use of biometrics in the market, and the following table displays how each of these biometrics break out by market share in 2006 (see Table 1).

Table 1. Percent of Biometric Market by Technology in 2006



Source: Biometrics Market and Industry Report 2006-2010 (International Biometric Group, 2006)

### Fingerprint technology

A fingerprint is a ridges and grooves at a fingertip surface. Fingerprints are exceptionally stable and distinctive. The uniqueness of fingerprint is defined by global characteristics such as valleys and ridges, and by local characteristics such as ridge ends and ridge bifurcations, refer as minutiae. (Mir A.H, 2011) Recent studies show that there is less than one in a billion in likelihood of two persons having the very same fingerprint.

There are several fingerprint-matching algorithms such as minutiae based matching correlation based matching, based on genetic algorithms. The dominated one is among those minutiae-based matchings. (Aremu, 2014). There are advantages and disadvantages to a fingerprint biometric authentication system. One advantage of fingerprint recognition is that it has a long history of use. In relative terms, the use of fingerprints as an automated authentication tool is new compared to the centuries of manual fingerprinting of individuals for identification. Other advantages include factors such as the ability to use multiple fingers to scan for a template, the fingerprint is permanent and it does not change patterns with age, it is easy to use, and the sensors are inexpensive (NSTC, 2005). The disadvantages of fingerprint recognition include issues with public perceptions about its use such as touching the sensor will spread germs and the scanned image of the fingerprint could be reproduced or used for criminal investigations (NSTC, 2005). Research has also been performed on print quality in elderly individuals, which shows that as people grow older, there is a higher rate of reject rates in sensor recognition (Theofanos, et al., 2006).

### Face Recognition

Facial images are the mostly biometric feature used to identify yourself. Face recognition is done primarily through two methods, which are recognition based on one's own face and recognition of 3D face. The identification of one's own face works by analyzing face images and computing one's own faces, which are faces composed of individual vectors. According to (Millett, 2011) the comparative study of Eigen faces is used to determine the presence and individuality of the face. The Eigene face technique is simple, effective and, under controlled circumstances, usually offers decent results. (Millett, 2011)

3D facial recognition algorithms make 3D facial prototypes and compare the recognition faces for 3D. These systems are often more precise because although they capture the exact facial structure. One of the big concerns for 3D systems is the purchase of 3D data. (Millett, 2011)Facial thermos-grams, another face identification technology, uses an infrared heat scans to identify facial features. This nonintrusive technique is slightly independent and is not disguising fragile. Even plastic surgery, the process cannot be hindered. (Asima Akber Abbasi, 2013).

In contrast to fingerprint biometrics, there is no contact made in facial recognition biometrics. The disadvantage to this type of biometric is that the condition of the environment while obtaining the sample can affect the quality of the image (FDIC, 2004) Poor lighting, camera quality, and obstructions on the face by the individual requesting access can make a significant difference in the initial enrollment as well as subsequent attempts for access (NSTC, 2006).

### Iris recognition

Today, there are many biometric security systems in the world that use human body components like the vein, face, fingerprint, hand or voice. Yet the iris is a biometric identifier that is much more sophisticated and precise. (C.B. Tatepamulwar, 2014) No two irises are the same, like a snowflake. There is actually no similarity between the identical twins, or an individual's right and left eyes. In addition, the volume of information collected from a single iris is now significantly higher than fingerprints; the precision is vastly higher than DNA. (Dr. P.S. . Aithal, 2017) Therefore, the iris is the key component of all the most faultless of human authentication technologies.

(Asima Akber Abbasi, 2013)] In their research, they demonstrated that the eye iris detection system of this implemented eye system. A biometric system is an automated identification device based on a specific template or matching feature. Biometric system is one of the methods that has been used as a useful authentication mechanism for days now. (Millett, 2011) Iris recognition system is one of the most credible and distinctive biometric identifiers. The solution in this paper is to build a biometric authentication method using parallel approached iris recognition. (Sharma, 2015). Just as with the facial recognition biometric, there is no physical contact with a sensor. Noise such as eyelids, eyelashes, and contact lenses can decrease the accuracy of the biometric. There is also a negative public misperception that the eye is scanned with a light source, and that it would damage the eye (NSTC, 2006). Although the automated technology is new and consumer education is needed to reduce fears, research has found it to be very accurate (Bolle, 2004).

### Speech recognition

Speech Recognition (also known as Automatic Speech Recognition (ASR) or computer speech recognition). The method of transforming a speech signal to a set of words using a computer program (Peter Peer, 2013). Voice recognition technology has been widely used within telecommunication systems to automate the operator services as well as improve them (Anthony Vetro, 2009). There are usually three approaches to the recognition of biometric speech; Acoustic Phonetic Approach, Pattern Recognition Approach and Artificial Intelligence Approach (Clearbridge Mobile, 2016). The Acoustic Phonetic Approach was focused on identifying speech sounds and presenting certain sounds with correct labels. The pattern matching method involves two steps: pattern training and comparison of patterns.

One advantage to voice/Speech recognition is that the sensor needed to acquire the voiceprint is commonly available (i.e., telephones, cellphones) (NSTC, 2005). One of the disadvantages that have caused the need for more sophisticated technology is the threat of replay attacks where an unauthorized person attempts to gain access with a recorded version of the authorized user’s voice. Another disadvantage is that there can be a high false accept rate if a person has a cold or there is noise on the sensor (Bolle, 2004).

### Hand geometry

Hand geometry recognition systems use a variety of human hand dimensions including its form, palm size, and finger lengths and widths (Patrick Shen-Pei Wang, 2007). The technique is very simple, fairly user friendly, and inexpensive. Hand geometry based identification consists of the following steps, the capture and pre-processing of images, the choice of measurements and characteristics and, finally, designation and validation (Moss, 2009). The imaging equipment that is used for hand geometry recognition is simple and includes a platform where the hand and a camera should be placed. Pre-processing of the hand image to obtain the characteristics. The color image is transformed into a gray image with a subtracted background. (A Jain, 1999) In hand geometry, the measured features are the length, width and palm dimensions of the fingers. Once the characteristics are measured, a statistical analysis was conducted for choosing significant characteristics. Comparison of the features extracted using common distance measures such as Euclidean or Hamming distance (Sushma Jaiswal, 2011). Comparison is performed by normalized correlation between vectors of the sample and the vectors of the template function. If the connection meets the predetermined threshold, the user's identifier will be checked (Sushma Jaiswal, 2011).

### Signature

Recognition for signatures is based on how a person signs his or her name. Signatures are a biometric pattern that varies over time, and is affected by individuals' physical and emotional conditions. Advanced fraudsters may replicate signatures, which fool the system (Sushma Jaiswal, 2011). Biometric signatures are used to limit duplicate signature frauds in the banking and finance industries. Dynamic signature verification technology is used in which the parson makes signatures on sensitive contact devices such as PDA or tablet PC (Anthony Vetro, 2009). This technology is also configured to prevent unauthorized access in mobile phones, even when the device is stolen.

**Prior Research**

In a review of the research available concerning biometric technology, various types of research has emerged. There are studies available that are definitional in nature, such as an article by (Sanderson, 2000) which primarily outlines biometric technology as well as the different types of biometrics available. The researchers concluded from the information that the most suitable biometric technology for military battlefield requirements would be iris scanning due to the environmental conditions found on the battlefield. In an article by (Whisenant, 2003), the researcher bases a review of various biometrics as the reasoning behind his proposition that facial recognition integrated with an additional biometric, such as fingerprint recognition, would be a non-intrusive solution for sport venue management in deterring terrorist attacks.

**Biometric Adoption Studies**

In relation to biometric adoption research, two studies have focused on the acceptance of the technology by the individual. (James, et al., 2006) Used the Technology Acceptance Model (TAM) to determine the intention to use security technologies, and in the case of this study, specifically the use of biometric technology devices. The researchers surveyed the faculty staff and students at the University of Mississippi to which they were able to acquire 298 usable responses for the analysis of the following constructs: perceived physical invasiveness, perceived usefulness, perceived ease of use and intention to use. (James, et al., 2006) State that the results of the study found that the perceived need for security and perceived ease of use positively affected the individual’s perception of the usefulness of the biometric device, yet perceived physical invasiveness of the device had a negative impact for adoption intention. In a similar study, (Moody, 2004) researches why biometrics adoption has been slow, and in turn attempts to identify the public perceptions of biometric technology. A survey instrument was developed and produced a 27 sample of 300 usable responses. Moody found that individuals responding to her survey are not ready to participate in the commercial use of biometric devices.

**Security Controls**

Another focus of research in biometrics involves the benefits of biometric technology as a method of security control. For example, (Harris, 2002) study the benefits of biometric technology over the use of person identification numbers (PINs), cards or tokens for access to secure systems. They point out that with PINs, cards, and tokens an individual is identified as having the ability to access the information, whereas biometrics identifies the actual person requesting the access to the information. The purpose of their study is to provide information to organizations on the added security benefits of biometric technology and the need for stronger information assurance. This was accomplished by analyzing a set of pros and cons for biometric technology as well as six factors that would affect the adoption of biometrics. The six factors include economical, managerial, operational, technological, process-related, governmental and standards-related factors. In the analysis of this study, (Harris, 2002) find that biometric technology offers a level of security that cannot compare to traditional passwords. The researchers explain that biometrics offer multiple levels of security thresholds for how specific the individual’s access request is to the template of the biometric stored in the database, and any concerns with biometric security can be remedied with proper education and awareness. While (Harris, 2002) discuss the need to use biometric technology as a greater level of security, an article by (Ahmed, 2005)develop a system for enhancing the security of private keys with biometric technology. The researchers acknowledge the need for greater security in private keys due to the increase in electronic commerce and the information that is being stored on smart cards. By analyzing the current method for assembling a private key, the researchers added another factor by including a biometric fingerprint. The result is an enhanced security mechanism for dynamically regenerating private keys with the use of an individual’s fingerprint, password and smart card. As research is performed on the security benefits of biometric technology, there is equivalent research on the privacy concerns that surround it.

**Privacy Concerns**

(Zorkadis, 2004) produced an article analyzing the rising legal concerns related to the personal nature of biometric data as described in a paper by (Prabhakar, et al., 2003) where the researchers address three specific concerns: unintended functional scope, unintended application scope and covert recognition. For (Zorkadis, 2004) , the purpose of the study is to explain the principles that must be followed by biometric systems to be in compliance with current legislation, and to propose a method for securing the privacy of an individual’s information stored in a biometric database. This was accomplished by comparing the principles of purpose and the proportionality of biometric systems with current legal obligations. The researchers concluded that in order for biometric data to be kept private and follow current legislation rules, the following must occur:

1) The biometric identification data must only be used for the purpose that it was originally collected for,

2) The data would be less accessible to others for further processing if it were to be stored in a device owned by the data subject (such as a smart card), and

3) The data controllers must be educated on the rights of data subjects and to be aware of the techniques available that prevent a re-identification issue.

In a related article pertaining to the issue of privacy, (Alterman, 2003), (Langenderfer, 2005) discuss the use of biometric identification systems in relation to ethical concerns for one’s privacy. As with (Prabhakar, et al., 2003) and (Zorkadis, 2004), (Alterman, 2003) reiterates that the ensuing widespread deployment of biometric implementations must also provide a means for protecting the data from misuse. (N. K. Ratha, 2007) Add to this concern with an article describing vulnerabilities in a biometric system and how to potentially prevent them with techniques that, if implemented, would decrease the threat of information theft.

**Implementation Considerations**

With security and privacy concerns in mind, the following research papers describe what it would entail to successfully implement a biometric system into an organization. (Jain, et al., 2004) Identify in a discussion of pattern recognition the fundamental problems facing organizations when implementing biometric technology for widespread use: accuracy, scale, security and privacy. They further explain in detail how each of barrier requires further research and how each one stands in the way of widespread deployment. The researchers conclude that while there are adequate biometric systems deployed today on a small scale, not enough research has been performed on the wide use of sensitive personal data. As research projects are under way to answer the call of Jain et al., one paper in particular by

(Elliott, et al., 2004) describes research projects being performed at Purdue University in biometric technology. The result has been that when implementing a biometric system into an organization, the researchers have identified a few important factors to consider: the environment that the biometric scanner will be placed in, the quality of the image that is obtained, and the selection of the device used in acquiring the biometric element from an individual. In a related article, (Sticha, 1999) explain how the use of biometric technology has the potential in this industry to thwart duplicate enrollments and fraud found in the Food Stamp Program. (Sticha, 1999) found in their research that the biometric technology used must be acceptable to the user, accurate, resistant to fraud, and quick. Policy decisions are also vital to deterring fraud because fraud attempts occur most frequently at the point of enrollment.

In determining what barriers are in the way of implementation, (Riley Jr, 2005)studied the challenge organizations face when deciding if the implementation of a biometric system would be beneficial. The researchers identify a strategy for the decision making process by providing the reader with a step by step method in developing a business case specifically for the implementation of a biometric technology system. In addition to the previous paper, (Riley Jr, 2005) produced a paper on a method for identifying how biometric technology may be a valuable tool in mitigating organizational risk based on the level of risk and type of biometric used. (Chandra, 2005) provide a similar article for those organizations considering the implementation of a biometric authentication system by describing challenges, constraints and limitations of biometric technology that every organization should review while evaluating this type of technology.

**Biometric Technology in Financial Institutions**

While there is not widespread use of biometrics in financial institutions, there are a few organizations utilizing the technology. NCR and Diebold have each deployed biometric enabled ATMs overseas according to an article in the ABA Banking Journal (Orr, 2006)Various financial institutions have found biometrics useful for safety deposit box access, self-service kiosks and teller line transaction access (Giesen, 2006)The research in biometric technology has uncovered some common concerns among society. If an organization can be assured that, these concerns have been identified and resolved, is this enough of a tipping point for acceptance of the technology? If that still does not invoke acceptance, is there a particular issue that cannot be overcome?

# 2.2 Brief history of fingerprint.

The earliest date when prints of the ridged skin on human and feet were made was about 4,000 years ago during the pyramid building era in Egypt. In addition, one small portion of palm prints not known to be human has been found impressed in hardened mud at a 10,000years old sit in Egypt (Author, 2013). Although recent researches confirm that ancient human beings were aware of the individuality of the fingerprint, systematic studies of the fingerprint structure were initiated in the late of the seventeenth century. The story starts in 1684 by the anatomist Nehemiah Grew who was the first who scientifically studied the friction ridges. Later, Marcello Malpighi is credited to be the first who used the microscope to study the skin. He noted the presence of ridges, spirals and loops in fingerprints. Since then, friction ridge had been studied for many years (Belhadj, 2017). In 1788, the uniqueness of the ridge structure was announced by the German J. C. A. Mayer, whereas Hermann Welcker remarked that his fingerprint hadn’t change between the first impression and the second one taken after 40 years, he is credited to be the first who claimed the permanence of the friction ridges (Belhadj, 2017). In 1880, Henry Faulds published in a journal the value of friction ridge skin for individualization, especially its use as evidence of crimes. He is credited to be the first who used the ink to take fingerprint impressions. Just later, Francis Galton wrote a book on fingerprints, he introduced the notion of 'minutia' as permanent and unique characteristic. (Maltoni, et al., 2009)

In 1882, Gilbert Thompson of the U.S. geological survey in New Mexico used his own fingerprints on a document to prevent forgery; this is the first known use of fingerprint in the United States. (Author, 2013)

In 1901, witness the introduction of fingerprint for criminal identification in England and Wales using Galton’s observation and revised by Sir Edward Richard Henry. (Author, 2013)

By 1946, the FBI had processed 100 million-fingerprint card in manually maintained files and by 1971, 200 million cards. With the introduction of AFIS technology, the file was split into computerized criminal file and manually maintained civil files. **(**Moore G, 2005)

At the beginning of the 20th century, recognition of criminals by means of fingerprints became standard practices (Belhadj, 2017). “It would seem that nothing much more happened with regard to the wider area of biometrics until the 1960s, when the advent of electronics and integrated circuits presented the promise of automation” (Krishan, 2012). This helped a lot to make it possible at the beginning of 1970s to write algorithms and to use sensors to identify humans. A brief history timeline about the fingerprint recognition is given in Figure 3. It was common practice for the Chinese to use inked fingerprints on official documents, land sales, contracts, loans and acknowledgments of debts. The oldest existing documents so endorsed date from the 3rd century BC, and it was still an effective practice until recent times. Even though it is recorded that the Chinese used their fingerprints to establish identity in courts in litigation over disputed business dealings, researchers fail to agree as to whether the Chinese were fully aware of the uniqueness of a fingerprint or whether the physical contact with documents had some spiritual significance. (Author, 2013).

Thanks to these efforts, automated fingerprint recognition technologies have now rapidly grown to be used not only in forensic applications, that were the first adopters of the fingerprint recognition, but also in a wide range of applications such as control access, computer logon, e-commerce, etc. This is due to its high accuracy and acceptability as well as its low-cost technology.

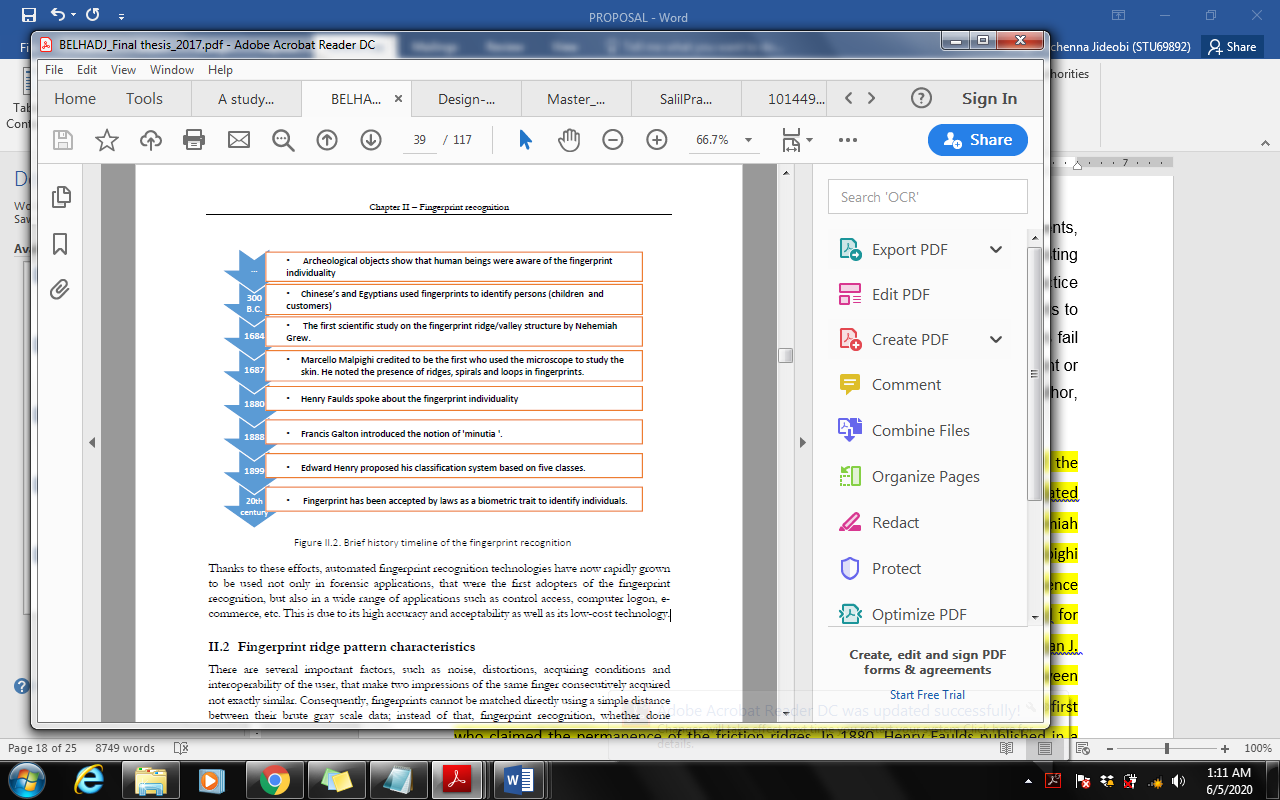


Figure 3. History of fingerprint recognition source: (Belhadj, 2017)

## 2.3.1 Using Biometrics:

Some of the instruments used for unique identification of humans include biometric identification systems known mainly for identification and verification. Here, we will use biometrics as for access management and access control of identity. Therefore, use of biometrics in fingerprint recognition is secure and easy for image acquisition step in fingerprint recognition as well. We can see many varieties of biometric systems like face detection, fingerprint recognition, iris recognition, voice recognition, palm recognition etc. but this project will only go for fingerprint recognition using a biometric device to capture fingerprint image.

# 2.5 WHY I USE FINGERPRINTS:

Fingerprints are considered as a unique identification of a person and due to easy access it’s the best and one of the fastest methods used in biometric identification systems. They are unique, so secure and reliable to use and doesn’t change for one in a lifetime. And beside these things, fingerprint recognition using minutiae matching technique is cheap, reliable and accurate up to a satisfactory limit.

Hence, fingerprint recognition is being widely used in both civilian and forensic applications. If, we will compare with other biometric devices then fingerprint recognition devices will hold the maximum market share and are most proven ones also. And we can also say that it’s not only faster than other biometric devices but its energy efficient also, as it consumes very less energy.

## 2.5.1 What is Fingerprint Recognition?

 The fingerprint recognition problem can be grouped into two sub-domains: one is fingerprint verification and the other is fingerprint identification. In addition, different from the manual approach to fingerprint recognition by experts, the fingerprint recognition here is referred as EFRMS (Electronic Fingerprint Recognition Management System), which is program-based.

**Identification Vs. Verification**

(Bolle et al., 2004, p. 17) define authentication as *“the process of reliably determining the identity of a communicating party”*. It is essentially the process ofestablishing who a given person is. Authentication is a process that involves bothidentification and verification. While identification answers the question “Who ishe?” verification answers the question “Is he Mr. X?” where Mr. X is the claimedidentity. For example, when a person withdraws money from the ATM, his card isused to identify him. Here, the account number is read from the card and is thencompared to all account numbers in the database, till a match is found. This isidentification. After the user has been identified, he is asked to enter his PIN,which is checked against the one associated with the identified account number.This is verification. Now that the person has been authenticated, he is free to continue with his banking issues. These same concepts of identification, verification and authentication are extended to biometrics as well. Identification is more time-consuming as well as a more difficult biometricprocess when compared to verification. When biometrically identifying a person,the biometric template is matched against all templates in the database to find outwho the person is. In other words, a **1:N matching** takes place (Nanavati et al.,2002). A 1:N matching is a one-to-many matching where ‘N’ is the number of database records. Given the value of **N**, this matching process can take a very long time since a decision (Match or No – Match) has to be made for each template in the database.

During verification on the other hand, the identity of the person is already established by some other distinct means. The biometric template only serves the purpose of validating this identity. Quoting (Furui, 1996), *“the fundamental* *difference between identification and verification is the number of decision* *alternatives”.* Verification matches the one live template against the one template stored for the established identity. It is a **1:1 matching** (Nanavati et al., 2002)where there are only two decision alternatives and where only a single decision needs to be taken.

Between a 1:1 and a 1: N matching, there is also a 1:few (one-to-few) matching method. Here, the template is matched against a small group of known users (Nanavati et al., 2002) to identify the person. The number of users may range from as few as five to as many as a hundred users. There is no clear distinction as to when a 1: few matching becomes a 1: N matching. For the scope of this thesis, we will concentrate on the verification process as we are looking to use biometrics for the verification process in mobile banking.

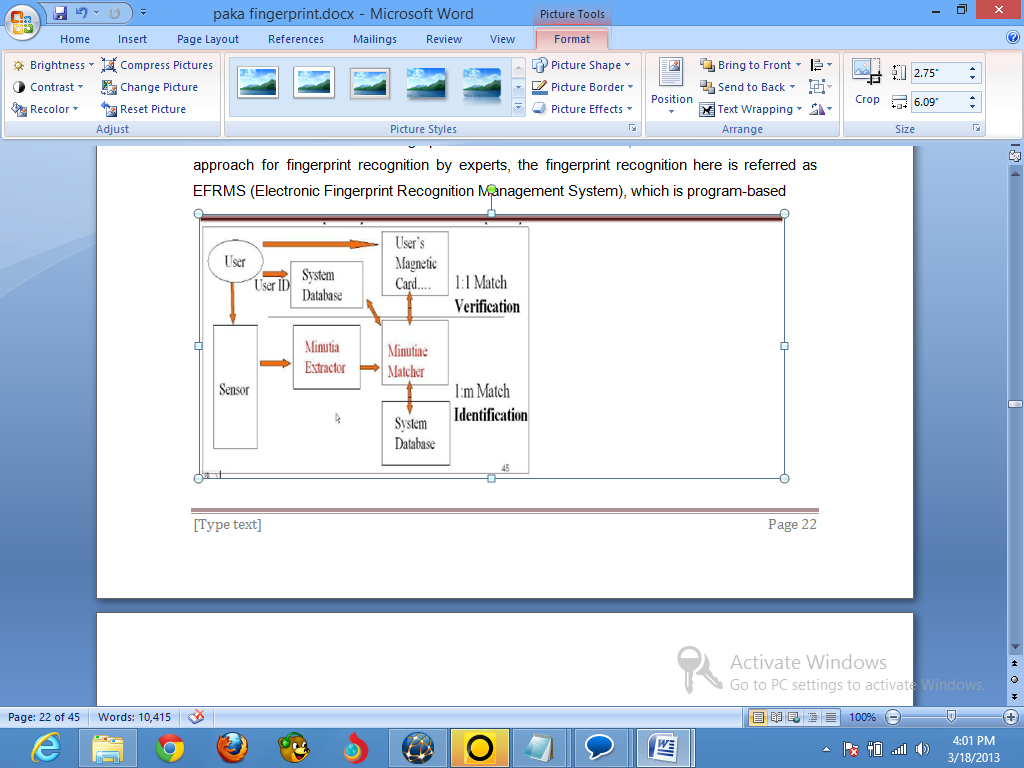


Figure 2 Verification vs. Identification. (Author, 2013)

## Two approaches for Fingerprint recognition

Two representation forms for fingerprints separate the two approaches to fingerprint recognition. The first approach, which is minutia-based, represents the fingerprint by its local features, like terminations and bifurcations. This approach has been intensively studied, also is the backbone of the current available fingerprint recognition products. This project also concentrates on this approach. The second approach, which uses image-based methods (LC Jain, 1999)tries to do matching based on the global features of a whole fingerprint image. It is an advanced and newly emerging method for fingerprint recognition. And it is useful to solve some intractable problems of the first approach. (Author, 2013).

**Using Biometrics in Mobile banking Systems**

In a set of interviews conducted by (Mallat et al., 2003), the results showed that one of the risks consumers see with mobile banking is that an unauthorized person would be able to make a transaction with their mobile banking application in case of loss or theft of the mobile device. Using biometrics instead of present authentication techniques could possibly eliminate this fear altogether. In terms of implementation, biometrics can be easily employed in mobile banking.

Depending on the type of biometric used, only a small hardware device needs to be added to the mobile device. If using speaker recognition, even this would not be necessary, since the microphone which is required for speaker recognition is already present in all mobile devices. For fingerprint recognition, a small reader would have to be fitted into the mobile device. There are already mobile phones fitted with fingerprint sensors. On research, the earliest model that could be found was the Korean company Pantech’s GI100 which was launched in 2004. In 2006, Pantech launched a follow-up model, the PG 6200 in Asia and the USA; Interestingly, the PG 6200 also has voice recognition capabilities. In 2008, the laptop company Lenovo introduced their first mobile phone, the P620, with a fingerprint sensor. In January 2009, NTT DOCOMO launched the Fujitsu F-01A mobile phone with fingerprint technology from AuthenTec, which is supposed to be waterproof as well. All these phones use fingerprint recognition to “unlock” the phone. This means that only the owner is able to use the phone.

There are also a few banking applications that use biometric authentication. Mobilkom Austria and ekey biometric systems had launched a project where visitors could buy tickets to the Ars Electronica Festival 2001 using mobile banking secured by fingerprint recognition (ekey Biometric Systems, 2001). Although not a mobile banking application, in parts of Germany consumers are able to buy products at their local supermarket using fingerprint verification through DigiPROOF.

**Biometric system architecture** A typical biometric system is constituted of four principal modules **Figure 3**:

* **Biometric sensor**: it is responsible for capturing the biometric characteristics from the biometric subject and converting it to a digital form to be transferred to the subsequent module. The performance of the overall process depends heavily on the quality of the acquired raw data. In fact, this data is a result of transforming a real continuous phenomenon (such as a face) to a digital discreet form (face image) resulting in a loss of data. The quality of the acquired data depends on the technology of the reader, the added noise and the degree of the interoperability of the user with the system.
* **Enrollment**: the acquired raw data is first preprocessed to enhance its quality. After that, some relevant discriminatory features are extracted, by the extractor sub-module, to generate a compact representation called “template” that efficiently resumes the biometric characteristics. The generated template is then sent to the storage system. Generally, the enrollment step allows the biometrics recognition system to learn the identities of the authentic persons in working environment.
* **Storage system**: the storage system can be a simple file in a simple smartcard as it can be a big database managed by an SGBD. In association with the generated template, some biographic information (name, passwords, address, etc.) can be stored. In any case, the important factor to deal with is the security of the stored template. A compromised template can help to reconstruct the original biometric characteristics, which constitutes a real threat.
* **Matching module**: during the operating phase, the system is requested to identify a person. It proceeds to extract his discriminatory features using the extractor sub-module in the same manner that it has been done in the enrollment step. These extracted features are called query features. After that, the stored template is revoked to be compared with the query. The comparison aims to confirm that both the query and the template features originate from the same biometric subject (person). Generally, the comparison result is a degree of similarity ranging between 0 (total mismatch) and 1 (perfect match) that allows the system to take the suitable decision about the identity of the user.

On the other hand, the biometric system can operate either in verification or identification mode. In verification mode, the comparison is made only against one template in the system by conducting 1 to 1 comparison. This is possible when we want to confirm the identity claimed by a user. In the identification mode, the comparison is achieved against all records in the database by conducting 1 to many comparisons. This is the case when we want to know if the individual already exists in the database. Therefore, the system try to answer the question “who is the user?”

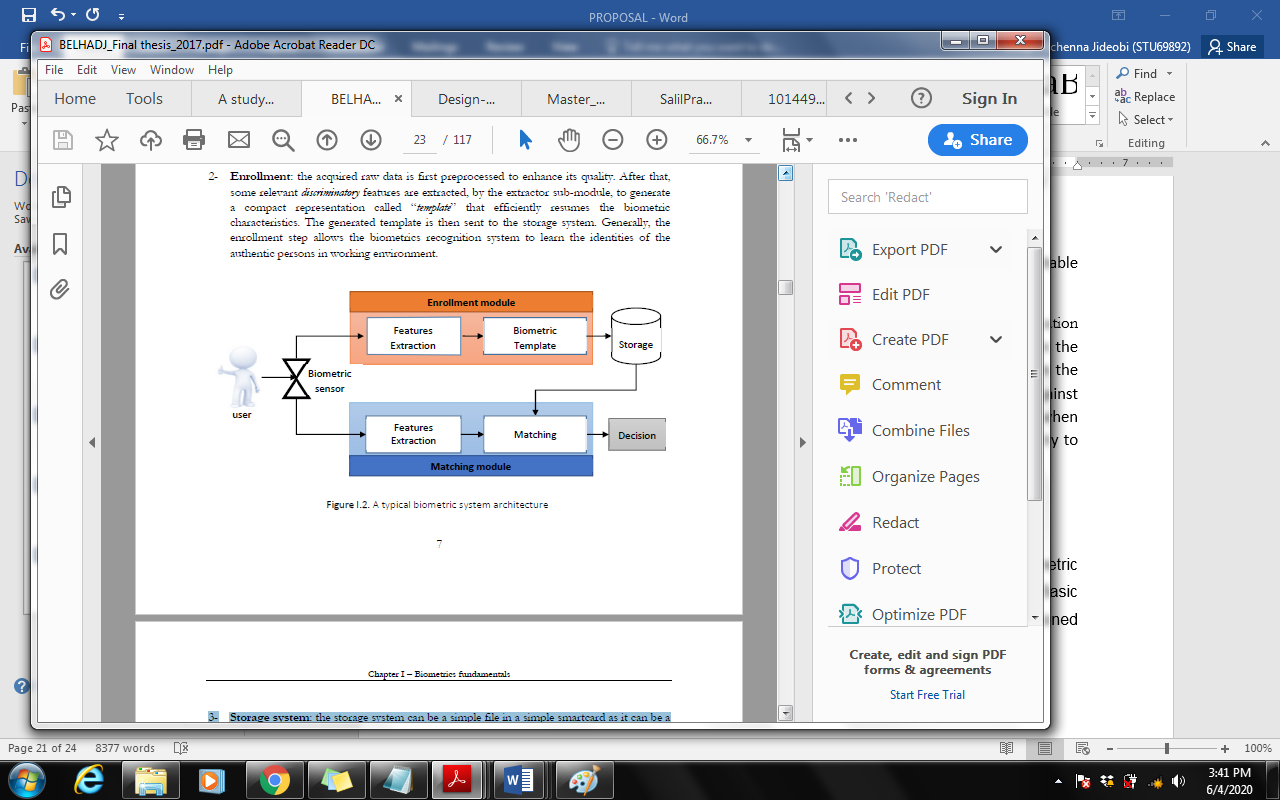


Figure 3: Biometric system matching architecture (Belhadj, 2017)

# **Programming Language Research**

The most popular programming language in designing such mobile Biometric identification system is Java, C#, Visual Basic, and MATLAB. Since C# and Visual Basic share the same .Net framework, the developer decided to compare one of the mentioned .NET programming language, Java, and MATLAB.

# 

# **Methodology**

# **3.0 Overview of Research methodology**

Research methodology is a collective term for the structured process of conducting research.  There are many different methodologies used in various types of research and the term is usually considered to include research design, data gathering and data analysis. Research methodologies can be quantitative (for example, measuring the number of times someone does something under certain conditions) or qualitative (for example, asking people how they feel about a certain situation). It’s includes the following concepts as they relate to a particular discipline or field of inquiry.

* A collection of theories, concepts or ideas.
* Comparative study of different approaches and
* Critique of the individual methods (Author, 2013)

# 3.1 **Fact Findings Methods**

Fact finding is the process of collecting information with regards to the proposed system. Interviews, questionnaires, samplings and readings manual are the typically traditional ways of fact finding but, there are other techniques used to collect information about systems, requirements and preferences. It’s also known as information gathering or data collection.

# **3.2 Gathering User Requirements**

A good set of user requirement are needed for any project to be successful**,** mostly computer system projects. This is where many projects fail, in that they do not specify correctly what the system should do. In fact many systems have just been given a deadline for delivery, a budget to spend, and a vague notion of what it should do. The root of this problem is:

* Computer systems developers rarely have a good idea of how a business runs and should run, compared with a business user,
* Business users have little idea of what a computer system could achieve for them.

# **3.3 Interviews**

Goals are important information that can be gleaned from interviewing. The Facts that the developer obtain from hard data may explain past performance, but goals project the organization’s future. Developer may not be able to determine goals through any other data-gathering methods. In doing qualitative research, there is often the need to conduct interviews for the purpose of data collection.

# **3.4 Survey**

The Survey method is the technique of gathering data by asking questions to people who are thought to have desired information. A formal list of questionnaire is prepared. Generally a non-disguised approach is used. The respondents are asked questions on their demographic interest opinion.

##### **Advantages of Survey Method**

* As compared to other methods (direct observation, experimentation) survey yield a broader range of information. Surveys are effective to produce information on socio-economic characteristics, attitudes, opinions, motives etc and to gather information for planning product features, advertising media, sales promotion, channels of distribution and other marketing variables.
* Questioning is usually faster and cheaper than Observation.
* Questions are simple to administer.
* Data is reliable
* The variability of results is reduced.

It is relatively simple to analyze, quote and interrelate the data obtained by survey method.

# 3.5 Questionnaire

Questionnaires are an inexpensive way to gather data from a potentially large number of respondents (Bell, J (1998)). Often they are the only feasible way to reach a number of reviewers large enough to allow statistically analysis of the results. Although questionnaires may be cheap to administer compared to other data collection methods, they are every bit as expensive in terms of design time and interpretation. (Denial, 2006)

# **System requirement**

## Hardware Architecture

The hardware to be used mobile phone that has fingerprint sensor which captures the image, and also houses the database, which runs the comparison algorithm and simulates the application function. Basically this work does not involve the development of hardware. The SDK can be used as an interface between the fingerprint reader and the mobile banking software. We also need a printer and a server.

## Software Architecture

The software architecture consists of: the database and the application program.

**Database:** The database consists of tables that stores records implemented in Microsoft SQL database. However, this can be migrated to any other relational database of choice. SQL/Amazon database is fast and easy, it can store a very large record and requires little configuration.

## Functional requirement

Functional requirementscapture the intended behavior of the system. This behavior may be expressed as services, tasks or functions the system is required to perform. The functional requirement here is refer to the ability of the system to manipulate the data’s in the database. (Author, 2013).

* Ability to save, update, customer information: this function enables the system user to enroll, make transactions, and view account statement information.
* Ability to view and generate account statement: this function enables the user to view his/her account statement. Here only the system administrator can be able to view all user account statement.
* Ability to login to the system: this function allows the user to be able to log into the system. Even though the user only have access to certain or only his or her information because of restricted access, the administrator of the system have access to all the system.
* Ability to authenticate user: this function allow the system to verify the user.

## Nonfunctional requirement

They are some obvious features and functions that are required in a system, there are other requirements that don't actually perform any task, but are important characteristics nevertheless. These are called "non-functional requirements" or sometimes "Quality Attributes."  For example, attributes such as performance, security, usability, compatibility. They aren’t a "feature" of the system, but are a required characteristic. One can't write a specific line of code to implement them; rather they are "emergent" properties that arise from the entire solution. (Author, 2013)

* **Reliability**: Reliability is the ability of a system to perform its required functions under stated conditions for a specific period of time
* **Availability:** is the ability of the system to be available for service when requested by end-users.
* **Failure rate**: Is the function that tells us how often the system fails to deliver the services as expected by end-users.
* **Dependability:** Dependability of the system is the ability to deliver service that can justifiably be trusted by users
* **Usability**: Usability is the ease with which a user can learn to operate, prepare inputs for, and interpret outputs of the system or command.
* **Security:** Security requirements are included in a system to ensure:

1. Unauthorized access to the system and its data is not permissible.
2. Ensure the integrity of the system from accidental or malicious damage.

A good example of security requirement in the system is that the access permissions for the system data can only be changed by the system’s administrator with the permission of the account holder.

**Software development methodology**

# **Methodology Overview**

Before considering a framework for selecting a given SDLC methodology, one needs to understand the choices. SDLC methodologies all focus on the common goal of defining the steps and processes from the beginning of a software project through its completion. Traditional engineering models have depicted these steps as Requirements Analysis, Design, Development, Test, and Implementation. However, contemporary thinking provides for a cradle-to-grave perspective by which IT and LOB are closely linked in the process. Accordingly, the models herein presented add a step to the beginning (Scope) and Ending (Operations and Maintenance) of each methodology. Scope (sometimes referred to as Strategy, Feasibility, or Concept of Operations) captures the preplanning, business case, and boundaries of the software project. Operations and Maintenance (sometimes referred to as Production Support, Post Install, or Execution) captures the day-to-day ongoing activities necessary to sustain the system.

# **Rational Unified Process (RUP) Methodology**

The rational unified process (RUP) is a software process product designed as an object oriented and web-enabled program development methodology by Rational Software Corporation, a division acquired By IBM since 2003.

This methodology is fast becoming a popular software development to map business process and practices. Development is phased into four stages. RUP methodology is highly flexible in its developmental path, as any stage can be updated at any time. The first stage or inception centers on assessing needs, requirements, viability and feasibility of the program or project. The second step or elaboration measures the architecture of the system's appropriateness based on the project needs. The third stage is the construction phase, wherein the actual software system is made, by developing components and features. This phase also includes the first release of the developed software. The final stage is that of transition, and marks the end of the development cycle, if all objectives are met. This phase deals with the training of the end users, beta testing and the final implementation of the system.

## Six best industry practices of RUP

RUP is designed to incorporate the six best software industry practices for software development, while stressing strongly on object-oriented design. They are basically six ideas, when followed while designing any software project, will reduce errors and faults and ensure optimal productivity. The practices are listed below:

* **Develop Iteratively**

Loops are created to add extra information or to facilitate processes that are added later in the development stage.

* **Requirements**

Gathering requirements is essential to the success of any project. The end users' needs have to be built into the system completely.

* **Components**

Large projects, when split into components, are easier to test and can be more methodically integrated into a larger system. Components allow the use of code reuse through the use of object-oriented programming.

* **Design Model Visual**

Many projects use Unified Modeling Language (UML) to perform object-oriented analysis and designs, which consist of diagrams to visually, represent all major components.

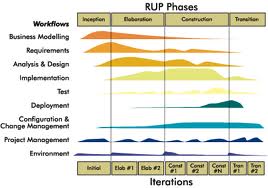
* **Quality and Defects Management**

Testing for quality and defects is an integral part of software development. There are also a number of testing patterns that should be developed, to gauge the readiness of the project for its release.

* **Synchronized Changes**

All components created by separate teams, either from different locations or on different platforms need to be synchronized and verified constantly.

RUP's developmental approach has proved to be very resourceful and successful for a number of reasons. The entire development process takes into account the changing requirements and integrates them. Risks and defects cannot only be discovered but addressed, and reduced or eliminated in the middle of integration process. As defects are detected along the process, errors and performance bottlenecks can be rectified by making use of the several iterations (loops). RUP provides a prototype at the completion of each iteration, which makes it easier for the developers to synchronize and implement changes.



RUP Methodology (Author, 2013)

## The six engineering discipline

* **Business modeling discipline**

Business modeling explain how to describe a vision of the organization in which the system will be deployed and how to then use this vision as a basis to outline the process, role and responsibly.

* **Requirement discipline**

Requirement explain how to elicit stakeholder request and transform them into a set of work product that scope the system to be built and provide detailed requirement for what the system must do.

* **Analysis and design discipline**

The goal of analysis and design is to show how the system will be realized. The aim is to build a system that: performance fulfills requirement and easy to change when functional requirement change.

Design result into a design model and analysis optionally into an analysis model. The design model serves as an abstraction of source code; that is the design model acts as a blueprint of how the source code is structured and written.

* **Implementation discipline**

The purposes of implementation are:

* To define the organization of the code in terms of implementation subsystems that is organized in layers.
* To implement class and object in terms of components
* To test the developed components as unit.
* **Test discipline**

The purposes of test are:

* To verify the interaction between object
* To verify the proper integration of all components of the software
* To verify that all requirement have been correctly implemented.
* **Deployment discipline**

The purpose of deployment is to successfully produce product releases, and to deliver the software to it end users. It covers a wide range of activities including producing external releases of the software.

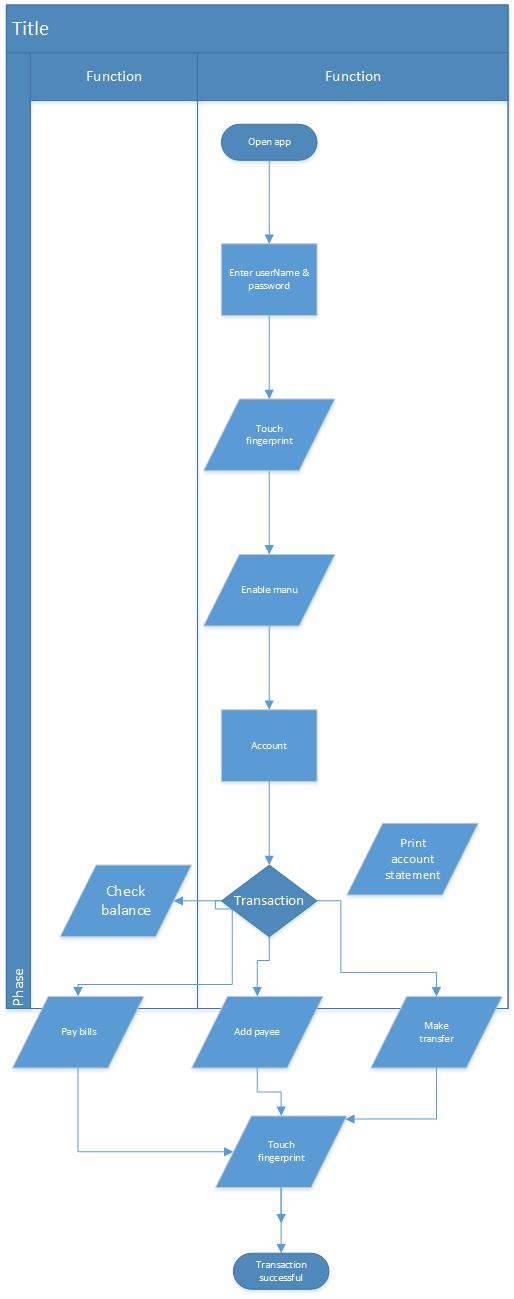
However after analyzing all the methodology I found that RUP offers more plus points than any other methodologies. With the assistance of RUP one can be able to effectively structure and manage the development of a mobile application such as mobile banking using fingerprint authentication, focusing on the vital area of image processing, and user involvement. Since RUP allows for flexible integration of other techniques. The benefits of other methods will be used to complement it at various stage in it lifecycle.

|  |  |  |  |
| --- | --- | --- | --- |
| Criteria | Waterfall | Spiral | RUP |
| Cover all the aspect of SDLC |  |  |  |
| Provides support for data modeling |  |  |  |
| Able to define technical problem |  |  |  |
| Involves user in development |  |  |  |
| Provide support for project management control |  |  |  |

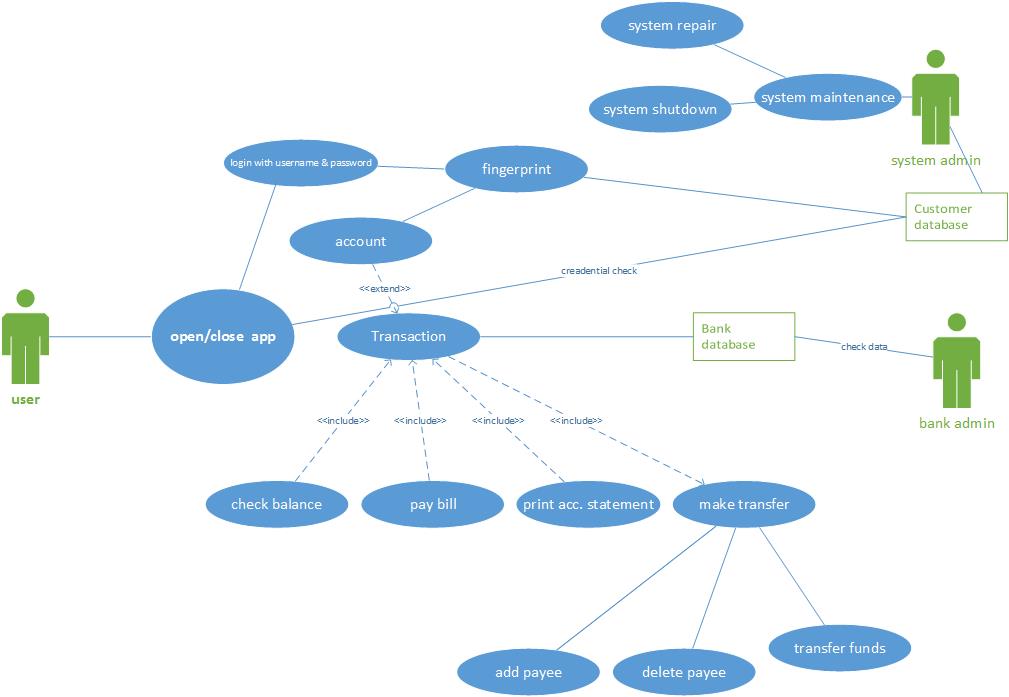
The table above show that fact that RUP is the closest matches to mobile application requirement. RUP has many advantages which help in developing a sturdy mobile application over other system development methodologies.

# **Conclusion:**

In this chapter, I was able to discuss about different types of programming paradigm, as well as different types of fact-finding, and software development life cycle.



Flow chat diagram



Use case diagram